Faculté de droit
de sciences politiques et de gestion
Université de Strasbourg

eucor
Le Campus européen

Mémoire de recherche

Master 2 droit public comparé EUCOR

2019 – 2020

Intelligence artificielle, justice pénale et protection des données à caractère personnel

Yamina Bouadi

Sous la direction de **Madame la Professeure Juliette Lelieur**
Professeure de droit pénal à l'Université de Strasbourg

Assesseur : **Monsieur Yannick Meneceur**
Conseiller en politiques de transformation numérique et d'intelligence artificielle au Conseil de l'Europe

J'adresse mes remerciements à ma directrice de mémoire, Professeure Juliette Lelieur, pour sa patience, ses conseils et ses encouragements.

Je remercie Monsieur Yannick Meneceur pour sa disponibilité.

Je suis également reconnaissante envers l'expérience apportée par ma participation avec l'Université de Bâle (Suisse) au concours René Cassin 2020 dont le sujet m'a inspirée. Merci au Professeur Dr. iur. Stephan Breitenmoser.

Enfin, je remercie mes parents, ma sœur, mon frère et l'ensemble de mes amis pour leur soutien.
En particulier Isabelle, pour son amitié inconditionnelle et nos encouragements mutuels dans la rédaction confinée de nos mémoires.

Sommaire

Table des matières

Liste des abréviations

§	paragraphe
§§	paragraphes
al.	alinéa(s)
art.	article(s)
c.	contre
ConvEDH	Convention de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950
CEDH	Cour Européenne des Droits de l'Homme
CEPEJ	Commission Européenne pour l'efficacité de la Justice
CNIL	Commission Nationale de l'Information et des libertés
cf.	confer
Cour	Cour européenne des droits de l'Homme
CJUE	Cour de justice de l'Union européenne
Ed.	Édition
IA	Intelligence artificielle
Ibid.	Ibidem
no	numéro
nos	numéros
op. cit.	opus citatum
p.	page
pp.	pages
RGPD	Règlement (UE)2016/679 règlement général sur la protection des données, 27 avril 2016
s.	suivant(e)
UE	Union Européenne
vol.	volume

Introduction générale

« Ces quantités massives de données et les Big data entrent en opposition frontale avec les grands principes de la protection des données : la minimisation, la finalité, la limitation dans le temps. Les Big data, c'est au contraire une collecte maximale, automatique, par défaut, et la conservation illimitée de tout ce qui existe sous une forme numérique, sans qu'il y ait, nécessairement, de finalité établie a priori. »

Antoinette Rouvroy[1]

L'actualité de la thématique de l'utilisation des données à caractère personnel par des dispositifs technologiques pouvant mener à des sanctions, en fait son intérêt. En raison d'une pandémie, du 17 mars au 11 mai 2020, la France est plongée dans une période de confinement et le décret n°2020-293 du 23 mars 2020, impose aux individus de rester au maximum au sein de leur habitation et de n'en sortir qu'en cas d'urgence ou lors d'achats de première nécessité. Le fait de sortir de chez soi pour une raison non prévue par le décret susmentionné, constitue une infraction punie d'une amende s'élevant à 135 euros. Avant même de penser à une possibilité de vaccin afin d'éliminer le virus, une multitude de mesures de surveillance du respect de cette obligation a vu le jour en France, dans le but d'empêcher la propagation du pathogène. Prenons l'exemple de l'attestation de déplacement dérogatoire, initialement en papier, à imprimer ou recopier à la main.

La sanction dont l'attribution repose sur l'engrenage des données et des nombres. La version numérique de l'attestation est apparue sous la forme d'un formulaire en ligne. Ce dernier fut à remplir avec les informations d'identité de l'individu (nom, prénom, date de naissance, adresse), la date, l'heure et bien-sûr, la raison du déplacement. Dès le lendemain de l'annonce du confinement, la Commission Nationale de l'Information et des Libertés (CNIL) – autorité chargée de veiller à ce que l'informatique ne nuise pas aux droits de l'Homme – a mis les français en garde contre les *cookies*[2] provenant des sites non officiels susceptibles de collecter les données des appareils utilisés, et capables d'identifier de quel ordinateur ou téléphone, l'attestation en ligne a été téléchargée. L'ancien ministre de l'intérieur français a confirmé que, par cette attestation en ligne, aucune donnée

[1] Entretien d'Antoinette Rouvroy, « Big data : l'enjeu est moins la donnée personnelle que la disparition de la personne », recueilli par Serge Abiteboul et Christine Froidevaux, Le Monde, le 22 janvier 2016.

[2] Adrien Basdevant, Jean-Pierre Mignard, « L'empire des données, essai sur la société, les algorithmes et la loi », Ed. Don Quichotte, 2018, p. 65 : « Les cookies sont des petits fichiers texte – moins de 4 kilooctets – stockés par le navigateur web sur le disque dur du visiteur d'un site. Ils contiennent généralement une chaîne de nombres utilisée pour identifier un ordinateur. Par la reconnaissance de cette clé d'identification incluse dans toutes les requêtes suivantes faites au même serveur, les cookies permettent d'établir le profil de navigation de l'internaute ».

personnelle ne fût collectée ou enregistrée au sein de la base de données du ministère de l'intérieur[3]. En revanche, il est possible de consulter l'heure à laquelle l'attestation a été établie et l'adresse de son propriétaire passible d'une amende, s'il est sorti de chez lui pour une durée et dans un périmètre dépassant la limite imposée.

La société est « subordonnée à la technique »[4]. Le débat de la collecte des données s'est de nouveau ouvert les semaines suivantes par la création d'une application mobile de traçage des individus atteints du virus ou ayant été en contact avec un individu infecté. Ces applications ont fait l'objet d'une importante médiatisation, partagée d'une part entre la perception positive de l'avancée de cette technologie – permettant si elle est téléchargée par un grand nombre d'individus, de réguler la propagation du virus. D'autre part, c'est un sentiment de crainte qui apparaît par la surexposition des individus à la surveillance de leurs déplacements pouvant nuire à leurs libertés fondamentales.

La justification contextuelle d'une telle restriction des libertés et des droits fondamentaux. La CNIL est saisie en urgence le 15 mai dernier par le ministère des solidarités et de la santé, questionnant la conformité de l'application mobile aux mesures de protection des données, soit principalement à la loi informatique et libertés du 6 janvier 1978 (citée « Loi informatique et libertés ») [5] ainsi qu'au règlement général européen relatif à la protection des données (cité « RGPD »)[6]. La CNIL rappelle au sein de son avis du 25 mai 2020 que, dans ce contexte d'état d'urgence sanitaire, « la lutte contre cette épidémie, […] constitue un impératif majeur de nature à justifier, des atteintes transitoires au droit à la protection de la vie privée et des données à caractère personnel »[7]. Après examen des conditions de mise en œuvre de l'application mobile, la CNIL « estime que ce dispositif temporaire, dont l'utilisation repose sur le volontariat, peut légalement être mis en œuvre »[8]. L'application *Stopcovid* est alors disponible sur les plateformes de téléchargement depuis le 2 juin 2020, à la suite de l'approbation du dispositif par l'Assemblée Nationale et le Sénat le 27 mai dernier. Elle est dépeinte par le gouvernement comme un outil permettant de « prévenir les personnes qui ont été à proximité d'une personne testée positive, afin que celles-ci puissent être prises en charge le plus tôt possible, le tout sans jamais sacrifier nos libertés individuelles »[9]. Le

---

3 Christophe Castaner, Twitter, 6 avril 2020, https://twitter.com/CCastaner/status/1247102332162244608?ref.

4 Maurice Weyemberg, *J. Ellul et M. Heidegger. Le prophète et le penseur*, dans Troude-Chastenet P., *Sur Jacques Ellul*, PUF, 1994, p. 86.

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

6 Règlement (UE) 2016/679 du parlement, sur la protection des données à caractère personnel.

7 Délibération de la CNIL, n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid », §4. Passage souligné par mes soins.

8 CNIL, avis sur les conditions de mise en œuvre de l'application Stopcovid, 25 mai 2020.

9 Site internet du ministère français de l'économie, des finances, de l'action et des comptes publics, 2 juin 2020.

gouvernement anticipe ainsi la crainte des risques portés à la protection des données à caractère personnel et à d'autres droits fondamentaux, constitués par cette application.

L'utilisation des données personnelles par des dispositifs technologiques afin de surveiller des comportements contraires à des règles sociales, en l'occurrence des règles sanitaires, s'inscrit dans un mouvement large de la transformation numérique de la répression des comportements transgressifs à la norme. Cette transformation numérique est menée par l'utilisation de dispositifs de plus en plus automatisés et auto-apprenants, tels que l'IA.

1. L'intelligence artificielle, un terme fréquemment employé mais rarement défini. L'emploi du terme IA est parfois étendu de manière erronée à toute technique informatique simplifiant le travail exercé par l'être humain. Il convient d'apporter une définition appropriée à ce terme non récent. La naissance de l'IA remonte aux années 1950, lors desquelles, l'idée de machine universelle apparaît dans les écrits d'Alan Turing notamment[10]. En août 1955, l'appellation « intelligence artificielle » est employée par John McCarthy et Marvin Minsky[11]. En 1956, l'ordinateur *Deuce* est conçu suivant les plans d'Alan Turing et l'idée que l'ordinateur puisse reproduire l'esprit, soit l'intelligence de manière artificielle, est mise en pratique[12]. A partir des années 1980, pour simplifier la réalisation de ce genre de dispositifs, il est décidé de les appliquer à des cas précis et réels, ce qui donnera l'émergence des systèmes experts. En 1997, le programme d'échec *Deepblue* a réussi à battre le champion du monde, par exemple. En 2016, un nouveau programme, dénommé *Alphago*, appartenant aujourd'hui à Google, a réussi à battre *Deepblue* au jeu de go[13]. Outre la parfaite opération de communication de cet exploit pour la qualité des dispositifs d'apprentissage de Google, la victoire d'*Alphago* démontre la rapidité avec laquelle se développent ces logiciels tout en surpassant de manière inédite les capacités humaines aux jeux de logique dont les combinaisons sont infinies.

Ainsi, l'IA existe depuis la moitié du XXe siècle, cependant récemment, une croissance constante des données est observée et la définition de l'IA s'étend à de plus en plus d'outils. Par exemple, il y a deux ans, l'IA ne s'appliquait pas aux arbres de décisions « *decision trees* », fonctionnant sous la

---

[10] Alan Turing, « Computing Machinery and Intelligence », Revue philosophique Mind, 1950. Dans cet ouvrage, il étudie la possibilité pour une machine d'être consciente ou non. Alan Turing s'est notamment concentré sur le fait d'introduire une intelligence au sein de machines.

[11] John McCarthy, Marvin Minsky, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 31 août 1955, http://raysolomonoff.com/dartmouth/boxa/dart564props.pdf.

Voir aussi : Yannick Meneceur, « Intelligence artificielle et droits fondamentaux », dans Patrick Gielen et Marc Schmitz, Avoirs dématérialisés et exécution forcée, Ed. Bruylant, novembre 2019, p. 94.

[12] En 1956, l'ordinateur anglais prénommé « Deuce » est conçu suivant les plans d'Alan Turing.

[13] Le jeu de go est d'origine chinoise et est le plus ancien jeu de stratégie combinatoire.

forme d'arbres de probabilité[14]. L'IA a récemment été définie par la Commission européenne pour l'efficacité de la justice (CEPEJ)[15], dans sa charte éthique de 2018, comme étant un « ensemble de sciences, théories et techniques dont le but est de reproduire par une machine des capacités cognitives d'un être humain. Les développements actuels visent à pouvoir confier à une machine des tâches complexes auparavant déléguées à un humain »[16]. La complexité de ces tâches est notamment due à la somme massive de données à traiter par l'humain. En effet, nous vivons dans un « monde des données »[17], dont l'utilisation est normalisée lorsqu'il s'agit de prévenir et réprimer des actes infractionnels.

2. La transformation numérique de la justice pénale. La notion d'IA employée avec le concept de justice pénale peut facilement renvoyer d'une part aux technologies participant aux infractions pénales intentionnellement produites, notamment en matière de cybercriminalité[18]. D'autre part, est également observé en Europe, un débat quant à la commission d'infractions pénales de manière involontaire en raison des biais présents dans des dispositifs d'IA tels que les voitures autonomes[19]. Ce sont deux thématiques profondément passionnantes qu'abritent les termes de l'IA et de la justice pénale cumulés. En revanche, ces sujets ne seront pas traités dans le cadre de notre étude, consacrée à l'utilisation de dispositifs d'IA assistants la justice pénale, notamment en matière de la prévention et la répression des infractions pénales.

L'utilisation de dispositifs d'IA au sein du secteur de « justice pénale » vise la prévention des infractions, la résolution d'enquêtes judiciaires et le procès pénal, au sein notamment des autorités de prévention et de répression des infractions pénales. Le traitement des données dans le cadre pénal n'est pas récent et est intrinsèquement lié à la prévention et la répression des infractions. Il peut être automatisé ou non. A titre d'exemple, l'organisation de données en version papier par ordre alphabétique dans une étagère, est inclue dans le terme traitement, bien que cette notion tende aujourd'hui à exclusivement diriger notre esprit vers le domaine numérique et automatisé.

La production de données judiciaires est aujourd'hui massive, notamment par le phénomène de l'*open data* des décisions judiciaires dont il est question en France depuis la loi pour une République numérique[20] et entraîne une interaction avec des dispositifs d'IA développés par des *legaltechs*,

---

[14] Ronald LEENES, Professeur de Régulation par la technologie, Institut du droit, de la technologie et de la société de Tilburg, Université de Tilburg, lors de la session parlementaire européenne sur « L'intelligence artificielle au sein de la justice pénale et son utilisation par la police et les autorités judiciaires en matière pénale », 20 février 2020.
[15] Commission créée en 2002, réunissant des experts issus des 47 Etats membres du Conseil de l'Europe.
[16] Charte éthique de la CEPEJ, p. 77.
[17] Adrien Basdevant, Jean-Pierre Mignard, op.cit., p. 10.
[18] Voir à ce sujet les travaux du comité de la convention sur la cybercriminalité (T-CY).
[19] Voir à ce sujet les travaux du comité européen pour les problèmes criminels (CDPC).
[20] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

sociétés privées. Ces dispositifs permettent de traiter l'importante quantité de données et sont alors utiles à la préparation du procès pénal. Par ailleurs, les données utilisées par l'IA peuvent être sujettes à une publication ou à des transferts transfrontaliers à des fins de coopération pénale, notamment à destination de dispositifs d'IA étrangers non régulés de façon identique dans l'ensemble de l'UE. En revanche, les enjeux et risques portant sur les droits relatifs à la protection des données sont accentués par l'utilisation de ces dispositifs.

3. Les dispositifs d'IA traitant des données personnelles : des « héros positifs […] pour lesquels la gloire et l'abomination n'étaient pas dissociées » [21]. L'utilisation des données personnelles par ces systèmes algorithmiques auto-apprenants n'est pas sans risque pour les droits et libertés individuelles, notamment le droit à la protection des données personnelles. Ce droit prend sa source au sein du concept du droit à la vie privée. La protection de la vie privée figure au sein de nombreux textes recensant les droits fondamentaux en Europe, notamment à l'article 8 de la Convention Européenne des Droits de l'Homme (ConvEDH) depuis 1950, ou encore à l'article 7 de la Charte des droits fondamentaux de l'Union Européenne, depuis 2000. Par ailleurs, ce dernier texte prend en compte l'évolution technologique en remplaçant le terme « correspondances » par « communications ». Au fil des années, la protection des données à caractère personnel a été englobée dans l'article 8 de la ConvEDH, entrant dans la protection de la « sphère privée »[22].

Dans l'optique de ne pas tomber dans « deux travers symétriquement caricaturaux que sont le techno-optimisme et le techno-pessimisme »[23], il faut ici souligner l'importance que cette étude donne à la recherche d'un équilibre entre le besoin d'efficacité de la justice pénale par le recours à l'IA et la promesse européenne de protection des données à caractère personnel. Il s'agit d'un sujet dont la régulation est en constante évolution au sein des institutions européennes. Il s'agit d'offrir aux individus une protection optimale de leurs données à caractère personnel sans que ces textes deviennent obsolètes dès leur mise en application. Il est à noter que le concept européen de la protection des données à caractère personnel en matière pénale au sein de cette étude est observé sous deux angles généraux. Dans un premier temps, du point de vue du **Conseil de l'Europe**, possédant pour ambition et but premiers un espace européen responsable et respectueux des **droits de l'Homme**. Dans un deuxième temps, une vision de l'**UE**, prenant la forme d'un équilibre entre d'une part, la **nécessité de faciliter le transfert des données entre Etats membres** dans l'optique d'une sécurité communautaire, notamment en matière de coopération pénale transfrontalière. D'autre part, une

---

[21] Michel Foucault, « Surveiller et punir, naissance de la prison », 1975, Ed. Gallimard, p. 70.
[22] Agence des droits fondamentaux de l'UE et Conseil de l'Europe, Manuel de droit européen en matière de protection des données, Avril 2018, pp. 20-24.
[23] Adrien Basdevant, Jean-Pierre Mignard, op. cit., p.22.

nécessité de protéger les **données à caractère personnel** dans la justice pénale, domaine réservé à la souveraineté des Etats membres « dont le droit de punir est l'expression par excellence »[24].

Il conviendra de se concentrer sur la communion de ces trois intérêts, à savoir la volonté d'innover par le **recours à l'IA** et d'accroître l'efficacité de **la justice pénale** dans un environnement où les notions de sécurité et de dangerosité permettent l'acceptation de déployer des ressources y compris reposant sur l'ingérence à la **protection des données personnelles**.

Dans quelle mesure le traitement des données par des dispositifs d'IA au sein de la justice pénale constitue un risque pour les droits fondamentaux européens de protection des données à caractère personnel des individus, sujets de mesures automatisées aux fins de prévention et de répression pénales ? Quelles sont les limites du cadre normatif européen consacré aux données personnelles en matière pénale et comment les nouveaux textes anticipent-ils les enjeux de cette matière amplifiés par le recours à l'IA ?

Cette étude sera divisée en trois temps. Dans un premier temps, il s'agira de comprendre la place qu'occupent aujourd'hui les dispositifs d'IA au sein de la justice pénale européenne. La réflexion s'appuiera sur des situations rencontrées en France principalement. Une étude préliminaire sera consacrée à l'évolution de la place des données et de leur traitement en matière pénale. L'attention sera ensuite portée sur des cas d'utilisation de dispositifs d'IA par les autorités françaises de prévention et de répression des infractions pénales (**Partie I**).

Cette analyse permettra d'appréhender dans un deuxième temps les risques de l'utilisation de ces dispositifs portant sur le droit à la protection des données personnelles des individus sujets de ces mesures. En effet, il s'agira d'étudier les risques portant sur ce droit simultanément aux étapes du traitement des données personnelles. A savoir, la collecte, l'enregistrement, l'exploitation, la conservation, la publication et le transfert transfrontière de ces données personnelles à des fins pénales (**Partie II**).

Dans un troisième temps, il conviendra d'étudier le cadre normatif européen consacré aux données personnelles en matière pénale, afin d'en considérer les limites. Cette analyse permettra de comprendre comment les nouveaux textes anticipent-ils les enjeux portant sur la protection des données personnelles, liés notamment à l'introduction des dispositifs d'IA en matière pénale. En fin d'étude, une approche de droit comparé permettra d'appréhender les différences potentielles entre les Etats membres et non-membres de l'Union Européenne (UE) des parties au Conseil de l'Europe. (**Partie III**).

---

[24] Cahiers du Conseil constitutionnel n° 26 (Dossier : La Constitution et le droit pénal), Août 2009.

Partie I : L'intelligence artificielle en matière de prévention et de répression des infractions pénales

De manière générale, l'assistance des autorités pénales par l'Intelligence artificielle, renvoie notre pensée au modèle américain et ses outils « investis de manière assez décomplexée »[25]. En Europe, il s'agit d'un sujet en effervescence faisant l'objet de plusieurs textes, projets de textes, groupes de travail ou commissions. Le terme de justice pénale renvoi à la prévention des infractions et à la répression pénale lors du procès. Il sera également nécessaire d'étudier certains aspects de la prévention des infractions à la lumière du maintien de l'ordre public et de la sécurité publique, relevant de la police administrative et non judiciaire. Les missions de police administratives et judiciaires sont dans certaines situations liées, en ce que « le clivage entre la prévention et la répression, encore souvent avancé par les auteurs, ne permet pas en effet d'en saisir toute la complexité »[26]. Par ailleurs, « le critère finaliste, fondé sur la commission d'une infraction, semble de son côté quelque peu dépassé, à l'aune notamment des évolutions législatives récentes qui octroient des moyens considérables à la police de l'ordre public, qui se rapprochent de ceux utilisés par la police judiciaire »[27].

En France, à la suite des attentats ayant eu lieu à Paris en 2015, la question de la nécessité d'une meilleure surveillance publique est ravivée et de celle-ci émanent des discours dirigés vers l'idée de renforcer la sécurité en modernisant l'action des forces de l'ordre, notamment durant la campagne présidentielle de 2017. Il s'agit de comprendre quelles formes prend l'utilisation de l'IA en matière prévention et de répression des infractions pénales. Au sein d'une part, des autorités administratives et judiciaires lors de la prévention des infractions pénales et de la résolution d'enquêtes (Titre 1). D'autre part, il conviendra d'étudier le procès pénal assisté par des dispositifs d'IA (Titre 2).

[25] Charte éthique de la CEPEJ, p. 17.
[26] Présentation du colloque « La distinction entre polices administrative et judiciaire a-t-elle encore un sens ?», Université de Tours, 19 octobre 2018.
[27] Ibid.

Titre I : Le recours à l'IA pour la prévention des infractions et de la résolution d'enquêtes

Ce titre est consacré à la façon dont a progressivement été intégrée l'IA au sein de la prévention des infractions mais également, lors de la résolution d'enquêtes. Au cours de l'Histoire de la prévention des infractions et résolution d'enquêtes, le traitement des données a eu tendance à s'automatiser, voire à s'effectuer via des dispositifs intelligents. Il convient dans un premier temps, de traiter du contexte antérieur à cette automatisation du traitement, afin de comprendre quels besoins ont fait surface dans un contexte où le big data s'est rapidement installé et si l'IA répond à ces besoins (Chapitre 1).

Dans l'optique de mieux appréhender le déploiement de l'IA au sein de la prévention des infractions, il est intéressant de se pencher sur le fonctionnement de deux cas concrets présents en France et en Europe. Dans un second temps, les dispositifs utilisés dans le cadre de la prévention des infractions et de la résolution d'enquête sera étudié (Chapitre 2). Dans un troisième temps, il s'agira de réfléchir à la reconnaissance faciale, inscrite dans l'objectif de mieux surveiller pour protéger et prévenir les infractions pénales (Chapitre 3). Nous étudierons les besoins auxquels ils doivent répondre ainsi que les apports de ces dispositifs à la matière pénale.

Chapitre 1 : L'utilité de l'IA pour le traitement des données

Le but de ce chapitre est de déterminer le contexte dans lequel l'IA s'est développée en matière pénale. Il conviendra de délimiter l'approche historique du traitement des données en matière pénale, principalement par l'étude du traitement des données en matière d'enquête et de prévention des infractions, sans oublier que la phase de la poursuite est également concernée, du fait de l'utilisation probatoire du fruit dudit traitement. Le maniement des données est inhérent à la prévention des infractions. Il s'agit de comprendre comment le traitement des données a progressivement vu sa place gagner en importance dans ce domaine (Section 1), afin de démontrer comment la prévention des infractions par l'automatisation du traitement des données est devenue incontournable, jusqu'à observer le déploiement de l'IA, notamment au sein des forces de police et de gendarmerie (Section 2).

Section 1 : L'historique du traitement des données en matière de prévention des infractions pénales

Il convient de comprendre dans quelle mesure le traitement des données a progressivement obtenu une place importante au sein de la matière pénale. Il est incontestable que le traitement des données, dès ses prémices, a vu sa définition et sa signification évoluer, par la transformation même du rôle du traitement des données (§1). La définition actuelle du traitement des données est vaste (§2) et se veut être applicable à toute sorte de traitement des données.

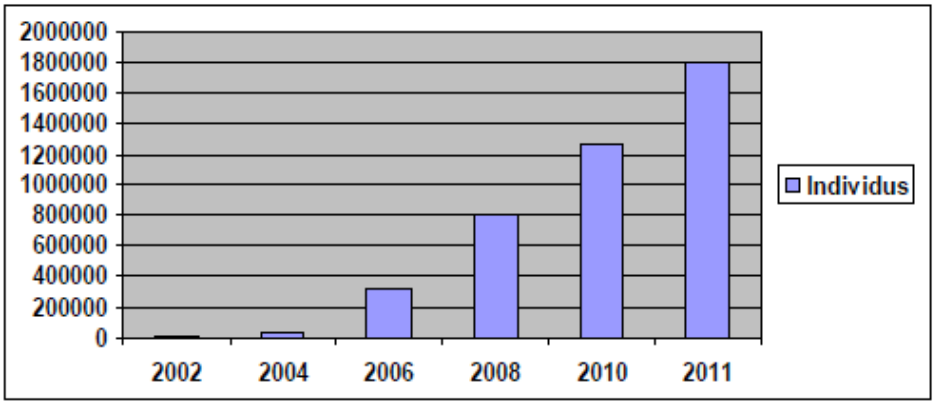
§1. L'évolution de la place du traitement des données

En 1893, par la création du Service d'identité judiciaire, on observe une volonté de mise en commun d'un ensemble de données recueillies par la police, afin qu'elles soient accessibles et utilisables sur l'ensemble du territoire, et non uniquement par la capitale. C'est un phénomène de transfert des données de manière à les décentraliser. Une fois les données rassemblées à l'échelle nationale par les dispositifs policiers, le traitement des données s'étend à un autre genre de prévention des infractions liée à la sécurité : la prévention des comportements pouvant nuire à l'Etat, notamment en période de guerre. Le traitement des données devient progressivement au centre de l'action de sécurité publique. Cette dernière varie en fonction du contexte politique mais aussi géopolitique de l'Etat. C'est le cas en temps de guerre ou d'instabilité politique. A titre d'exemple, durant la première guerre mondiale, un fichier est créé afin de regrouper les données concernant les suspects d'espionnage. D'autre part en 1933, un fichier, appelé la machine de Hollerith, est créé, afin de recenser les individus de confession juive, alors qu'un tel traitement des données s'éloigne du but principal de prévention des infractions pénales.

Il s'agit toujours de l'optique de création de dispositifs afin de structurer au mieux les données récoltées par les forces de police dans un but premier de sécurité publique et de prévention des infractions. Grossièrement dit, **les dispositifs sont créés au service de la donnée, dans un but de préservation de l'ordre public**. Il est important de nuancer ce propos, par une exception qui viendrait confirmer la règle. La donnée aurait été dans certains cas créée pour satisfaire l'utilisation des dispositifs de classement des données à des fins d'enquête et de prévention des infractions. En période de colonisation de territoires africains notamment, les populations indigènes ne possédaient pas d'état civil à proprement parler. Il a ainsi été question de leur attribuer une identification civile, afin d'utiliser les dispositifs de recensement par les forces de l'ordre, et de mieux prévenir et identifier les individus faisant l'objet d'une surveillance particulière pour trouble à l'ordre public et plus

particulièrement, à la stabilité de l'Etat français[28]. Au début des années 1990 cependant, une vague technologique apparaît avec le développement d'objets technologiques en tout genre (Internet, téléphone portable, biométrie, etc.), et vient bouleverser la façon dont sont appréhendés les contrôles. La création de fichiers mis en place pour prévenir la production d'infractions s'accélère depuis 1987, par la mise en place du fichier automatisé des empreintes digitales, en 1998 pour les empreintes génétiques[29]. **La donnée serait-elle alors de plus en plus au service de ces nouveaux dispositifs, en matière de prévention des infractions ?**

Une chose est certaine, comme le souligne Alex Türk, ancien président de la CNIL, lors de la conférence internationale des commissaires à la protection des données de Londres en 2006, les données et ces dispositifs de plus en plus à jour sont conjugués par l'avènement d'une « vague sécuritaire »[30], de laquelle émane une floraison de fichiers et d'outils d'investigation dans les systèmes d'information au profit des autorités de police. Cela s'explique également par une réaction aux attentats contre les Etats-Unis en 2001, soit cinq ans plus tôt. Ce recueil massif de données a pour but de mieux surveiller, classer les individus, afin d'éviter que ce genre d'évènements se reproduise. Le nombre de fichiers mis au profit des autorités de police ne cesse d'augmenter. Par ailleurs, le nombre d'individus fichés augmente de façon également considérable. A titre indicatif, « l'accroissement très important du fichier des empreintes génétiques (FNAEG), qui est passé de 806 356 profils génétiques en 2008 à 1,79 million en novembre 2011, est particulièrement révélateur de cette tendance de fond. Le fichier des empreintes digitales (FAED), qui comportait moins de trois millions d'empreintes fin 2008, en comptait 4,06 millions au 1er novembre 2011 »[31]. Ci-après l'évolution du nombre d'individus enregistrés au sein du fichier FNAEG[32] :



[28] Pierre PIAZZA, « Alphonse Bertillon et l'identification des personnes (1880-1914) », 2018.
[29] Yanis ZOUBEIDI-DEFERT, « Fichier ELOI : Suite et fin », note sous Conseil d'État, 30 décembre 2009, *Association SOS Racisme – Groupe d'information et de soutien aux immigrés et autres*, Req. n^{os} 312051-313760.
[30] Alex Türk, Conférence internationale des commissaires à la protection des données de Londres, CNIL, Rapport d'activités 2006, Paris, La Documentation française, 2007, p. 89.
[31] Rapport d'information déposé à l'Assemblée Nationale par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police, par les députés Mme Delphine BATHO et M. Jacques Alain BENISTI, le 21 décembre 2011, p. 10.
[32] Ibid., p. 11.

L'accumulation de ces fichiers participent à l'avènement d'un phénomène pouvant être qualifié de « données massives », traduction littérale du terme « big data », dont il sera question dans les développements suivants. Ainsi, la matière pénale n'a pas échappé à cette vague technologique permettant aux autorités de police de mieux envisager la prévention des infractions pénales. Cependant, parallèlement à cette effervescence technologique, se développe concurremment une atmosphère sécuritaire, dans laquelle la donnée est la matière première de la surveillance.

§2. La définition vaste du traitement des données

Le traitement des données n'est pas une technique récente, puisqu'il permet par exemple depuis la Rome antique d'effectuer le recensement de la population pour prendre des décisions politiques, en anticipant le nombre de soldats qu'il y aurait dans l'armée[33]. En matière pénale, le traitement des données est intrinsèquement lié à la prévention des infractions et dans le cadre du rassemblement de preuves ou d'identification de personnes suspectes. Il existe depuis bien avant le développement de notre société d'information, dans laquelle les technologies de l'information et de communication jouent un rôle considérable.

Aujourd'hui, on parle principalement de traitement automatisé des données, notamment dès 1981 par la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, qui emploie ce terme moderne pour l'époque, dans le but d'anticiper les techniques à venir, afin que le texte reste à jour le plus longtemps possible. Le traitement automatisé est alors défini comme : *« Des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion »*[34].

En matière de prévention des infractions et de poursuite pénale, tout traitement des données n'est pas automatisé. Comme le reprend la définition du terme traitement à l'article 3.2 de la directive UE 2016/680[35], que l'on citera « Directive Police-Justice », disposition européenne dédiée à la protection des données à caractère personnel traitées en matière de prévention et de détection d'infractions pénales, d'enquête ou de poursuite en la matière : *« Aux fins de la présente directive, on entend par: « traitement », toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés*

---

33 Adrien Basdevant, « Les données, la nouvelle ingénierie du pouvoir, quelles conséquences pour l'Etat de droit ? », conférence IA and Law Breakfasts, Conseil de l'Europe, 2 décembre 2019.

34 Article 2.c. de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, 28 janvier 1981.

35 Directive (UE) 2016/680, dite « Directive police-justice », du parlement européen et du conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

La définition du traitement des données reste large dans la majorité des dispositions nationales et européennes lui étant consacrées. Il n'est pas rare d'observer dans ces définitions une liste de tout type de processus dont les données peuvent faire l'objet. L'ensemble de ces techniques répondent à l'étendue du traitement des données telle qu'elle est représentée en matière pénale aujourd'hui. Notamment via la communication, la transmission, la diffusion et l'interconnexion des données, techniques inhérentes aux évolutions de la société de l'information et automatisée. Les techniques ont évolué et la liste présente au sein de la définition s'est agrandie, en fonction de la place même que possédaient les données dans l'automatisation du traitement.

Il s'agit de revenir sur la place que les données pouvaient posséder au sein de la matière pénale, aux prémices de leur traitement. Les données n'étant que de pures informations dépourvues de sens si elles ne sont pas traitées, il s'agit par leur interconnexion d'en tirer une idée afin de pouvoir s'en servir en matière d'enquête notamment.

A titre d'exemple, au XIXe siècle, Alphonse Bertillon, célèbre anthropologue criminel français, participe à une révolution bureaucratique en matière de traitement des données dans le cadre d'enquêtes judiciaires. Il précise la collecte et la structuration des données d'identification des suspects inscrits dans les fichiers de police. Avant son arrivée au sein de la préfecture de police de Paris, les données relatives à la taille des individus étaient divisées en neuf mesures, elles-mêmes réparties en trois parties : petit, moyen et grand. Il décide alors d'entrer la taille exacte du suspect afin de pouvoir l'identifier. En précisant la saisie, le classement et la structuration des données, un accroissement de l'efficacité des enquêtes de police est observé. Cette technique remporte un franc succès lorsqu'un récidiviste recherché est pris en flagrant délit durant un cambriolage puis identifié. Trahi par sa taille, il avoue son identité.

La mesure de sa taille, comme plusieurs données d'identification avaient été recueillies et enregistrées, comme pour l'ensemble des individus déjà arrêtés et écroués, au sein des institutions policières, judiciaires et carcérales. D'un point de vue historique, l'objectif de lire les données de façon toujours plus claire se poursuit encore aujourd'hui.

Ainsi, la définition du traitement des données a évolué pour devenir de plus en plus large, du point de vue de l'évolution historique des processus de traitement ayant existé. En effet, l'importance de la

donnée a rendu considérable l'objectif de pouvoir mieux la lire. Il convient de comprendre comment l'automatisation du traitement des données est devenue incontournable pour la prévention des infractions, jusqu'à observer le déploiement de l'IA au sein des forces de police et de gendarmerie.

Section 2 : L'automatisation du traitement des données et l'avènement de l'IA

« L'algorithme, l'IA aide à appréhender une infinité qui dépasse l'Homme, algorithme sur lequel on peut avoir une emprise »[36]. L'IA est devenue un outil indispensable dans tous les domaines, et le droit n'y a pas échappé (§1). En effet, l'IA en droit est un sujet phare depuis 2015[37]. Alors que sa régulation fait constamment débat depuis son introduction en la matière, elle est de plus en plus utilisée. Il convient de comprendre dans quel contexte l'IA s'est introduite en matière de prévention des infractions (§2).

§1. L'avènement de l'IA en matière juridique

Il convient de poser préliminairement les caractéristiques composant l'IA afin de comprendre comment elle peut être utilisée par tout corps de la justice pénale. Plusieurs étapes lors de la conception d'un dispositif d'intelligence artificielle sont à prendre en compte. D'abord, l'entrée de données, puis, l'intervention algorithmique aussi appelée phase d'apprentissage, suivie d'une phase de fonctionnement autonome appelée « l'auto-apprentissage », enfin, la phase finale, consistant à obtenir le résultat souhaité après plusieurs entraînements.

En tant qu'outil permettant le traitement automatisé et intelligent des données, l'IA représente une avancée en matière technologique. Cependant, il ne s'agit pas d'un phénomène nouveau. Au vu de l'étude historique ci-dessus, il s'agit de la répétition de l'Histoire. En reprenant la comparaison établie par Antoine Garapon, l'IA est assimilable à la « machine à vapeur [ayant] révolutionné l'industrie et tous les secteurs »[38]. Afin de comprendre dans quelle mesure l'IA a pris racine au sein du traitement des données en matière de prévention des infractions, il convient d'appréhender son rapport au concept de Big Data, mentionné précédemment comme un phénomène de « données massives ».

Il est important de poser une distinction primordiale au sujet de la définition du terme Big data. Au cours de l'étude du sujet, s'est posée la question de savoir quel concept de l'IA ou du big data s'est développé en premier afin que l'autre en découle. L'IA a-t-elle été introduite en droit pénal, à la suite d'un phénomène de big data ? Ou bien, le concept de big data a-t-il été créé dans un but de répondre au besoin créé par les startups développant de nouveaux dispositifs d'IA ? Les deux hypothèses sont

---

[36] Adrien Basdevant, « Les données, la nouvelle ingénierie du pouvoir, quelles conséquences pour l'Etat de droit ? », conférence IA and Law Breakfasts, Conseil de l'Europe, 2 décembre 2019.

[37] Intelligence artificielle et enjeux juridiques, par Antoine Chéron, avocat, Village de la Justice, 3 avril 2018.

[38] Interview d'Antoine Garapon, « le numérique est un remède à la lenteur de la justice », Dalloz actualité.

vraies car la confusion provient des définitions formelles et informelles du big data. En effet, la réponse dépend de la définition du terme big data que l'on choisit.

Selon le Conseil de l'Europe, via le Comité Consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, le big data est définit comme : « *La capacité technologique croissante de collecter, traiter et extraire très rapidement des connaissances nouvelles et prédictives à partir d'un gros volume, d'une grande variété de données et à une vélocité considérable. Sous l'angle de la protection des données, les principaux problèmes ne viennent pas uniquement du volume, de la variété des données traitées et de la vitesse du processus, mais également de l'analyse de ces données au moyen d'un logiciel dans le but d'extraire des connaissances prédictives de nature à orienter un processus décisionnel à l'égard de personnes ou de groupes. Aux fins des présentes lignes directrices, la définition des mégadonnées englobe donc à la fois les données elles-mêmes et le procédé analytique* »[39].

Cette définition est également reprise par la Commission Européenne pour l'Efficacité de la Justice (CEPEJ), au sein de sa charte éthique rédigée en 2018. De ce point de vue, le phénomène de big data, en tant que technique de traitement des données, est créé après l'IA. En revanche, selon la CNIL et par pure traduction de l'anglais, le big data signifie « données massives »[40], ainsi, l'IA est créée après le phénomène de big data, en tant qu'accumulation d'informations, en réponse à l'obsolescence des anciens dispositifs de traitement des données non massives. Au sein de cette étude, il conviendra de comprendre le terme *big data*, au sens de la définition de la CEPEJ, comme la capacité à traiter une masse de données.

§2. L'utilisation de l'IA en matière de prévention des infractions pénales

En matière de prévention des infractions, comme il a été étudié, le besoin d'effectivité de la lecture des données est ravivé par l'apparition de chaque nouvelle technique de traitement de l'information, comme l'apparition de la photographie en 1874, ou celle de la saisie des empreintes digitales dans les fichiers de police en 1902. En revanche dans certains cas, l'outil lui-même devient un besoin, afin de lire les données. Par exemple, en 1882, les fichiers de police, en lacune de précision, nécessitaient l'utilisation de nouveaux objets pour l'époque, comme le compas ou les échelles graduées, etc.

« La décennie 2000-2010 a joué un rôle crucial dans le développement, la démocratisation et l'acceptation des technologies »[41]. Depuis 2008, plusieurs projets de fichiers de police sont assistés

---

[39] Définition du terme big data par la CEPEJ, Charte éthique de la CEPEJ, p.20.
[40] Définition du terme big data par la CNIL, https://www.cnil.fr/fr/definition/big-data.
[41] Sandra Bertin, directrice de la police municipale de Nice, interviewé dans le cadre de ce mémoire. L'interview est disponible en annexe.

par des dispositifs informatiques, c'est-à-dire, des algorithmes. C'est le cas du dispositif de lecture automatisé des plaques d'immatriculation (LAPI) utile matière de recherche de véhicules volés, suspects ou signalés. Le dispositif prend la forme de caméras, permettant de « lire automatiquement la plaque d'immatriculation des véhicules ; comparer ces données au Fichier des véhicules volés (FVV) et au Système d'information Schengen ; prendre la photographie des occupants des véhicules »[42]. Il a été utilisé dans le cadre d'une expérimentation de deux ans de 2009 à 2011. En revanche, la CNIL avant d'avoir accepté cette expérience à pu exprimer ses réticences au projet de loi quant aux risques pour les libertés individuelles. La CNIL a regretté qu' « aucune étude d'impact n'ai été présentée à l'appui du projet de loi ni d'élément concret à l'appui de ces dispositions bien que l'exposé des motifs du projet de loi fasse état des « enseignements opérationnels recueillis après les attentats les plus récents » pour justifier l'adoption de nouveaux instruments juridiques, et mentionne, en présentant l'article 4, « des systèmes de nature équivalente (…) mis en place dans d'autres pays européens, comme la Grande-Bretagne qui dispose d'une expérience incontestable en ce domaine et qui a montré l'utilité d'un tel dispositif »[43]. Le projet LAPI a pris aujourd'hui une autre tournure, et est désormais utilisé aujourd'hui en matière de sécurité et infraction routières.

Le phénomène de l'accumulation des données, notamment en matière de fichiers de police a été traité précédemment. En raison de ce phénomène, le traitement des données en matière de prévention des infractions témoigne d'un besoin d'automatisation et d'effectivité. En 2018, un rapport parlementaire souligne qu'« il faut désormais développer l'analyse massive des données pour détecter plus largement les comportements irréguliers. En effet, les traces collectées pourraient être davantage exploitées grâce à la puissance de calcul, au recours aux algorithmes et à la collecte de données de masse »[44]. Un constat positif en a été tiré, puisqu'après les travaux effectués par le service des technologies et des systèmes d'information de la sécurité intérieure[45], une alimentation automatique des fichiers depuis les logiciels de rédaction de procédure de la gendarmerie et de la police nationales a vu le jour.

Des moyens nouveaux inspirés des modèles américains sont peu à peu introduits en Europe. C'est le cas des dispositifs utilisés dans le cadre de cartographie interactive pour la prévention des infractions et la résolution d'enquêtes. Il convient d'étudier les cas présents en France.

---

[42] Décrit par le site internet afs2r, https://www.afs2r.fr/glossaire/vehicule-lapi.
[43] CNIL, Délibération n°2005-208 portant avis sur le projet de loi relatif à la lutte contre le terrorisme.
[44] Rapport d'information déposé devant l'Assemblée Nationale française par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, M. Didier PARIS et M. Pierre MOREL-À-L'HUISSIER, p. 18.
[45] Créé par l'arrêté du 27 août 2010 modifiant l'arrêté du 23 décembre 2009 portant organisation de la direction générale de la gendarmerie nationale (NOR: IOCJ1020161A).

Chapitre 2 : Le recours à l'IA pour la prévention des infractions et la résolution d'enquêtes

L'automatisation de procédés est présente en matière de prévention des infractions et la résolution d'enquête par les autorités de police et de gendarmerie. Il s'agit dans ce chapitre de prendre l'exemple de la police prédictive en matière de prévention des infractions. Elle est d'ores-et-déjà présente aux Etats-Unis (EU). En Europe, notamment au Royaume-Uni, nous observons l'avènement d'outils au profit de la police tels que la prédiction géographique des infractions, dont il sera question dans notre étude. Le recours à l'IA intervient également après commission d'infractions. Ce fut le cas, au sein de la tristement célèbre affaire « Gregory » en France. Ainsi, il convient au sein de ce chapitre d'appréhender le concept de d'automatisation de procédés au profit des forces de police et de gendarmerie et d'en étudier les cas concrets présents en France. Premièrement en analysant le fonctionnement de la police prédictive, notamment dans le cadre de la prédiction géographique des infractions, le « crime mapping », par les services de police et de gendarmerie (Section 1), c'est-à-dire, afin de s'intéresser aux endroits propices à la réalisation de l'infraction. Dans un second temps, il s'agira de s'intéresser à la résolution des enquêtes, après commission d'infractions (Section 2).

Section 1 : L'identification des zones prioritaires à surveiller en matière de police prédictive : le « crime mapping »

Le terme police prédictive est défini comme étant un outil à la disposition des autorités de police et de gendarmerie. Cet outil utilise des « nouvelles formes de quantification afin de lire une quantité massive de données et en extraire de l'information »[46]. Il a pour but, une meilleure appréhension de la répartition géographiques des infractions, afin de les anticiper et de prioriser des zones à patrouiller. Ainsi, le sens de l'adjectif « prédictive » ne peut être celui selon lequel la police peut instantanément détecter des lieux dans lesquels une infraction est susceptible de se produire. Il s'agirait plutôt de l'utilisation de ces outils afin que les officiers de police soient informés des secteurs à contrôler en priorité. Il s'agit du crime mapping. Il convient dans une première partie de comprendre la définition et la provenance de ce concept (§1), afin d'en étudier des cas concrets en France (§2).

§1. La définition et la provenance du concept de « crime mapping »

En France, le terme de police prédictive est un terme revenant souvent en matière de sécurité du territoire, depuis la survenance d'attentats terroristes. C'est un enjeu de plus en plus présent au sein du discours politique français, corrélé à un besoin de modernité au sein des forces de sécurité

[46] Marine Kettani, « *Predictive policing and Rule of technology* », Webinaire IA and Law Breakfasts, organisé par le Conseil de l'Europe, le 02.07.2020.

françaises. Le président Emmanuel Macron, lors de sa campagne présidentielle de 2017, l'a plusieurs fois rappelé : « Seul un modèle de police renouvelé, proche du terrain et présent partout sur le territoire, permettra de réduire la délinquance et d'améliorer les relations avec la population »[47]. Le terme d'IA n'est pas employé dans le contexte policier. En 2018, une fois élu président, Emmanuel Macron entame une véritable politique d'innovation technologique par l'utilisation de l'IA. Au sein d'un discours consacré à l'IA[48], ni la matière policière ni la justice pénale de manière globale ne sont évoquées. Est-ce un choix stratégique que de vouloir l'occulter dans les discours publics pour mieux l'appliquer en pratique ?

A la différence des discours, l'IA en tant que gage de modernité, a en pratique été rapidement intégrée en matière de prévention des infractions. Il fleurit ainsi en France, dans des régions anciennement touchées par ce type d'évènements meurtriers, des dispositifs d'IA au profit des autorités de police afin de mieux surveiller la population, notamment lors de rassemblements publics. Fin 2016, à Marseille par exemple, naît le concept de « Big data de la tranquillité publique ». Il s'agit d'une collecte et interconnexion de sources informatiques au profit des agents de police municipale. Notamment en suivant le mouvement de modernisation des forces de police ci-dessus mentionné, par un renforcement des effectifs ou encore le déploiement des dispositifs de vidéosurveillance. La ville met à l'honneur l'aspect prédictif du projet afin de prévenir les infractions, en expliquant qu'il s'agit : « de recueillir, auprès de partenaires institutionnels du territoire, des données précieuses pour essayer de prévenir certains événements avant qu'ils ne se produisent »[49].

Il est nécessaire d'appréhender le concept de police prédictive qui parfois peut faire l'objet d'un abus de langage, car il n'est pas encore possible de connaître, par exemple, l'adresse exacte du vol de voiture qui se produira demain, dans telle ville et à tel moment, comme l'explique le colonel Laurent Collorig[50], au sein d'une étude réalisée en Île-de-France. La police prédictive est une utilisation algorithmique antérieure et postérieure à la commission de l'infraction.

Le « crime mapping » aussi appelé, cartographie de la criminalité n'est pas récent en tant que tel. Il se développe en effet aux Etats-Unis au milieu du XIXe siècle. La première ville à s'en servir est Chicago, dans laquelle les policiers sont informés de manière instantanée des données de prédiction. Ensuite, entre les années 1900 et 2000, le processus s'automatise.

---

[47] Campagne présidentielle d'Emmanuel Macron 2017, programme de sécurité, https://en-marche.fr/emmanuel-macron/le-programme/securite. Passage souligné par mes soins.
[48] Discours du Président de la République Emmanuel Macron #Aiforhumanity, 29 mars 2018.
[49] Ville de Masreille, « Le Big data de la tranquillité publique ».
[50] Camille Gosselin, « La police prédictive – enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique », Institut d'Aménagement et d'urbanisme d'Ile de France, Avril 2019 p. 21.

En Europe, il se développe au Royaume-Uni depuis 2004. Il s'agit de l'utilisation de données propres aux infractions passées, comme la nature de l'infraction, la date et l'heure ainsi que leur localisation. En rendant ces infractions passées traçables, les officiers peuvent prioriser leur lieu d'action. Naturellement, les officiers connaissent déjà les « points chauds » de leurs secteurs attribués, cependant, en utilisant un algorithme de « crime mapping », la détermination de cette future infraction est plus précise, l'outil se concentrant de façon plus précise sur les infractions ayant eu lieu les deux à trois jours précédents et se met à jour automatiquement toutes les 12 à 24 heures. Selon le Royal United Services Institutes (RUSI), les algorithmes de « crime mapping » seraient dix fois plus performants pour prédire la nature de la prochaine infraction, et deux fois plus efficaces pour en prédire la situation géographique[51].

Ici, les opinions peuvent diverger. Monsieur le Professeur Ronald Leenes[52] par exemple, souligne la difficulté à lire les données et ainsi explique que pour certaines tâches, l'algorithme n'est pas plus performant qu'un humain « plus lent ». Par ailleurs, comme a pu l'expliquer le colonel Collorig, le terme « prédictive » renvoie à une obligation de résultat, qui viendrait contraindre le travail.[53] Les mots de Jan Kleijssen, président de la direction de la société de l'information et de l'action contre la criminalité, au conseil de l'Europe, vont en ce sens. Il rappelle que « predicting », au sens de prévision, ne doit pas être confondu par « prescribing », au sens de recommandation, prédire.[54] Ainsi, pour une plus ample compréhension de ce genre d'outils, il convient de s'intéresser à leur fonctionnement.

§2. Le fonctionnement technique du crime mapping en France

Cette technique prend la forme d'un logiciel cartographique mis à la disposition des autorités de police, accessible depuis un ordinateur ou une tablette. Le crime mapping possède les caractéristiques propres à ceux de l'IA. Les données entrées au sein de l'algorithme prennent leur source dans les dépôts de plaintes de la police (LRPPN) et de la gendarmerie (LRPGN), les bases de données policières mais aussi, les réseaux sociaux. En effet, comme l'indique un colonel, commandant de groupement du Nord de la France, les réseaux sociaux possèdent parfois des précisions plus à jour que celles présentes au sein des fichiers des services de l'Etat[55].

---

51 « Algorithms in the Criminal Justice System », The Law Society, Juin 2019, p. 33.

52 Professeur Ronald Leenes, professeur de régulation par la technologie à l'Université de Tilburg (Pays-Bas). Session parlementaire européenne du 20.02.2020 sur « L'intelligence artificielle au sein de la justice pénale et son utilisation par la police et les autorités judiciaires en matière pénale ».

53 « 22 v'là la police prédictive ! », par Antoine Beauchamp, France culture, le 05 décembre 2018.

54 Jan Kleijssen, « *Predictive policing and Rule of technology* », Webinaire IA and Law Breakfasts, organisé par le Conseil de l'Europe, le 02.07.2020.

55 Camille Gosselin, « La police prédictive – enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique », Institut d'Aménagement et d'urbanisme d'Ile de France, Avril 2019, p. 27.

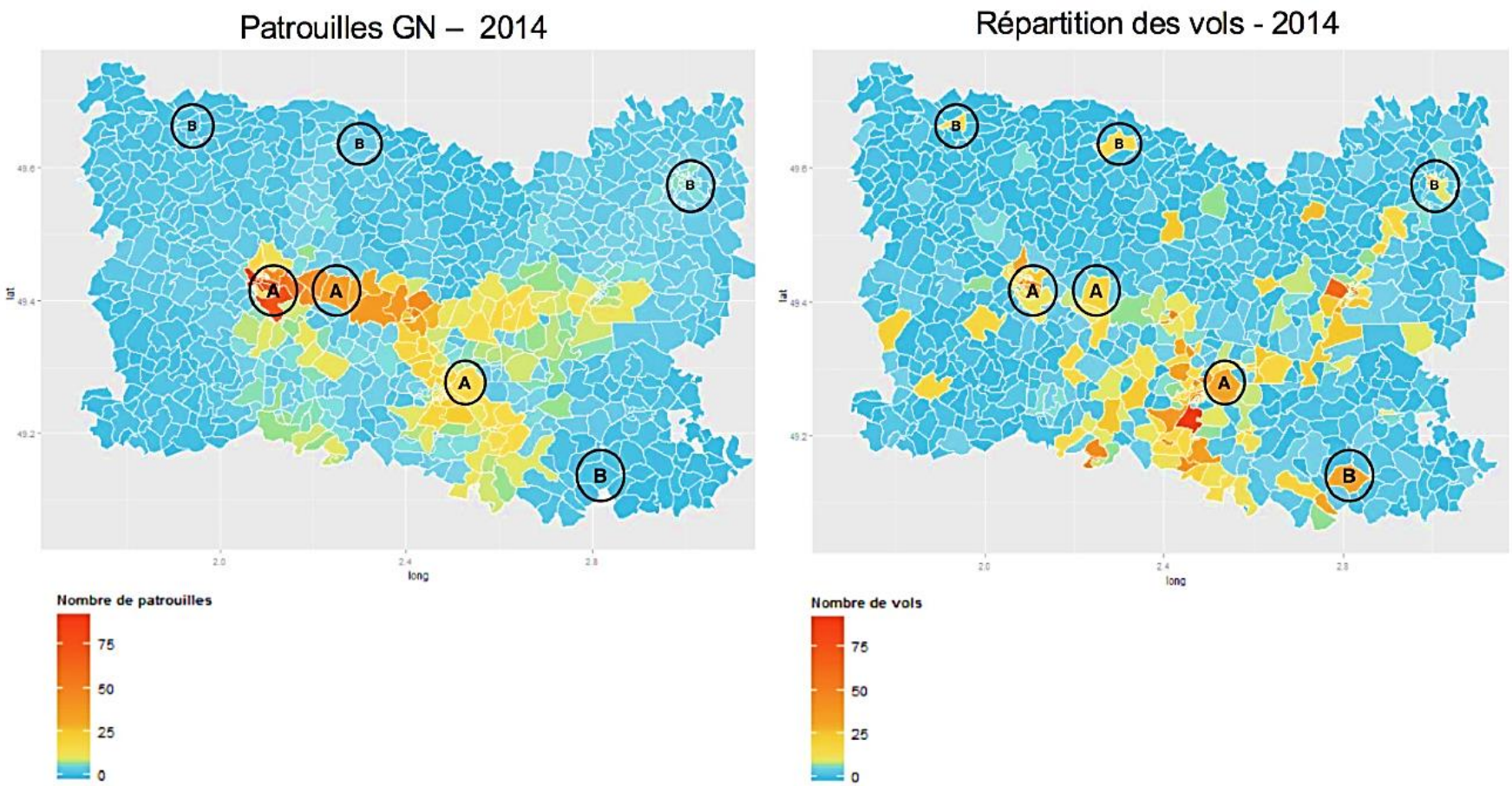
On y trouve des informations relatives aux lieux de commission de précédentes infractions, catégorisés par la date, la nature et l'heure de l'infraction. Des variables socio-démographiques (taux de chômage, scolarisation des jeunes, nombre de commerces de proximité, âges moyens des habitants, etc.) et des indicateurs concernant les circonstances temporelles d'infractions (météo, fréquence des vols, etc.), sont également prises en compte. Il est nécessaire de déduire une information de ces données. Ces facteurs socio-temporels participent à l'appréhension de la production d'infractions.

Une fois les données entrées au sein de l'algorithme, la phase d'entraînement débute. Une équipe de développeurs entraîne l'IA à distinguer les informations, puis à les classer, à la manière du Machine Learning. Par exemple, distinguer les informations « patrouilles » et « infractions ». Il s'agit d'un système supervisé par étiquetage de l'information au départ, afin d'aider l'algorithme à devenir autonome, dans le but de passer d'une donnée brute, comme le nom d'une rue, à une information utile. L'IA transforme ensuite ses informations en modèles, c'est-à-dire, en la représentation mathématique d'un problème donné. Notamment, comprendre et déterminer les zones de patrouilles et les comparer avec les zones d'infractions.

A la suite de cette phase d'entraînement, l'IA devient auto-apprenante. Des données sont massivement traitées par l'algorithme qui va au fur et à mesure de son fonctionnement devenir plus autonome et va anticiper les lieux et natures des infractions. A ce raisonnement autonome s'ajoutent des mises à jour de données de nature différente et de précision plus importante, telles que les circonstances temporelles, que l'IA va transformer en informations et les conjuguer à des informations similaires. Ce processus reste supervisé pour que l'IA ne relie pas des informations n'ayant aucun lien, cela nuirait à l'efficacité et à la qualité du résultat. En matière de crime mapping, le résultat issu de l'algorithme prend la forme de la détermination cartographique des zones à patrouiller en priorité en fonction des données comparées.

Ci-après, la comparaison des zones d'infractions patrouillées (A), et des zones d'infractions non ou peu patrouillées (B) par la gendarmerie du département de l'Oise.[56] Cette démonstration, dépeint la nécessité de mieux répartir les patrouilles pour une meilleure prévention.

[56] Ibid., p.16.



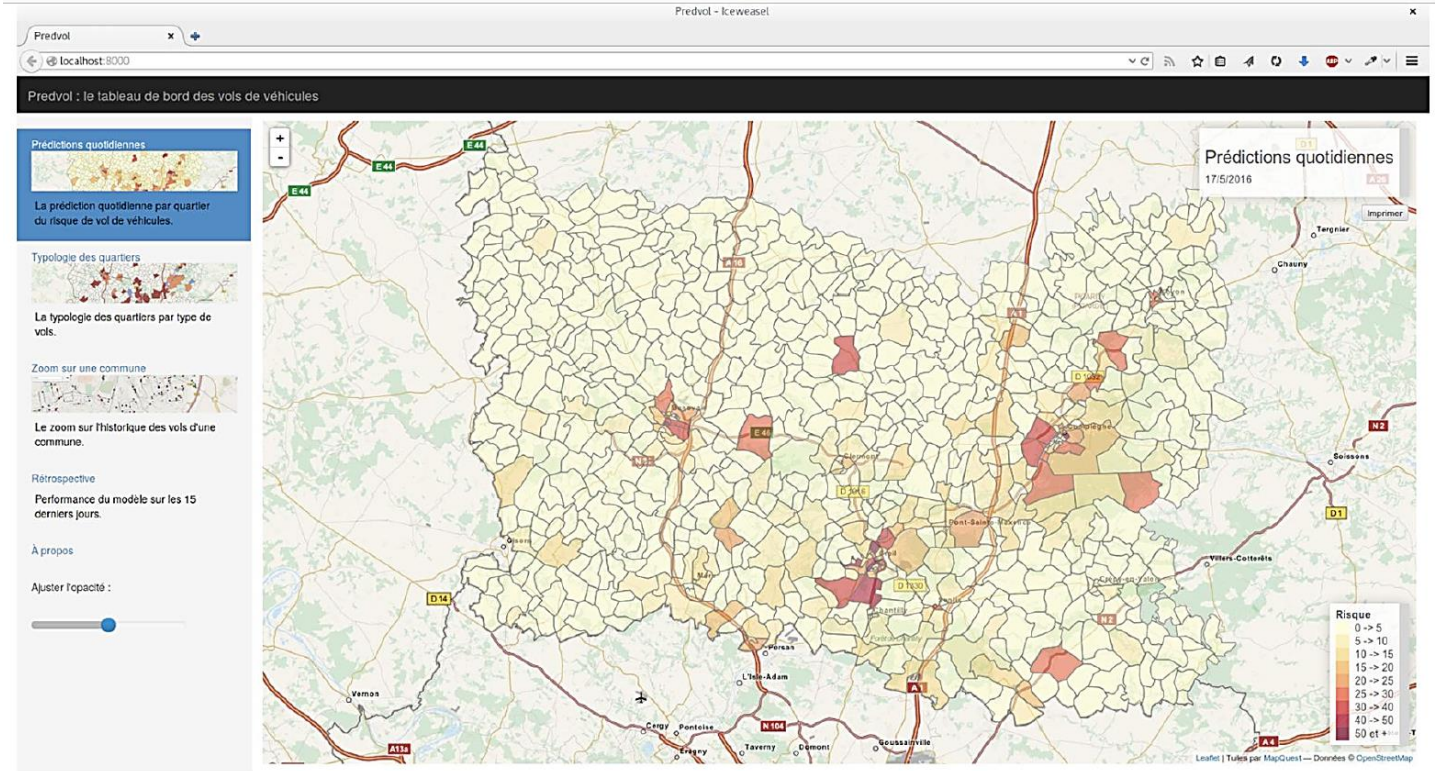
Source : administration générale des données, Secrétariat général pour la modernisation de l'action publique.

(A) Zones très surveillées par les gendarmes et nombreux vols de véhicules répertoriés
(B) Zones touchées par les vols de véhicules mais peu empruntées par les gendarmes

La mission *Etalab*, fondée en 2011 au sein de la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), est chargée de coordonner la conception et la stratégie dans le domaine de la donnée, notamment en matière de développement de dispositifs de cartographies policières. Elle participe en 2015, au lancement du logiciel *Predvol* dans l'Oise. Ce département a été choisi car il est particulièrement exposé aux vols de voiture.

Selon les *datascientists*, le test de l'outil *Predvol* obtient un bilan plutôt satisfaisant statistiquement parlant : « Le modèle prédisait 74% des faits. Et 10% des quartiers représentaient 50% du nombre de vols »[57]. Cependant, lors d'un colloque à l'Institut national des hautes études de la Sécurité et de la Justice en juin 2017, le commissaire divisionnaire Yves Gallot, de la direction centrale de la sécurité publique, exprime que le logiciel *Predvol* était inadapté pour la Police[58]. En effet, le logiciel était composé des données de zones de compétence de la gendarmerie et de la police, difficilement conciliables.

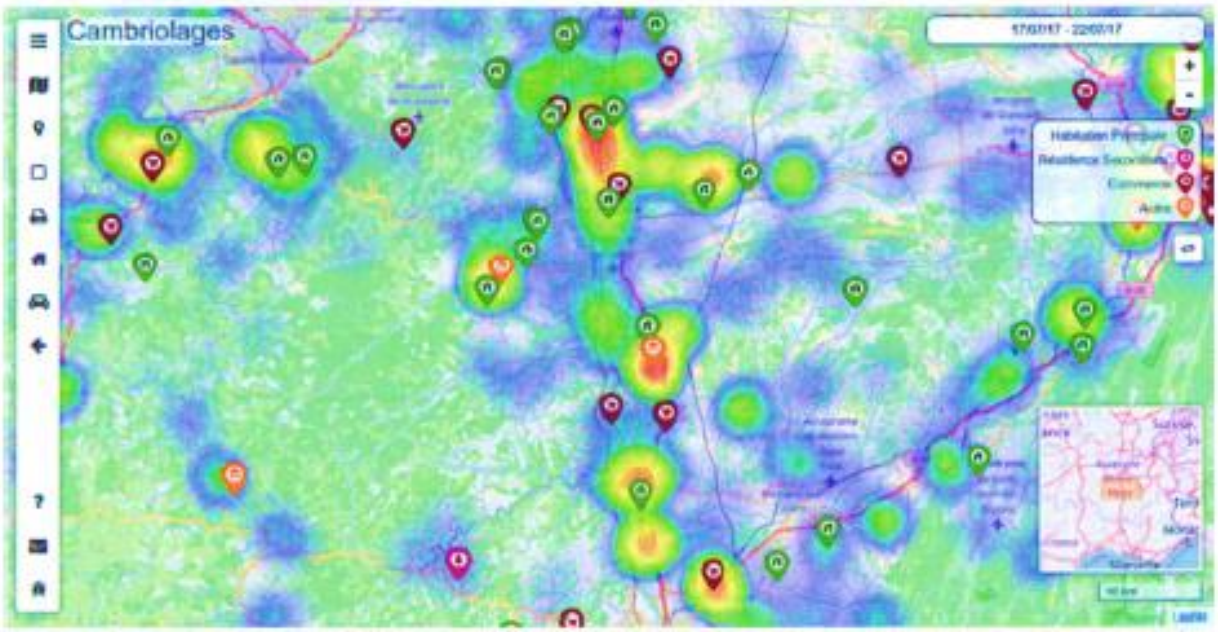
Ci-après, les images du logiciel *Predvol* destiné à la détection des zones de patrouilles à prioriser[59] :



[57] Christophe Le-Bas, « Sous le capot de la police prédictive », Courrier picard, publié le 04 février 2018.
[58] Gabriel Thierry, « La Gendarmerie, de l'analyse prédictive à l'analyse décisionnelle », L'Essor de la Gendarmerie nationale, publié le 26 janvier 2018.
[59] Camille Gosselin, « La police prédictive – enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique », Institut d'Aménagement et d'urbanisme d'Ile de France, Avril 2019 p.17.

Dans le cadre d'outils de cartographie criminelle, un autre type de logiciel capable de déterminer des zones de délinquance a été mis en place au sein de la gendarmerie : le logiciel PAVED (Plateforme d'analyse et de visualisation évolutive de la délinquance). Il s'agit d'un logiciel composé d'un algorithme traitant en temps réel les évolutions des zones de délinquance, sous forme de carte de chaleur interactive. Le terme « chaleur » renvoie à l'idée de « hotspots » anglosaxons précédemment évoqués, soit les lieux sujets à des actes de délinquance dans la ville.

Il a été apporté encore une fois une nuance au terme de « police prédictive » en tant que détection des infractions, du fait que les responsables se servant de cette application, connaissent déjà les zones délicates de leur ville et l'utilisent parfois uniquement afin de prendre leurs décisions « en connaissance de cause » et d'« évaluer un petit peu l'organisation de leur service au quotidien »[60] à titre informatif. Ci-après, l'interface du logiciel PAVED[61] :



L'IA est déployée auprès de l'anticipation de la délinquance. En outre, elle est également présente postérieurement à la commission d'infractions. Il convient de s'intéresser à l'utilisation de l'IA lors de la résolution des enquêtes.

[60] Camille Gosselin, « La police prédictive – enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique », Institut d'Aménagement et d'urbanisme d'Ile de France, Avril 2019 p.17.
[61] Ibid.

Section 2 : L'utilisation de l'IA lors de la résolution d'enquêtes

En matière de résolution d'enquêtes, il est fréquent que les autorités de police et de gendarmerie se tournent vers les nouvelles technologies, dans le but de recueillir des informations de meilleure qualité notamment. Les réseaux sociaux sont en la matière un atout. Comme il a été précédemment exprimé, on y trouve des informations plus à jour que celles possédées par les services de l'Etat.

Par ailleurs, la gendarmerie française utilise également plusieurs logiciels développés par IBM, définis sous l'acronyme *Anacrim*, du terme analyse criminelle. Ils prennent la forme de serveurs permettant de regrouper une masse de données que l'on retrouve au sein d'enquêtes judiciaires très complexes. Sans logiciel, ces enquêtes sont rarement résolues, puisqu'il est « physiquement très difficile d'extraire des liens subtiles »[62] de ce très grand nombre de pièces provenant de diverses entités de l'Etat. Ce genre de dispositifs capable de faire des liens entre une masse de données dans le but de résoudre une enquête n'est pas récent. Les prémices de ces derniers remontent à 1994[63] et comme l'indique le titre de l'ouvrage à paraître de François et Chantal Cazals, cette intelligence a aujourd'hui été « amplifiée par la technologie ».

On retrouve l'usage du logiciel *Anacrim* par la gendarmerie française lors de la réouverture de l'affaire Grégory. Trente ans plus tard, de nouvelles pistes sont explorées. Il s'agit d'un outil d'analyse criminelle, basée sur le rapprochement des données identiques, telles que les conversations téléphoniques, y compris quand les protagonistes sont très nombreux. Une fois les données identifiées, il affiche un schéma relationnel, ainsi que des chronologies.

Ce logiciel est incontestablement plus performant que l'analyse humaine, qui ne pourrait traiter cette masse de données, grâce à une technique de *data mining*, qui consiste en l'extraction d'informations à partir de la fouille d'une grande quantité de données. Le *data mining* est également utilisé en matière de détection de fraudes fiscales pouvant entraîner des sanctions pénales. Notamment, le commerce de marchandises prohibées, l'activité professionnelle non déclarée ou la domiciliation fiscale frauduleuse. L'administration fiscale pourrait en effet, « posséder une vue très précise de nos activités professionnelles ou privées »[64].

---

[62] Cazals François, Cazals Chantal, « Intelligence artificielle : L'intelligence amplifiée par la technologie », Ed. De Boeck Supérieur, à paraître le 31 décembre 2021, p. 238.
[63] Ibid.
[64] Cédric Ingrand, « Le data-mining, l'intelligence artificielle au service du fisc », lci.fr, 2 juillet 2020.

Ci-après, un aperçu du logiciel *Anacrim*[65] :

Force est de constater que l'IA est un outil de surveillance des comportements déviants, ou d'individus déjà connus des autorités de police et de gendarmerie. Cet aspect est retrouvé dans le cadre d'enquêtes ou de la surveillance par le biais de la reconnaissance faciale.

[65] Capture d'écran de la démonstration interactive du logiciel Anacrim, Site IBM i2 Analyst's Notebook, https://www.ibm.com/security/resources/demos/i2-analysts-notebook-demo/#.

Chapitre 3 : La reconnaissance faciale : outil d'enquête et de surveillance massive

Lors de l'autorisation par le Conseil d'Etat de la création d'un fichier recensant les données biométriques relatives aux cartes d'identité et passeports, intitulé « Titres électroniques sécurisés »[66], de vives contestations relatives à cette ingérence au sein de la vie privée sont survenues. Cependant, les dispositifs de reconnaissance faciale et leurs expérimentations fleurissent en France.

Les outils de reconnaissance faciale peuvent être utilisés dans un but de classification sociale en catégories en identifiant les caractéristiques d'une personne (genre, âge, etc.), pour authentifier une personne, c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être – dans le cadre d'un contrôle douanier par exemple. Enfin, pour identifier une personne et la retrouver au sein d'un groupe d'individus, dans un lieu, une image ou une base de données.

Il convient préliminairement d'effectuer une distinction entre le terme reconnaissance faciale et l'utilisation de caméras de surveillance dans le cadre de la reconnaissance d'individus, cela porte souvent à confusion. La CNIL rappelle au sein d'un rapport consacré à la reconnaissance faciale[67], que de simples caméras de surveillance ne permettent pas naturellement de reconnaître automatiquement une personne, bien qu'elles puissent la filmer. Seules les caméras dotées d'un « traitement spécifique pour en extraire des données biométriques »[68], peuvent permettre l'identification d'un individu filmé par rapport à une autre image.

Par ailleurs, reconnaître un individu recherché parmi une foule de personnes peut s'avérer être un exercice difficile pour l'être humain, qui ne peut retenir précisément les caractéristiques physiques, parfois biométriques, de ces personnes. Cela relève d'une technique de *deep learning*, littéralement traduit de l'anglais par « apprentissage profond », dont il sera question dans ce chapitre. Les dispositifs de reconnaissance faciale sont utilisés pour déterminer l'identité d'une personne repérée dans l'espace public, en matière de surveillance publique. D'une part, dans un but de l'interpellation d'une personne non connue de ces services auparavant. D'autre part, dans l'identification au sein d'une masse de personnes, d'un individu recherché.

Les technologies de surveillance de masse ont été développées en France et en Europe, notamment après l'avènement d'attentats terroristes. Comme le rappelle Bertrand Pailhes, directeur des technologies et de l'innovation au sein de la CNIL, il devient de plus en plus courant de passer d'une

---

66 CE, 10ème - 9ème chambres réunies, Inédit au recueil Lebon, le 18 octobre 2018, n°404996.
Voir aussi : Décret n° 2016-1480 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

67 Reconnaissance faciale, pour un débat à la hauteur des enjeux, la CNIL, novembre 2019.

68 Ibid, p. 4.

approche ciblée – en cherchant une personne précise par les activités policières – à une approche générale – c'est-à-dire en observant « tout le monde » pour détecter une certaine personne.[69]

Plusieurs dispositifs de reconnaissance faciale sont expérimentés en Europe. Notamment, à Londres, le 27 février dernier, la reconnaissance faciale est utilisée afin de repérer le visage d'individus faisant partie d'un fichier de personnes recherchées spécifiquement pour des crimes violents. Cependant, le test présente 90% d'échec, malgré une promesse de succès de 70%. Le fonctionnement de cette expérience dans le cadre d'une enquête policière s'est déroulé de cette façon : une camionnette équipée de cette technologie capable de scanner les visages des personnes à la volée passant dans la rue se situait à la sortie d'une bouche de métro. L'opération a été signalée par des affiches mais la seule façon de s'y opposer était de changer de trottoir. Sur les 8600 visages scannés en une journée, huit personnes ont été détectées comme personnes recherchées spécifiquement pour des crimes violents, dont sept à tort.

Il convient alors de comprendre comment fonctionnent intrinsèquement ces dispositifs de reconnaissance faciale. Il s'agit dans un premier temps de s'intéresser à ces dispositifs dans un but de recherche ciblée d'un individu connu des services de police ou de gendarmerie (Section 1). Pour ensuite étudier le cas d'une surveillance de masse afin de détecter un comportement déviant (Section 2).

Section 1 : La reconnaissance faciale au service de la recherche ciblée

Les dispositifs de reconnaissance faciale sont utilisés en matière de recherche ciblée d'individus. Il convient de s'intéresser au fonctionnement de ces algorithmes (§1), pour ensuite étudier des cas existants en France et comprendre le contexte dans lequel ils sont développés (§2).

§1. Le fonctionnement des dispositifs d'IA de recherche ciblée

Ce type de dispositifs est utilisé dans le but de reconnaître un individu suspect au sein d'une foule ou à l'entrée d'un évènement par exemple, des caméras de surveillance disposées d'une habilité de reconnaissance faciale sont fixées sur des portiques de sécurité, sur des agents policiers ou tout objet permettant de repérer un individu recherché.

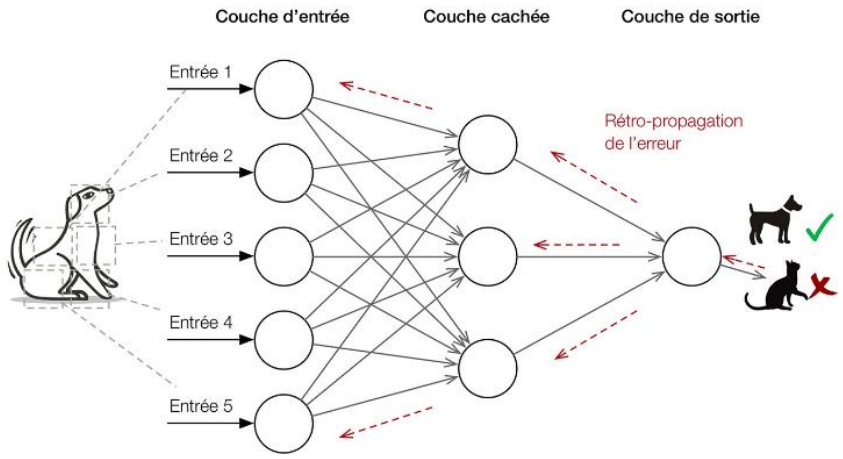
Les données entrées au sein d'un algorithme de reconnaissance faciale, dans le cadre de la recherche d'individus, prennent leur source dans les vidéos de caméras de surveillance, les vidéos témoins et les bases de données policières, dans lesquelles sont utilisées les images issues des vidéos

[69] Bertrand Pailhes, Session parlementaire européenne du 20.02.2020 sur « L'intelligence artificielle au sein de la justice pénale et son utilisation par la police et les autorités judiciaires en matière pénale ».

surveillance, les coordonnées de l'individu recherché ou encore les données biométriques recueillies des fichiers des services de l'Etat.

La donnée biométrique est définie par la CNIL comme n'étant « *pas une donnée d'identité comme les autres. Elle n'est pas attribuée par un tiers ou choisie par la personne. Elle est produite par le corps lui-même et le désigne de façon définitive. Le mauvais usage ou le détournement d'une telle donnée peut alors avoir des conséquences graves* »[70]. A titre d'exemple, sont des données biométriques : l'empreinte digitale, l'iris, le contour de la main, les contours du visage et le son de la voix.

Une fois ces données entrées au sein de l'algorithme, il convient de les traiter. Le dispositif de reconnaissance faciale appartient à la technique algorithmique de *deep learning*. C'est-à-dire que l'algorithme analyse la donnée en profondeur d'une part, pour en ressortir l'information d'autre part. Il s'agit d'un système inspiré du réseau neuronal humain.[71] Ci-après, un schéma explicatif de la technique de *deep learning*.[72]



Les données sont massivement entrées dans l'algorithme de reconnaissance faciale. Afin que l'algorithme soit le plus précis possible et ne se trompe pas avec les données d'une personne innocente, l'algorithme doit préciser la « découpe » de l'image analysée. En effet, lors de la lecture de la donnée issue de la caméra de surveillance, est procédé un découpage de l'image. Cette analyse est divisée en micro-pixels. Ces derniers seront ensuite comparés avec ceux de l'image de la personne à identifier. L'outil scanne instantanément le visage de toutes les personnes passant devant la caméra. A partir de chaque visage scanné, est extrait un modèle mathématique, représentant le visage par 500

---

70 Définition de la donnée biométrique par la CNIL.
71 Dominique Cardon, Jean-Philippe Cointet et Antoine Mazières, *L'invention des machines inductives et la controverse de l'intelligence artificielle*, La revanche des neurones, La découverte n°211, pp. 173-220, p. 199.
72 Schéma : Ibid.

millions de chiffres[73]. En comparant les visages scannés à une banque de données comprenant les visages des personnes recherchées, l'IA peut, parmi le visage de 500 suspects, retrouver le suspect identifié dans la vie réelle.

§2. Les applications au sein de municipalités françaises

En octobre 2017 en France, un mécanisme de reconnaissance faciale a été mis en place à Lyon par les forces de police : un algorithme recueillant les données du fichier de traitement des antécédents judiciaires (TAJ). Le TAJ succède aux fichiers de police STIC (Système de traitement des infractions constatées) et de gendarmerie JUDEX (Système judiciaire de documentation et d'exploitation). Ce fichier est ensuite utilisé en combinaison d'images de vidéosurveillance afin de confondre le suspect en question. Un homme suspecté d'avoir volé un camion a pu être identifié, puis poursuivi grâce au logiciel de reconnaissance faciale « Gestion Automatisé des Signalements et des Photographies Répertoriés et Distribuables » (G.A.S.P.A.R.D).

En octobre 2017, l'outil G.A.S.P.A.R.D est mis en œuvre. Ce dispositif a pour mission d'associer l'image récupérée des caméras de vidéos surveillance avec la base de données policières, afin d'identifier l'auteur d'une infraction. En possession de données telles que les images vidéo ou photographiques et les empreintes digitales de personnes ayant déjà fait l'objet de poursuite, le fichier alimente d'autres bases de données policières. Le dispositif alimente le TAJ des images des personnes mises en cause. Plusieurs parlementaires soulèvent le changement qu'a permis cette avancée ; « il est ainsi désormais possible de lancer dans le TAJ des recherches à partir d'une photographie. Les résultats de la recherche font apparaître les photographies déjà présentes susceptibles d'y correspondre en fonction d'un certain nombre de paramètres (écartement des yeux, etc.). La recherche peut d'ailleurs être affinée par certains critères, tels que le sexe, la couleur des yeux ou des cheveux, etc. Le TAJ constitue déjà, de ce point de vue, un outil de reconnaissance faciale »[74].

D'autres dispositifs continuent d'être explorés et fleurissent notamment après des évènements tragiques. C'est le cas de la ville de Nice, à la suite des attentats lors du rassemblement public du 14 juillet 2016. Les dispositifs de reconnaissance faciale ont été expérimentés et présentés par la direction de la police municipale niçoise[75], lors du carnaval de la ville du 16 février au 2 mars 2019. Cette expérimentation permettait de tester, cette IA sur des volontaires, appréhendés en tant que

---

[73] Directeur de la société Israélienne *Anyvision*, dans le reportage « Tous surveillés : 7 milliards de suspects », diffusé sur la chaîne Arte, le 21 avril 2020, op. cit.

[74] Rapport d'information déposé devant l'Assemblée Nationale française par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, M. Didier PARIS et M. Pierre MOREL-À-L'HUISSIER, p. 36.

[75] Sandra Bertin, directrice de la police municipale de Nice, dans le reportage « Tous surveillés : 7 milliards de suspects », diffusé sur la chaîne Arte, le 21 avril 2020.

terroristes ou personnes recherchées, dans le cadre de l'expérience. Le logiciel utilise les caméras de la ville pour mettre un nom sur le visage des volontaires. A la manière du *fast-access* [76] consistant en l'identification de l'individu dès son entrée du carnaval à l'aide d'une seule photographie. L'individu est reconnu par le logiciel et est directement interpellé par la police, qui reçoit instantanément un signal électronique.

Section 2 : La surveillance de masse au service de la recherche d'un comportement déviant

Afin d'écarter tout raisonnement erroné quant à la notion de reconnaissance faciale, il convient de d'apporter une nuance à la conception même de surveillance par caméras dans les lieux publics. Cette dernière ne renvoie pas systématiquement à des processus de reconnaissance faciale, puisque le couplement des caméras à des dispositifs d'extraction et de comparaison de données biométriques est nécessaire. La CNIL rappelle ainsi que des « techniques informatiques de détection de comportements anormaux ou d'événements violents, de reconnaissance d'émotions sur les visages ou même de silhouettes ne constituent généralement pas des systèmes biométriques »[77].

L'organisme ajoute que « ces illustrations ne sont cependant pas sans lien avec la reconnaissance faciale, car celle-ci peut être associée à d'autres dispositifs. En effet, à la différence par exemple des systèmes de captation et de traitement vidéo, qui nécessitent la mise en place de dispositifs physiques, la reconnaissance faciale est une fonctionnalité logicielle qui peut être mise en œuvre au sein de systèmes existants (caméras, base de données de photos, etc.). Cette fonctionnalité peut donc être connectée, branchée sur une multitude de systèmes, et combinée avec d'autres fonctionnalités »[78].

C'est le cas d'une technique développée en Chine, où les caméras de surveillance couplées à des fonctionnalités reconnaissant les individus via la consultation de leurs données biométriques, sont omniprésentes au sein des lieux publics. Il s'agit d'un outil politique permettant de conditionner les ressortissants chinois à un comportement de « citoyen parfait », par un système de notation des individus, notamment. Ce dispositif d'IA de reconnaissance faciale, fait également l'usage de la technique de *deep learning*. Pour des raisons de synthétisation, il y a lieu de renvoyer aux développements afférant à cette technique[79].

A titre d'exemple, la Chine possédait en 2013, 100 millions de caméras de surveillance dans l'espace public, et en possède désormais en 2020, près de 600 millions, « soit une caméra pour deux

---

[76] Le procédé de l'expérience de reconnaissance faciale a été détaillé dans l'interview de Mme Sandra Bertin, directrice de la police municipale de Nice, réalisé dans le cadre de cette étude. L'interview est disponible en Annexe.
[77] Reconnaissance faciale, pour un débat à la hauteur des enjeux, la CNIL, 15 novembre 2019, p. 4.
[78] Ibid.
[79] Cf. Partie 1, Titre 1, Chapitre 3, section 1, §1.

habitants »[80]. La politique chinoise de surveillance de masse tend à s'exporter. En Europe, la surveillance des comportements déviants s'effectue également par des caméras disposant d'outils de reconnaissance faciale et est interdite si elle n'est pas encadrée. Ainsi, la surveillance dite « à la volée », a pu être expérimentée au Royaume-Uni, comme détaillé en introduction du chapitre. Mais ces expérimentations sont strictement encadrées et signalées afin que les personnes ne soient pas filmées à leur insu par ces dispositifs. Ces mêmes règles s'imposent à l'expérimentation niçoise développée ci-dessus.

En France, la surveillance par identification faciale n'est pas uniquement reliée à la biométrie du visage, telle qu'expérimentée à Nice et à Lyon. Il est intéressant d'étudier le cas de la détection d'un comportement déviant par d'autres caractéristiques permettant aux autorités de police d'identifier un individu. A Paris, une technique d'identification d'une personne au comportement déviant, telle que des mouvements de foule, des comportements violents ou des objets délaissés, par la pixellisation, est utilisée au sein de la station de métro Châtelet-les-Halles. Ce mécanisme d'aide à l'interpellation, dans un but de sécurité publique, prend la forme d'une caméra reliée à un système permettant d'informer les autorités compétentes de la commission d'une infraction. La caméra détecte la couleur des vêtements de l'auteur de l'infraction et transmet l'information aux autorités, qui peuvent ainsi l'interpeller plus rapidement[81].

D'une part, la notion même d'aide à l'interpellation par ce type de dispositifs pourrait sur le long terme s'inscrire dans une « politique du chiffre »[82], finalement nuisible au bon fonctionnement de la prévention des infractions. D'autre part, ce concept est appréhendé comme maladroit, voire liberticide, par la confusion entre des voyageurs égarés et des maraudeurs, lorsqu'ils restent statiques pendant plus de 300 secondes[83]. Ces voyageurs malencontreusement interpellés, s'ils souhaitent connaître leurs droits, pourraient se diriger vers des dispositifs de communication en ligne développés par des *legaltechs*. Ces sociétés confectionnent des technologies, de plus en plus au service des justiciables, lors de la préparation à un procès notamment.

---

[80] Reportage « Tous surveillés : 7 milliards de suspects », diffusé sur la chaîne Arte, 21 avril 2020.

[81] Camille Gosselin, « La police prédictive – enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique op. cit., p. 7.

[82] La politique du chiffre est le fait pour les autorités de police d'effectuer massivement des interpellations concentrées sur des affaires moins pertinentes, afin de satisfaire les objectifs statistiques sur la forme mais pas sur le fond. Par exemple, interpeller de manière massive des acheteurs de drogue au lieu de « faire tomber un réseau de drogue ».

Jean-Yves Le Bouillonnec et Didier Quentin, Rapport d'information n°988, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, sur la mesure statistique des délinquances et de leurs conséquences, 24 avril 2013.

[83] Bastien Lepine, La RATP transforme Châtelet en laboratoire de test pour la reconnaissance faciale, Site internet le Bigdata, le 27 février 2020.

Titre II : Le recours à l'IA au cours du procès pénal

Les dispositifs d'IA permettraient de « rendre les rapports sociaux prévisibles »[84]. L'introduction de la technique dans le domaine juridique est une suite logique, puisqu'« après la santé, l'éducation, l'urbanisme ou la vie politique, la justice est bouleversée par la technologie »[85]. L'avènement des évolutions numériques et de l'IA comme le « grand mythe de notre temps »[86], est en effet devenu nécessaire à l'institution judiciaire devant intégrer l'apport des nouvelles technologies[87].

La digitalisation de la justice, au sens de procès, ainsi que son caractère prédictif se sont développés dans plusieurs secteurs du droit, comme le droit administratif, le droit de la famille ou encore le droit civil, notamment, en droit de la responsabilité civile. Le procès pénal est pour le moment écarté, principalement pour des raisons d'éthique. Cependant, le procès pénal n'échappe pas à la vague d'*open data,* libre accès des données sous forme d'information structurée[88], des décisions judiciaires dont il est question en France depuis la loi du 7 octobre 2016 pour une République numérique. Plusieurs outils sont à la disposition des justiciables pour préparer leur procès pénal. Lorsqu'Antoine Garapon distingue le terme « justice digitale »[89] de la justice prédictive, c'est que cette dernière est comprise au sein de la première. D'inspiration des pays anglosaxons, la justice prédictive apparaît. Il conviendra d'appréhender ce terme et son développement.

Il s'agit de comprendre quels sont les dispositifs présents au sein de la préparation du procès pénal (Chapitre 1). Il s'agira ensuite de s'intéresser à la justice prédictive en tant qu'aide à la décision, en nuançant l'idée selon laquelle, la prise de décision serait automatisée (Chapitre 2).

Chapitre 1 : La digitalisation de la préparation du justiciable au procès pénal

Les legaltechs sont des sociétés confectionnant des technologies, de plus en plus au service des justiciables et des professionnels du droit. S'il est possible que certains dispositifs automatisés soient créés à l'initiative d'avocats, à destination des avocats et des justiciables, d'autres sont créés par des sociétés privées à destination des justiciables. Le développement des *legaltechs* fait surface en France. Ces dispositifs sont utilisés dans un but de simplification des échanges entre les parties, du procès pénal – à titre d'exemple, pour simplifier les échanges d'informations, faciliter les audiences, sécuriser

---

84 Antoine Garapon, « *Les enjeux de la justice prédictive* », JCP G, 2017, n°01-02, p.48.
85 Ibid, p.47.
86 CNIL, « Comment permettre à l'homme de garder la main », rapport sur les enjeux éthiques des algorithmes et de l'IA, 15 décembre 2017, p.2.
87 Institut Montaigne, « *Justice : faîtes entrer le numérique* », Rapport de novembre 2017 : « L'institution judiciaire doit aujourd'hui intégrer l'apport des nouvelles technologies », p. 3.
88 Définition de l'open data par la charte éthique de la CEPEJ, §24 p. 20
89 Antoine Garapon, « *La justice digitale* », PUF, 2018.

la garde à vue, renforcer les outils d'investigation ou offrir une alternative à l'incarcération. Les nouvelles technologies « sont en train de bouleverser la pratique de la procédure pénale »[90].

Différents dispositifs d'aide à la préparation du procès pour les justiciables, ou bien de prise de connaissance de leurs droits de défense, apparaissent progressivement. En période de confinement notamment, rendant compliquée la rencontre avec un avocat, des logiciels de discussion juridique se développent. On les appelle les *legalbots*, issus du concept de *chat-bots*, traduits par robots de discussion, déjà présents sur plusieurs sites d'assurance, banque, vente en ligne, etc. pour un accès à l'information par les consommateurs et clients 24 heures sur 24, 7 jours sur 7. En France, les *legalbots* sont rares mais tendent à se développer. C'est le cas de « Justinien », créé en 2018 et permettant de diriger le justiciable lui ayant exposé les faits et les problèmes de droit rencontrés.

Justinien comprend le langage commun et juridique et s'améliore au fur et à mesure que les utilisateurs le consulte, il apprend également « comme les étudiants à l'Université »[91] à raisonner par syllogisme. Il est compétent pour résoudre les problèmes liés aux dommages corporels dans les accidents de la route, il est notamment spécialisé en matière d'agressions et harcèlements. Lors d'une interview en présence de ses développeurs, il explique essayer de « déceler une intention dans les mots exprimés »[92], il pose également des questions afin de comprendre quel texte juridique est applicable. Il a pour objectif d'apporter une réponse basique et compréhensible à toute personne souhaitant prendre connaissance de ses droits dans une situation donnée. Il dirige même les justiciables vers des spécialistes du droit. Les instruments intelligents, sont ainsi à la disposition des justiciables, mais également des professionnels du droit, pour préparer un procès.

Si Justinien n'a pas pour objectif initial de remplacer les avocats, il n'est pas impossible que sur le long terme cela soit le cas, notamment par le fait que la capacité de communication de ce dispositif soit plus efficace et moins coûteuse pour les justiciables. D'autre part, il pourrait également être utilisé au cœur du procès pénal, s'il est capable de « déceler une intention dans les mots exprimés »[93], afin d'être utilisé en tant que preuve de la culpabilité d'un individu par exemple.

Il s'agit de s'intéresser au cas des *legaltech*s, mettant en œuvre des dispositifs de moteurs de recherche légaux, extrayant des informations d'une quantité massive de jurisprudence, après le phénomène émergent d'*opendata* des décisions de justice en France. Il convient dans un premier temps de comprendre le fonctionnement de ces dispositifs prenant la forme de moteurs de recherche jurisprudentiels à la disposition des avocats et des justiciables, malgré l'arrivée tardive de la matière

---

90 Anne Moreaux, La procédure pénale et les nouvelles technologies, 21 décembre 2018.
91 Interview du legalbot Justinien par le site internet Village-justice.fr, février 2018. Passage souligné par mes soins.
92 Ibid.
93 Ibid.

pénale au sein du contexte des *legaltechs* (Section 1) pour étudier dans un second temps la tendance émergente à la digitalisation de la préparation du procès pénal (Section 2).

Section 1 : L'arrivée tardive des *legaltechs* en matière pénale

La CEPEJ définit les *legaltechs* comme étant des : *« Entreprises exploitant les technologies de l'information dans le domaine du droit afin de proposer des services juridiques innovants. Ces entreprises sont des startups spécialisées dans le domaine juridique. D'autres termes dérivés des secteurs d'activités sont aussi apparus comme les « fintechs » pour les startups déployant des services financiers, les « medtechs » dans le domaine médical, etc. »*

Les *legaltechs* se développent de façon exponentielle dans plusieurs secteurs du droit, en dehors du droit pénal. En 2018, le nombre de *legaltechs* s'élevait à 900[94]. Prenons le cas des *legaltechs* développant des dispositifs capables d'extraire et lire les données issues de la compilation d'une quantité massive de décisions juridiques. Il s'agit d'une part d'exploiter le phénomène récent et en émergence du *big data judiciaire*, soit l'abondante publication et diffusion de la jurisprudence. Après anonymisation, les arrêts de la chambre criminelle de la Cour de cassation sont publiés sur le site legifrance.gouv.fr en « *open data* »[95], libre accès des données.

Les avocats utilisent ces outils algorithmiques reprenant des données au sujet des décisions de justice passées ainsi que les données plus ou moins précises et détaillées sur les personnes jugées. Ces outils leur permettent de préparer la défense de leurs propres clients. Les outils d'intelligence artificielle utilisés par les avocats sont des outils ayant vocation à faciliter la recherche de l'information par l'avocat.

Des moteurs de recherches comme « Doctrine.fr » par exemple contribuent à assister les avocats dans leur recherche d'information. La société Doctrine, démontre que 88% de leurs clients avocats ont besoin d'outils facilitant la recherche d'information, car les données judiciaires, faisant l'objet par cette application d'une classification ultraperfectionnée et personnalisable, sont généralement enfouies dans une masse d'informations.

Comment fonctionne concrètement l'IA issue des dispositifs de lecture et d'extraction d'informations ? A la manière traditionnelle de la conjugaison entre l'algorithme et le *big data*, précédemment étudiée, il s'agit premièrement d'une entrée de données massives. Les données sont issues des juridictions, et comportent les variables suivantes : le nom de la juridiction, sa composition,

---

[94] Olivier Chaduteau, intervention lors du colloque à la Cour de cassation, « Justice prédictive : perspectives et limites », le 12 février 2018.

[95] Charte éthique CEPEJ, §24 p. 20 : l'open data concerne le libre accès des données sous forme d'information structurée.

la date de la décision, son visa, les faits, les motifs, les argumentaires des parties. Enfin, le dispositif. Les données transportent des informations. A la manière du *machine learning* précédemment étudié, une équipe de développeurs entraîne l'IA à distinguer les informations, puis à les classer par un étiquetage supervisé de l'information au départ, afin d'aider l'algorithme à devenir autonome. Le but de ces logiciels prenant la forme de moteurs de recherches jurisprudentiels est de passer d'une donnée brute, comme le visa ou les faits d'une décision, à une information utile, à un résultat cherché. L'IA transforme ensuite ces informations en « modèles », c'est-à-dire, en une représentation mathématique d'un problème donné. L'IA doit classer et repérer les contextes des décisions rendues afin d'organiser celles ayant un thème et une construction juridique similaires. L'algorithme effectue un traitement automatisé, répertoriant des décisions reçues tous les jours. Par le fait que la jurisprudence évolue, il est amené à traiter des décisions inédites et à les classer de manière pertinente. Lors de revirement de jurisprudence, l'algorithme pourrait ne pas être efficace et une totale autonomie n'aurait donc pas de sens. Il doit alors en matière de jurisprudence être particulièrement supervisé et régulé.

En dehors de la matière pénale – à titre d'exemple pour comprendre le but de certains algorithmes au sein de la préparation d'un jugement – le résultat peut prendre la forme d'une analyse stratégique, afin de savoir où l'avocat représentant un individu licencié, aurait le plus de chances de le voir reconnu en licenciement sans faute réelle et sérieuse. Selon le journal Libération, « en tapant des mots-clés [...] tels que « licenciement » et « ivresse », l'algorithme est capable d'estimer que dans 19 % des cas comprenant ces deux critères, un « licenciement sans cause réelle et sérieuse » a été prononcé. En la matière, un avocat a davantage de chances de succès à Rennes (où les statistiques sont de 35 %) qu'à Versailles (12 %), juridiction manifestement plus répressive avec l'alcool. »[96]

Le Conseil constitutionnel[97] est conscient d'un potentiel « profilage des professionnels de justice à partir des décisions rendues, pouvant conduire à des pressions ou des stratégies de choix de juridiction de nature à altérer le fonctionnement de la justice », si les données d'identification des professionnels de justice sont réutilisées. Il convient également de rappeler que la majorité des *legaltechs* permettant une évaluation des chances de succès à l'issu d'un litige s'interdisent la matière pénale, pour des raisons d'éthique, afin d'empêcher que l'auteur d'un crime ne choisisse ses victimes en fonction de leur lieu de résidence, auquel cas nous assisterions à un véritable *forum shopping*[98]. Ce concept pourrait apparaître sur le long terme, par le développement de *l'open data* des décisions de justice.

---

[96] Julie Brafman, « *Justice prédictive, l'augure des procédures* », Liberation.fr, 23 février 2017.
[97] Conseil constitutionnel, décision n° 2019-778 DC du 21 mars 2019 - Communiqué de presse, p.
[98] Il s'agit d'une pratique utilisée en droit international privé, consistant à saisir la juridiction qui rendrait la décision la plus favorable au demandeur.

Section 2 : L'expansion de l'open-data des décisions de justice et sa régulation en essor

Bien qu'en pratique la matière pénale n'offre d'abondants exemples comme en droit administratif ou en droit de la responsabilité civile, elle n'est pas formellement exclue. D'une part, puisque les décisions judiciaires concernent incontestablement les décisions pénales. Ainsi, l'article L 111-13 du code de l'organisation judiciaire issu de la loi du 7 octobre 2016 prévoit un principe d'*open data* concernant « *les décisions rendues par les juridictions judiciaires* »[99], pour une meilleure lisibilité du processus décisionnel. Par ailleurs, Monsieur Jean-Jacques Urvoas, ancien garde des sceaux, prévoyait en janvier 2017 que l'entièreté des décisions pénales des cours d'appel seraient mises à la disposition du public dans les deux à trois ans[100], soit actuellement.

Ainsi, le 29 juin dernier, le décret n°2020-797 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives, voit le jour. Son article 6 dispose des modalités d'accès aux tiers des décisions de juridictions pénales faisant suite à un débat public. Ci-après l'article 6, paragraphe 2 du décret : *« La section 5 du chapitre II du titre X du livre V est complétée par un c « Délivrance de copies aux tiers » ainsi rédigé :*

Art. R. 166. – En matière pénale, peut être délivrée à des tiers, sans autorisation préalable, la copie:

1. Des arrêts de la Cour de cassation ; 2. Des décisions des juridictions de jugement du premier ou du second degré, lorsqu'elles sont définitives et ont été rendues publiquement à la suite d'un débat public. »

Exception faite pour les « décisions non définitives, des décisions rendues par les juridictions d'instruction ou de l'application des peines et des décisions rendues par les juridictions pour mineurs ou après des débats tenus à huis clos »[101], ne figurant dans les catégories de données publiées dans le cadre de l'open data du fait que leur publicité puisse survenir uniquement après l'autorisation du procureur de la République. Une semaine après l'entrée en vigueur de ce décret, le Conseil d'Etat réagit et évoque l'ouverture par l'open data de « nouvelles perspectives dans l'exercice de la justice, il promet une accélération du règlement des litiges, une plus grande cohérence et prévisibilité des décisions de justice »[102].

Par ailleurs, le vice-président du Conseil d'Etat, à la suite de l'émergence de *l'open data* des décisions de justice ainsi que globalement celle du numérique au sein de la justice, rappelle que : *« Le*

---

[99] Article L 111-13 §1 du code de l'organisation judiciaire.
[100] Caroline Fleuriot, « Avec l'accès gratuit à toute la jurisprudence, des magistrats réclament l'anonymat », Dalloz actu., 06.02.2017.
[101] Article 6 du décret n°2020-797 du 29 juin 2020, art. R 170.
[102] Communiqué de Presse du Conseil d'Etat, « Open data des décisions de justice : une régulation nécessaire des algorithmes », le 6 juillet 2020.

numérique ne saurait non plus déshumaniser la justice : il doit être accueilli comme un moyen d'aiguiser l'intelligence du juge, pas de la remplacer. La déclaration commune signée par le Conseil d'État, le Conseil national des barreaux et l'Ordre des avocats au Conseil d'État et à la Cour de cassation contribue dans cet esprit à concilier l'émergence de l'open data et des algorithmes avec la confiance que doit continuer à susciter l'œuvre de justice. »[103]

Ce rappel se veut anticipateur des risques de transformer le juge en robot appliquant sans discernement le résultat fourni par l'algorithme de décision. Deux volets de la justice prédictive se trouvent dans cette réflexion : les dispositifs d'IA, en tant qu'aide à la décision, et en tant que prise de décision, pour l'instant purement fictionnel.

Chapitre 2 : Le futur incertain de la justice prédictive

Au sein du rapport sur l'*open data* des décisions de justice par Loïc Cadiet, la justice prédictive est définie comme un « ensemble d'instruments développés grâce à l'analyse de grandes masses de données de justice qui proposent notamment à partir d'un calcul de probabilité, de prévoir autant qu'il est possible l'issue d'un litige »[104]. C'est une description à visée technique, suivant également la définition de Bruno Dondero. Selon ce dernier, la justice prédictive « désigne non la justice en elle-même, mais des instruments d'analyse de la jurisprudence et des écritures des parties, instruments qui permettraient de prédire les décisions à venir dans des litiges »[105]. Le terme justice prédictive, signifierait littéralement, la prédiction de la décision de justice, alors même qu'une décision de justice n'est pas un élément prédictible par un algorithme, les données entrées au sein du dispositif d'IA aussi précises et mises à jour soient-elles.

Des algorithmes d'aide à la décision sont présents aux Etats-Unis. Ils sont capables d'évaluer le comportement récidiviste du prévenu dans le cadre de l'évaluation du *quantum* de sa peine notamment dans la décision *Loomis c. Wisconsin* [106] rendue par la Cour Suprême des Etats-Unis en 2017. En revanche en France, la justice prédictive en tant qu'aide à la résolution d'un procès possède une place moins importante, la justice pénale étant « en retard en matière informatique »[107], mais ses prémices sont visibles. Il convient d'étudier les prémices de la justice prédictive en tant qu'aide à la décision en matière pénale française (Section 1) et de nuancer l'idée fictive de « robotisation » du juge (Section 2).

---

[103] Intervention de Bruno Lasserre, vice-président du Conseil d'Etat, dans « Open data des décisions de justice : une régulation nécessaire des algorithmes », le 6 juillet 2020.
[104] Loïc Cadiet, Rapport sur l'open data des décisions juridiques prescrit par le Ministère de la Justice, 2017, p. 14.
[105] Bruno Dondero, « Justice prédictive : la fin de l'aléa judiciaire ? », D. 2017, n°10, p. 532.
[106] Cour Suprême des Etats-Unis, *Loomis c. Etat du Wisconsin*, n° 16-6387, 26 juin 2017
[107] Emmanuel Dreyer, « L'Intelligence artificielle et le droit pénal », dans Alexandra Bensamoun et Grégoire Loiseau, Le droit et l'intelligence artificielle, Ed. LGDJ, 219, p. 224.

Section 1 : Les prémices des formes d'aide à la décision pénale en France

Le développement d'algorithmes d'aide à la décision émerge, premièrement des Etats-Unis, utilisant la justice prédictive en matière d'« *evidence based sentencing* »[108] selon lequel un score est établi sur le risque de récidive et à partir duquel sera calculée la durée de la peine.[109]

Les magistrats français, pour établir leur décision, possèdent déjà un accès plus large que celui à disposition des avocats ou des justiciables. La Cour de cassation « gère (...) les bases de données Jurinet et Jurica, regroupant respectivement les décisions de la Cour de cassation et les décisions civiles des cours d'appel »[110] et « possède déjà l'expertise et la technicité requises »[111]. Par ailleurs depuis août 2018[112], lors de l'étude des dossiers, les magistrats ont également accès à des dossiers des services de police ou de gendarmerie. Ils ont directement accès au TAJ (traitement des antécédents judiciaires)[113], auparavant fourni en version papier par demande aux services de police ou de gendarmerie.[114]

Différents des dispositifs d'IA à proprement parlé, plusieurs tableaux d'analyse et d'étude au sujet de la récidive notamment, existent en France. Une modélisation des risques de récidives est observée au début des années 2000, c'est-à-dire qu'un calcul sous forme de modèle de régression permet de comparer les risques de récidive selon l'ensemble des caractéristiques connues des condamnés. Parmi ces huit caractéristiques, figurent des éléments d'identification propres à l'individu comme le sexe, la nationalité, l'âge à la libération, la situation matrimoniale et professionnelle ; mais également la durée et les modalités d'exécution de la peine et les infractions principales comparables. Cette étude, datant de 2002 estime que les personnes ayant été condamnées plusieurs fois dans le passé ont quatre fois plus de chance de récidiver dans les cinq années suivant leur libération, que les personnes condamnées qu'une seule fois.[115]

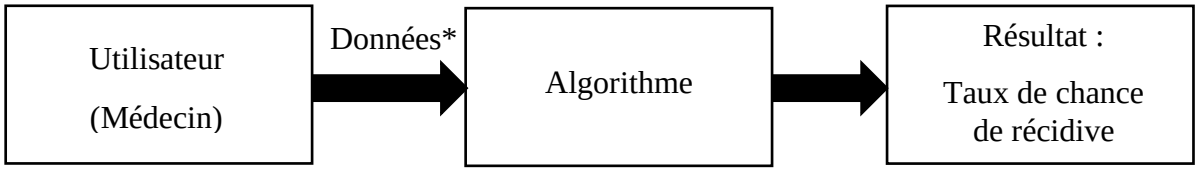
---

[108] « La pratique fondée sur les preuves, sur les faits, ou sur des données probantes ».
[109] Antoine Garapon et Jean Lassegue, « *La justice digitale* », PUF, 2018, pp. 255-256.
[110] Intervention de Monsieur Bertrand Louvel lors du colloque « La justice prédictive » organisé par l'Ordre des avocats au Conseil d'État et à la Cour de cassation, le lundi 12 février 2018.
[111] Bertrand louvel, introduction du livre, Alexandra Bensamoun et Grégoire Loiseau, Le droit et l'intelligence artificielle, Ed. LGDJ, 219, p. 16.
[112] Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
[113] Op. cit. P1. T1. Ch. 3. S1. §2.
[114] Rapport d'information déposé devant l'Assemblée Nationale française par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, M. Didier PARIS et M. Pierre MOREL-À-L'HUISSIER, p. 30.
[115] Florence De Bruyn et Annie Kensey, « 50 ans d'études quantitatives sur les récidives enregistrées », Direction de l'administration pénitentiaire, Collection Travaux et Documents, Décembre 2017, pp. 18-19.

Emmanuel Dreyer soulève alors pertinemment la question de la capacité des technicités des magistrats à « gérer ces données massives ? » [116]. Cependant, la France demeure réticente à l'appréhension algorithmique du comportement d'un prévenu afin de prendre une décision pénale. L'article 10 de la loi informatique et liberté dispose de cette interdiction, qui sera reprise au sein de l'article 22 du RGPD. Cela viendrait atteler le juge à un rôle secondaire, dans le procès pénal, « tel qu'en droit intermédiaire »[117], époque de transition entre l'ancien droit, avant la révolution française et le droit instauré par le code civil, soit entre 1789 et 1804.

En outre, des algorithmes d'évaluation de risque des individus sont présents en Europe, en Allemagne et en Autriche notamment. Il s'agit de l'examen comportemental d'un prévenu à l'aide d'un algorithme à disposition de psychologues assermentés par une juridiction, à des fins probatoires. En l'espèce prenons l'exemple de l'algorithme F.O.T.R.E.S (Forensic Operationalized Therapy and Risk Evaluation-System), il permet d'analyser la potentialité de récidive d'un condamné pour agression sexuelle. F.O.T.R.E.S est disponible en langue française, mais n'a pas été validé par la France.

Ci-après un schéma explicatif du fonctionnement de F.O.T.R.E.S [118].



Il est certain que l'on « peine à imaginer que le développement de cette IA soit abandonné à l'initiative privée »[119], puisqu'il ne serait pas rentable pour le ministère de la Justice d'effectuer un contrôle dans le développement de ses outils notamment[120]. En revanche, il ne faut pas sous-estimer les capacités du traitement automatisé des *legaltechs*, développant des outils mettant à disposition publique, les décisions anciennement rendues par les juridictions. Ces outils pourraient-ils être présents au sein de l'engrenage d'un juge-robot, capable de fonder des prévisions de décisions à la suite d'une analyse complexe des décisions précédemment rendues, grâce à des traitement algorithmiques[121]? Il convient d'apporter les nuances à la notion de justice prédictive, quant à son volet de « prise de décision ».

---

[116] Emmanuel Dreyer, op. cit., p. 225.
[117] Emmanuel Dreyer, op. cit., p. 215.
[118] Emmanuelle Walter, « Evaluation de la dangerosité et du risque de récidive d'auteurs mineurs d'infraction à caractère sexuel : à partie de 64 expertises psychiatriques pénales », Thèse universitaire, Université de Lorraine, 2015, pp. 87-88.
* Ces données sont issues de la clinique du patient, des éléments issus de ses dossiers administratifs et médicaux.
[119] Emmanuel Dreyer, op. cit., p. 229.
[120] Ibid.
[121] Loïc Cadiet, *Rapport sur l'open data des décisions juridiques prescrit par le Ministère de la Justice*, Novembre 2017, p. 24 : Le terme « prédictif », fréquemment employé par référence à l'anglais, peut en vérité être discuté : les traitements algorithmiques auxquels il fait référence déterminent davantage les probabilités de l'issue d'un litige – et encore, sous réserve que certaines conditions soient réunies – qu'ils ne prédisent le résultat de la cause.

Section 2 : La nuance nécessaire au volet de prise de décision robotisée

Après s'être intéressé au domaine de tout ce qui est calculable, Alan Turing le différencie du non-calculable, « c'est ce qui résiste à ce déterminisme, c'est ce qui peut évoluer de manière imprévisible »[122]. Alan Turing « se heurte aux processus biologiques qui entretiennent avec le déterminisme, un rapport tout autre »[123]. La justice prédictive peut être définie comme un ensemble de traitements visant à anticiper l'issue d'un contentieux. Il peut s'agir d'un moteur de recherche permettant de traiter un ensemble massif de données judiciaires comme il a été mentionné précédemment. À la suite du projet ayant déjà vu le jour en Estonie en 2019[124], naît l'idée d'un algorithme puisse assister le juge en imitant son raisonnement à l'issue d'une analyse précise et complexe des décisions précédemment rendues. Cependant, cela reste en France, quelque chose de spéculatif et non mis en place. Par ailleurs, si les algorithmes d'aide à la décision des juges en matière pénale, n'est que l'expression d'un futur plus ou moins proche pour l'instant en France, l'idée que l'IA soit capable de reprendre un raisonnement identique à celui d'un juge humain n'est pas acceptable, d'un point de vue pratique (§1) et éthique (§2).

§1. La nuance pratique

D'un point de vue pratique, une décision juridique fluctue en fonction de plusieurs critères, comme la nature de l'infraction, l'interprétation des faits, ainsi que les procédures et règles applicables au procès en question et bien d'autres critères encore. Les mots de Michel Foucault décrivent la composition d'un jugement : « connaissance de l'infraction, connaissance du responsable, connaissance de la loi, trois conditions qui permettaient de fonder en vérité un jugement »[125]. Emmanuel Dreyer conforte l'idée qu'un dispositif d'IA ne puisse pas entreprendre les mêmes réflexions d'un être humain, sensible. L'algorithme agit par induction, soit par corrélation, et le magistrat, par déduction, soit par syllogisme juridique. Le procès pénal est complexe à l'appréhension d'un algorithme et il est composé de « l'établissement des faits – l'évaluation de la force probante des éléments avancés -, l'appréciation de la culpabilité – même si elle est déduite le plus souvent des faits – et enfin, le choix de la peine »[126]. L'argument d'apprendre la réflexion syllogistique à un dispositif d'IA est pertinent et est déjà testé (voir les développements au sujet de Justinien ci-dessus). Or, il s'agit parfois pour le magistrat, d'aller au-delà de la déduction et de « prendre en compte les

---

[122] Pierre Lescanne, « L'héritage d'Alant Turing – l'inventeur de l'ordinateur, le pionnier de l'intelligence artificielle », CNRS Le journal, hors-série, Mai 2012, p.5.
[123] Jean Lassègue, « L'héritage d'Alant Turing – l'inventeur de l'ordinateur, le pionnier de l'intelligence artificielle », CNRS Le journal, hors-série, Mai 2012, p.8
[124] En 2019, le ministère estonien de la Justice a annoncé avoir décidé de travailler à la création d'un « juge-robot » chargé de trancher les litiges de moins de 7.000 euros, notamment en matière contractuelle.
[125] Michel Foucault, « Surveiller et punir, naissance de la prison », op. cit.
[126] Emmanuel Dreyer, op. cit., p. 223.

émotions afin d'évaluer une situation humaine »[127]. Professeur Emmanuel Jeuland décrit d'ailleurs une « période de décantation des faits et du droit »[128]

Quant à lui, l'algorithme d'aide à la décision à ce jour développé n'est pas un outil permettant une anticipation de la décision du juge pénal, puisque les décisions juridiques ayant été la base de données de l'IA sont de simples données statiques, qui ne peuvent être appliquées à un cas plus moderne et traité dans un contexte différent, que l'IA ne prendrait pas en compte.

§2. La nuance éthique

Antoinette Rouvroy, philosophe du droit, rappelle d'ailleurs en reprenant les écrits d'Alain Supiot, que l' « *homo juridicus* est irréductible à *l'homo numericus* »[129]. Elle précise par la même occasion, que l'algorithme ne laisse pas de place à l'interprétation, lors de ses calculs de probabilité. L'utilisation d'algorithmes à la place d'un raisonnement humain au sein de la prise de décision, selon Madame Rouvroy, nous éloignerait de l'essence même de la justice. « Les nouvelles opportunités d'agrégation, d'analyse et de corrélations statistiques au sein de quantités massives de données (les *big data*), nous éloignant des perspectives statistiques traditionnelles de l'homme moyen, semblent permettre de « saisir » la « réalité sociale » comme telle, de façon directe et immanente, dans une perspective émancipée de tout rapport à « la moyenne » ou à la « normale » ou, pour le dire autrement, affranchie de la « norme » »[130].

[127] Ibid.
[128] Emmanuel Jeuland, « Justice prédictive : de la factualisation au droit potentiel », Revue pratique de la prospective et de l'innovation, dossier 9 n°15, Octobre 2017.
[129] Antoinette Rouvroy, « *Predictive policing and Rule of technology* », Webinaire IA and Law Breakfasts, organisé par le Conseil de l'Europe, le 2 juillet.2020.
[130] Antoinette Rouvroy et Thomas Berns, « Gouvernementalité algorithmique et perspectives d'émancipation – Le disparate comme condition d'individuation par la relation ? » Dans Réseaux 2013/1 (n° 177), pp 163-196.

Conclusion de la Partie I

Il est incontestable qu'au niveau global, par le constat d'une augmentation de la signification des notions de dangerosité et de sécurité, l'économie de la donnée est devenue l'outil incontournable d'un monde sous surveillance. Parallèlement à ce contexte, éclot la révolution numérique. Lorsque cette dernière rencontre le premier constat, on assiste à une « révolution dans la révolution »[131], pour reprendre les mots d'Antoine Garapon et Jean Lassègue.

La conjugaison des paramètres sécuritaire et technologique est à l'échelle mondiale déjà expérimentée, comme aux Etats-Unis et en Chine notamment. Nous avons étudié la volonté à échelle mondiale de prédire les infractions ainsi que la façon dont elles sont appréhendées par la justice, pour une paix sociale sur le long terme.

Le droit en tant que nécessité de régulation sociale afin d'« unir les droits aux devoirs et ramener la justice à son objet »[132], n'apparaît que tardivement en droit chinois. Le droit chinois est basé sur la distinction remontant à l'époque de Confucius, du ***Li,*** la vertu, la moralité et du ***Fa***, le droit[133]. Ainsi, la régulation des comportements déviants à la morale sont plus sévèrement punis et régulés par la perte de l'honneur et de la vertu, que par le droit tel que nous le connaissons aujourd'hui.

Les auteurs d'infractions pénales contreviennent au ***Li*** – la vertu. La morale n'a plus autant de poids dans la prévention des infractions. Le ***Fa*** – le droit, gagne en répression et tend à une surveillance de masse par un développement des usages de dispositifs d'IA dans l'espace public, puisque « du fait de son apparition tardive en Chine, la notion de droits de l'homme fut à peine effleurée dans la culture traditionnelle chinoise » [134] . Assistons-nous à la combinaison inédite d'un ***Li***, au sens du comportement déviant et d'un ***Fa***, au sens du droit appréhendé par l'algorithme ?

L'ensemble de ces réflexions par rapport à un futur incertain ou fictif, nous amène à nous questionner sur les risques portant sur les données à caractère personnel, découlant de ces dispositifs réels ou fictifs. S'il est « extrêmement difficile pour un profane de parvenir à faire la part des choses, de distinguer les effets d'annonce de potentielles révolutions »[135], il est également complexe de d'en dévisager les risques portant sur nos droits les plus fondamentaux, comme la protection des données à caractère personnel.

---

[131] Antoine Garapon et Jean Lassègue, op. cit., p. 139.
[132] Jean-Jacques Rousseau, « Du contrat social », 1762, Ed. GF Flammarion 2012, p.72.
[133] Li Xiaoping, « L'esprit du droit chinois : perspectives comparatistes », Revue internationale de droit comparé. Vol. 49 n°1, Janvier-mars 1997, p.17.
[134] Ru Xin, « La personne humaine dans la civilisation chinoise », PUF, n° 215, 2006, p. 77.
[135] Yannick Meneceur, « Intelligence Artificielle et droits fondamentaux », dans Patrick Gielen et Marc Schmitz, « Avoirs dématérialisés et exécution forcée », novembre 2019, Ed. Bruylant, pp.91- 92.

Partie II : L'intelligence artificielle et la protection des données à caractère personnel

Selon Antoinette Rouvroy, philosophe juridique, « ce qui paraît nous menacer, est […] la prolifération et la disponibilité même de données numériques, fussent-elles impersonnelles, en quantités massives »[136]. Les données personnelles des personnes concernées par des procédures répressives prolifèrent sur internet. Elles peuvent ainsi être recueillies à la manière d'analyse des réseaux sociaux, « *social media forensics* »[137] par exemple.

Plus généralement, l'utilisation de ces données par les dispositifs d'IA étudiés peut constituer un traitement inapproprié, et ce malgré l'intention initiale d'améliorer et renforcer l'efficacité de la prévention des infractions, d'attaques terroristes et automatiser certains raisonnements juridiques. En revanche, il est difficile de garantir l'équilibre entre les libertés individuelles et l'efficacité des services de répression utilisant les technologies. Lorsque la balance entre ces deux intérêts n'est pas stable, de vives contestations de la part de l'opinion publique peuvent en émaner au vu des conséquences sur les libertés individuelles. A titre d'exemple en France, l'affaire SAFARI en 1974. L'administration française, lors du passage à l'informatique, met au point un fichier reposant sur le numéro de sécurité sociale du citoyen. Il permet l'accès à tout un ensemble d'informations sur lui. Adrien Basdevant, lors d'une conférence rappelle que cette prise de conscience des risques pour l'Etat de droit « atteint son paroxysme »[138] à ce moment.

La difficulté aujourd'hui comme le souligne Antoinette Rouvroy, est que les données prolifèrent en quantités massives. En outre, elle souligne que le caractère personnel de la donnée perd de sa valeur, puisqu'une donnée anonymisée, si elle est croisée avec d'autres données, peut être réidentifiée. La philosophe ajoute d'ailleurs que la notion d'anonymat est « obsolète à l'heure des *Big data* »[139]. Il convient dans cette seconde partie, d'appréhender les risques issus d'un « traitement inapproprié de données personnelles » concernant les outils utilisés et étudiés en première partie de cette étude. Nous suivrons le cheminement du traitement automatisé des données en matière de répression pénale. A savoir, la collecte, l'enregistrement et l'exploitation des données (Titre 1). Il ne faudra pas occulter

---

[136] Entretien d'Antoinette Rouvroy, « Big data : l'enjeu est moins la donnée personnelle que la disparition de la personne », recueilli par Serge Abiteboul et Christine Froidevaux, Le Monde, le 22 janvier 2016.

[137] Todd Piett, « *How Law Enforcement Uses Social Media for Forensic Investigation* », 13 février 2012.

La méthode de *social media forensics* est ancienne et permets d'identifier le suspect d'une infraction par la prolifération de données sur les réseaux sociaux. A titre d'exemple, par des images d'objets volés correspondant non seulement aux objets, mais également à la date et l'heure d'un cambriolage ou encore, la localisation géographique du suspect par image ou géolocalisation de la publication.

[138] Adrien Basdevant, « Les données, la nouvelle ingénierie du pouvoir, quelles conséquences pour l'Etat de droit ? », conférence IA and Law Breakfasts, Conseil de l'Europe, le 02 décembre 2019.

[139] Entretien d'Antoinette Rouvroy, « Big data : l'enjeu est moins la donnée personnelle que la disparition de la personne », op. cit.

le contexte général de « prolifération et disponibilité même de données numériques »[140], nous amenant à réfléchir au traitement des données au-delà des frontières, en matière de coopération pénale transfrontalière notamment, nous renvoyant aux sujets de la conservation et la publication (Titre 2).

Titre I : Les risques liés à la collecte, l'enregistrement et l'exploitation des données

La Cour européenne des droits de l'Homme (CEDH) reconnaît dans sa récente décision « Breyer »[141] que dans un contexte de « lutte contre la criminalité, et en particulier contre la criminalité organisée et le terrorisme, qui est l'un des défis auxquels sont confrontées les sociétés européennes actuelles, la préservation de la sécurité publique et la protection des citoyens constituent des besoins sociaux urgents »[142]. Elle reconnaît également que « les moyens modernes de télécommunication et les changements de comportement en matière de communication exigent que les outils d'enquête des services de police et de sécurité nationale soient adaptés »[143]. En l'espèce, il s'agissait de données recueillies au sein de carte SIM pré-enregistrées par la police allemande dans un but de facilitation des investigations. Il convient de comprendre quels sont les risques liés à la protection des données issus de ces nouvelles formes de traitements en matière pénale, facilitant la collecte, l'enregistrement et l'exploitation de ces informations.

Il s'agit d'étudier la façon dont l'équilibre entre l'efficacité de la répression pénale et le respect des libertés individuelles peut être néfaste pour la protection des données personnelles. Il convient dans ce premier titre d'appréhender les risques portant sur le droit à la protection des données personnelles lors de la collecte (Chapitre 1), l'enregistrement (Chapitre 2) et l'exploitation (Chapitre 3) des données en matière d'investigation et de répression pénale.

[140] Ibid.
[141] CEDH, *Breyer c. Allemagne*, n° 50001/12, 30 janvier 2020.
[142] Ibid., §88.
[143] Ibid.

Chapitre 1 : La collecte automatique des données à caractère personnel

La collecte des données est la première étape du traitement automatisé. La collecte automatique des données à caractère personnel en matière de répression pénale fait partie de l'essence même des activités liées à la prévention, l'investigation et la répression. En effet, les données en tant que ressources se doivent d'être collectées dans un but d'information. En reprenant les mots d'Antoinette Rouvroy, la menace majeure au droit des données personnelles est « la disponibilité même de données numériques, fussent-elles impersonnelles, en quantités massives »[144]. Le caractère disponible des données, au sein de ce contexte de big data, vient accélérer la facilité avec laquelle les données sont initialement recueillies par les autorités de répression en France.

Au niveau européen, la directive UE 2016/680[145] (citée « Directive Police-Justice), régit également la collecte de données, qui doit s'effectuer dans le respect de la finalité du traitement et être licite, c'est-à-dire être « nécessaire au traitement »[146]. En matière de protection des données à caractère personnel, la licéité du traitement est remplie lorsque la personne dont les données sont recueillies est informée d'une part, et consent d'autre part à ce traitement. La collecte des données en matière pénale échappe à ces conditions, perdant leur qualité de bases juridiques du traitement des données. Dans un premier temps, il convient d'étudier le caractère illusoire du droit à l'information (Section 1) afin d'appréhender dans un deuxième temps l'affaiblissement du consentement de la collecte (Section 2).

Section 1 : L'illusion du droit à l'information du traitement des données personnelles

La CNIL définit le droit à l'information en rappelant que « toute personne a un droit de regard sur ses propres données ; par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union européenne »[147]. En matière pénale cependant, le droit à l'information n'est pas prévu, et est en

[144] Entretien d'Antoinette Rouvroy, « Big data : l'enjeu est moins la donnée personnelle que la disparition de la personne », op. cit.
[145] Directive (UE) 2016/680 du parlement européen et du conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.
[146] Art. 4 Directive Police-Justice.
[147] Définition du droit à l'information par la CNIL, https://www.cnil.fr/fr/definition/droit-linformation.

revanche le plus souvent une exception au droit à l'information de la collecte[148]. Dans un but de préservation de l'efficacité de l'enquête judiciaire en matière pénale notamment.

Si cette justification est légitime, il demeure cependant uniquement une manière d'attester de la licéité du traitement, la preuve que les données recueillies ne sont nécessaires à la finalité dudit traitement[149]. Les finalités du traitement se doivent d'être « déterminées, explicites et légitimes »[150]. Ces termes sont larges et imprécis. La difficulté de démontrer que la collecte de données personnelles ait eu lieu en dehors de la finalité précisée est d'autant plus compromise du fait que « l'absence de définition de la finalité ne peut conduire de facto à la consécration d'un principe »[151]. Par ailleurs, les fichiers de police, dont les classements alimentent ensuite des dispositifs d'IA, possèdent des finalités également larges. Prenons l'exemple du fichier TAJ (Traitement d'antécédents judiciaires), il possédait 18,9 millions de fiches de personnes en 2018[152] et sa finalité est de « faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs »[153] . Le fait d'employer des termes simples et larges serait-il une manière de faire accepter largement ce traitement à l'opinion publique ?

Ainsi, plusieurs collectes de données sont effectuées à l'insu de leurs propriétaires en vertu de finalités liées aux enquêtes et aux répressions pénales. À titre d'exemple et au vu de la disponibilité des données personnelles et de leur multiplication, l'extraction des informations par les autorités de police et de gendarmerie sur les réseaux sociaux notamment, devient une source contenant des informations souvent plus fiables que celles contenues dans un fichier de police[154], non mis à jour régulièrement. Les autorités procèdent à une réelle analyse approfondie des données, « *data mining* » des réseaux sociaux afin de détecter les acteurs importants d'un réseau criminel (*centrability analysis*), son groupe et les personnes liées à son réseau (*community detection*), la propagation de l'information criminelle (*information diffusion*) et enfin les liens entre ces éléments (*link prediction*).[155].

Par ailleurs, le droit à l'information d'un traitement par des dispositifs d'IA tend à devenir de plus en plus présent. C'est le cas du recours aux dispositifs de reconnaissance faciale invisibles à l'œil nu au

---

[148] Art. 42§2 Règlement « SIS II », Règlement (CE) nº 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), JO L 381, 28 décembre 2006.
[149] Article 4, 1, b, Directive Police-Justice.
[150] Ibid. ; Article 4, 2, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (citée « Loi informatique et libertés »).
[151] David Larbre, « Les fichiers de police : une catégorie juridique incertaine ? », Les libertés à l'épreuve de l'informatique : : fichage et contrôle social, 15ème colloque Creis-Terminal, 2011, pp. 141 – 151.
[152] CNIL, « TAJ : traitement d'antécédents judiciaires », 15 novembre 2018.
[153] Article 230-9 du code de procédure pénale.
[154] Cf. Partie I, Titre I, Chap. 2, S1.
[155] Mohammad A. Tayebi, Uwe Glässer, « Social network analysis in predictive policing », Concepts, Models and Methods, Ed. Springer Switzerland, 2016, p.9.

sein d'aéroports notamment. Bertrand Pailhes, directeur des technologies et de l'innovation à la CNIL, rappelait ce contraste d'information « en comparaison avec le nombre de fois où l'on scanne son passeport à l'aéroport, puisque la friction permet à l'individu d'être informé du traitement de ses données, or en matière de reconnaissance faciale ça n'est pas le cas »[156]. La reconnaissance faciale remet également en jeu la question du consentement.

Section 2 : L'absence de consultation du consentement de l'individu concerné

Le consentement au traitement est renforcé en 2018 par l'entrée en vigueur du RGPD notamment. Le consentement devient l'emblème pour les entreprises notamment d'un gage de qualité et de respect des données à caractère personnel[157]. La question du consentement de l'individu concerné ne constitue pas une base juridique du traitement[158].

Par ailleurs, au sein de la directive Police-Justice à titre d'illustration, le terme consentement n'apparaît qu'une seule fois, à l'occasion de rappeler son exclusion en la matière. *« Dans ce cas, le consentement de la personne concernée, au sens du règlement (UE) 2016/679, ne devrait pas constituer une base juridique pour le traitement de données à caractère personnel par les autorités compétentes. Lorsqu'elle est tenue de respecter une obligation légale, la personne concernée ne dispose pas d'une véritable liberté de choix »*[159]. En plus de ne pas être une base légale du traitement des données personnelles, le refus pour un individu suspect, de remettre ses données personnelles est punissable pénalement. En effet en France, le prélèvement de données est « nécessaire à la réalisation d'examens techniques et scientifiques de comparaison avec les traces et indices prélevés pour les nécessités de l'enquête »[160]. L'individu s'opposant à la relève de ses données est puni d'un an d'emprisonnement et de 15 000€ d'amende. Cela est problématique au vu du traitement davantage automatisé de ces données.

Une exception à la règle apparaît lorsqu'il est question de prélèvement des données dites « particulièrement sensibles »[161] dont font parties les données biométriques[162]. Le prérequis du consentement dans ce cas particulier démontre la volonté du législateur et des organismes protecteurs

---

[156] Bertrand Paihles, Session parlementaire européenne du 20.02.2020 sur « L'intelligence artificielle au sein de la justice pénale et son utilisation par la police et les autorités judiciaires en matière pénale ».
[157] Antoinette Rouvroy et Anne Debet, « Protection des données personnelles : souriez, vous être traqués », émission la méthode scientifiques par Nicolas Martin sur France culture du 23 mai 2018 : Elles expliquent la volonté massive des sociétés collectant des données personnelles - à des fins commerciales notamment -, de s'assurer par l'envoi d'e-mails, que leurs clients étaient consentant au traitement de leurs données. Cela est apparu ironique puisqu'à partir du moment où les sociétés possèdent les adresses e-mails de leurs clients, elles collectent d'ores-et-déjà leurs données personnelles.
[158] Article 8 Directive Police-Justice : le consentement n'apparaît pas dans les conditions de licéité du traitement.
[159] Cons. 35 Directive Police-Justice. Passage souligné par mes soins.
[160] Art. 55-1 Code français de procédure pénale.
[161] Cons. 37 Directive Police-Justice.
[162] Cf. Partie I, Titre I, Chap. 3.

des données personnelles, de mettre en balance les intérêts des individus concernés et ceux des autorités d'enquêtes et de répression. La crainte du recours aux dispositifs d'IA prévaudrait-elle sur les situations où les données sont collectées à des finalités non précises, moins dangereuses ? La sensibilité du débat au niveau européen est également ressenti. La marge de manœuvre permettant aux Etats membres d'imposer le consentement de l'intéressé avant toute collecte d'ADN notamment, est présente au sein d'un considérant de la directive Police-Justice[163]. Le considérant d'un texte européen est important, « c'est la seule trace de l'historique et du pourquoi du texte des articles qui suivent »[164]. En outre, le concept du consentement n'est mentionné uniquement dans ce considérant. Le silence de l'UE à ce sujet est démonstratif de l'importance de ce débat.

Pour l'instant, le cadre normatif français, restreint l'utilisation de la reconnaissance faciale aux situations nécessitant le consentement des individus. Pour toute expérimentation par les autorités de police ou de gendarmerie, d'un dispositif de reconnaissance faciale, en matière de prévention des infractions notamment, le consentement des personnes testées est à obtenir. Ce fut le cas dans la ville de Nice, lors de la 135è édition du Carnaval en 2019, dont l'expérimentation de reconnaissance faciale « a reposé sur la base de licéité du consentement »[165]. Pour Sandra Bertin ayant participé à la mise en place de l'expérimentation à Nice, il est regrettable que cette expérience utilisant des données par des dispositifs d'intelligence artificielle soit encadrée par une loi datant de 1978 « plus adaptée au contexte actuel »[166]. Il est incontestable qu'il peut être frustrant de restreindre l'utilisation des dispositifs d'IA plus performants que la surveillance par des policiers. Cela peut paraître être incohérent « avec la société dans laquelle nous évoluons »[167]. Madame Bertin conçoit cependant que les risques liés à la présence de ces dispositifs au sein de l'espace public ne sont pas négligeables.

La CNIL est également consciente de l'efficacité des dispositifs d'IA, notamment en matière de reconnaissance faciale, mais rappelle cependant depuis septembre 2018 le besoin de « faire des **choix politiques** : sur le rôle dévolu à la technologie, sur ses effets sur les libertés fondamentales des individus, sur la place de l'humain à l'ère numérique »[168]. Il s'agit en effet de trouver le « juste équilibre entre les impératifs de sécurisation, notamment des espaces publics, et la préservation des droits et libertés de chacun »[169]. Si les expérimentations menées en France se sont déroulées de manière à mettre en avant l'efficacité des dispositifs d'IA en matière de prévention et de répression

---

[163] Cons. 35 Directive Police-Justice.
[164] Axel Beelen, « Directive œuvres orphelines : de l'importance des considérants », 2012.
[165] Sandra Bertin, directrice de la police municipale de Nice, interviewée dans le cadre de ce mémoire. L'interview est disponible en annexe.
[166] Ibid.
[167] Ibid.
[168] CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019.
[169] CNIL, « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », le 19 septembre 2018.

des infractions, c'est avant tout parce qu'un encadrement strict de ces expérimentations était nécessaire. Aussi, la présence d'expérimentations de ce type conforte l'idée que dans un futur proche ces dispositifs d'IA, mieux connus des autorités pénales, seront mis en application et encadrés de manière moins stricte qu'aujourd'hui. La Commission européenne, dans son livre blanc consacré à l'intelligence artificielle, publié le 19 février dernier, énonce notamment avoir pour projet d'établir « un vaste débat européen sur les circonstances particulières, le cas échéant, qui pourraient justifier une telle utilisation, ainsi que sur les garanties communes à mettre en place »[170].

L'effet pervers d'une tendance à supprimer le consentement des individus concernés lors de l'utilisation de ces dispositifs d'IA est de tomber dans un « paradigme de la surveillance »[171]. Bertrand Pailhes évoque également la notion d'« ubiquité de la reconnaissance faciale »[172] selon laquelle, les dispositifs de reconnaissance faciale deviendraient omniprésents. Cette idée est corrélée au concept « de disponibilité en quantités massives » mentionnée par Antoinette Rouvroy. En effet, le risque de la combinaison de l'omniprésence des données et des dispositifs de reconnaissance faciale conduirait à ce que les données soient disponibles partout et collectées à l'insu des personnes en vertu de la prévention et la répression des infractions pénales.

L'étape de la disponibilité des données est déjà atteinte, et celle de l'ubiquité de la reconnaissance faciale est déjà présente dans plusieurs Etats. C'est le cas en Chine où les individus obtiennent des notes sociales en fonction de leurs comportements. Monsieur Pailhes mentionne également l'utilité dans ce futur aussi proche qu'incertain, d'un « droit fondamental de l'anonymat dans l'espace public »[173].

---

[170] Commission européenne, livre blanc « *Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance* », Bruxelles, le 19 février 2020, p. 26.
[171] Bertrand Paihles, op. cit.
[172] Ibid.
[173] Ibid.

Chapitre 2 : L'enregistrement et la structuration des données dans l'IA

Une fois les données collectées à des fins de répression pénale, le responsable du traitement procède à l'enregistrement et la structuration des données au sein de l'IA. La structuration permet l'utilisation de la donnée « sous forme parfaitement adaptée à une base de données classique »[174]. Seulement, de moins en moins de données numériques sont structurées, du fait que le *big data*, technique algorithmique de traitement de données massives, est capable de les traiter. Adrien Basdevant et Jean-Pierre Mignard réagissent également au fait que ces données « peu structurées et très souvent incomplètes » [175] soient traitées par le *big data* qui « identifie les répétitions, modélise les comportements et sélectionne les schémas applicables, procédant par corrélation » [176]. Cette mécanique d'analyse conjuguée à une étude algorithmique par corrélation est susceptible de nuire à l'intégrité mêmes des données (Section 1). Ce risque est parfois rendu imprévisible et incontrôlable par la limitation du droit à l'accès aux données en matière de répression pénale notamment (Section 2).

Section 1 : Les nuisances à l'intégrité des données des personnes suspectes ou prévenues

L'intégrité d'une donnée peut être définie comme la « qualité d'un document ou d'une donnée qui n'a pas été altéré. Dans le monde numérique, un document ou une donnée est réputé intègre si son empreinte à un temps t+1 est identique à l'empreinte prise à un temps t »[177]. L'altération de la donnée peut s'étendre à « la perte, la destruction ou les dégâts d'origine accidentelle »[178].

Les données des suspects ou prévenus, pourraient perdre de leur valeur ou de leur sens lors d'un traitement de données par corrélation algorithmique au cœur d'un dispositif d'IA. La corrélation algorithmique peut entraîner des altérations à l'intelligibilité et à l'interprétabilité des données de l'individu concerné. D'une part, le dispositif d'IA peut comprendre des difficultés au sein même de son fonctionnement (§1). D'autre part, il est possible que des éléments tiers à l'algorithme viennent tromper son raisonnement sans que le dispositif de calcul ne puisse les repérer (§2).

---

[174] Viktor Mayer-Schönberger et Kenneth Cukier, « Big data : la révolution des données est en marche », Ed. Robert Laffont, 2013.
[175] Adrien Basdevant et Jean-Pierre Mignard, op. cit., p. 63.
[176] Ibid.
[177] Référentiel General de Gestion des Archives R2GA, Octobre 2013, p. 63.
[178] Art. 4, 1, f) Directive Police-Justice.

§1. Les difficultés inhérentes au dispositif d'IA

La corrélation algorithmique est intrinsèquement opposée au raisonnement juridique syllogistique. Il s'agit de l'une des raisons pour lesquelles des dispositifs d'IA ne pourraient complètement remplacer un juge humain, puisque la logique déductive devient inductive[179]. En outre, des corrélations algorithmiques sont utilisées par les autorités de police, notamment les logiciels d'apprentissage automatique en matière de résolution d'enquêtes[180]. Il est essentiel de s'intéresser dans un premier temps à la notion de reconnaissance de formes, « *pattern recognition* » (a), pour ensuite comprendre le processus dans lequel le dispositif d'IA est amené à corréler des données de manière erronée (b).

a. Les difficultés de la reconnaissance de formes

La reconnaissance de formes, procédé inhérent à certains dispositifs d'IA, est une « technique d'analyse par ordinateur d'un ensemble de données (photographies, dessins, etc.) en vue d'y trouver des configurations particulières spécifiées »[181].

Il s'agit concrètement de repérer des motifs informatiques au sein de données brutes. Dans le cadre de résolution d'enquêtes, cela est utilisé lors des reconnaissances d'empreintes vocales, faciales, manuscrites et digitales. La reconnaissance vocale est d'autant plus importante depuis que les conversations téléphoniques peuvent être transmises aux autorités supervisant les dispositifs d'IA afin de résoudre des enquêtes. Les difficultés auxquelles peuvent-être confrontées les techniques de reconnaissance de formes sont liées au degré d'intelligibilité du motif informatique devant être calibré avant de pouvoir être lu.

Professeur Philippe Muller[182] compare cette difficulté de calibrage avec la distinction biologique entre la part infime d'ADN codant et de la majorité d'ADN non codant que l'on retrouve dans le génome humain. Cette dernière représente « un diagramme représentant la position relative des gènes (séquences d'ADN) sur un chromosome et les distances entre ces gènes. La molécule d'ADN est une suite de séquences de petites molécules (les nucléotides) dont il existe 4 sortes abrégées en A C G T »[183]. Parmi ce digramme, seulement une infime partie est dite « codante », c'est-à-dire traduite en protéine. Elle représente uniquement 1/4.000.000e du segment de gène[184]. Il est difficile de rendre intelligible cette donnée biométrique, pour tout professionnel traitant des séquences d'ADN.

---

[179] Adrien Basdevant et Jean-Pierre Mignard, op. cit., pp.63-64.
[180] Cf. Partie I, Titre I, Chap. 2, S2.
[181] Définition Larousse : https://www.larousse.fr/dictionnaires/francais/reconnaissance/67116.
[182] Philippe Muller, « Intelligence artificielle et reconnaissance de formes », Institut de recherche en informatique de Toulouse, 27 mars 2014.
[183] Philippe Muller, op. cit., p. 24.
[184] Ibid

En d'autres termes, les séquences intelligibles d'une empreinte ne représentent en réalité, qu'une infime partie de cette dernière et cela rend difficile la reconnaissance de formes. En revanche, afin de contourner cette contrainte, il convient de former de bonnes séquences avec minutie.

Le professeur Muller prend alors l'exemple de la reconnaissance d'une empreinte vocale, inhérente aux algorithmes de gendarmerie dans le cadre d'écoute téléphonique au cours d'une enquête notamment. Ci-après, l'exemple de reconnaissance d'empreinte vocale, aussi intitulé « analyse et paramétrisation de la parole »[185]. L'image témoigne de la découpe des séquences d'une empreinte vocale, polluée de plusieurs nuisances sonores, appelées « bruits ». Une fois tous les bruits soustraits de l'enregistrement, la séquence lisible est minime.

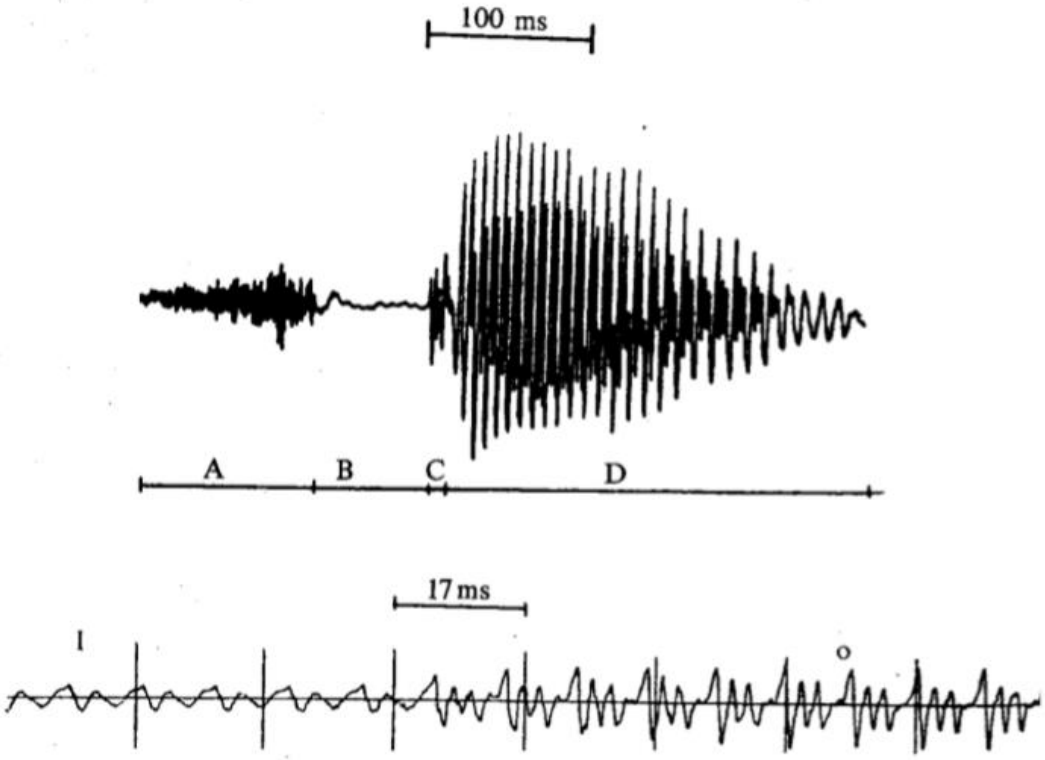


FIG. IX.1. — *Le signal vocal.* A : aléatoire, B : bruit, C : impulsion, D : pseudo-périodique. Mot prononcé en haut /ski/, en bas, syllabe prononcée /lo/ signal plus détaillé.

La parole est paramétrée afin qu'uniquement les séquences lisibles puissent être recueillies et lues par l'algorithme. Ce type de paramétrage est également effectué en matière de reconnaissance d'empreintes faciale, manuscrite et digitale. Les algorithmes utilisés en matière de résolution d'enquêtes, s'améliorent par la méthode d'apprentissage. En revanche, bien qu'ils demeurent supervisés, le risque 0 n'existe pas. Ainsi, la difficulté de reconnaissance de formes s'ajoute à la complexité de la lecture des données du fait de leur quantité massive. Par ailleurs, les données peuvent être corrélées de manière erronée.

[185] Schémas : Philippe Muller, op. cit., pp. 29-30.

b. La présence de « corrélations fallacieuses »[186]

Les données peuvent être corrélées de manière incorrecte, il s'agit des corrélations fallacieuses, traduit de l'anglais « *spurious correlations* »[187]. Elles apparaissent du fait d'une analogie hasardeuse de la part de l'algorithme. Les dispositifs d'IA étudiés en première partie sont amenés à traiter des quantités massives de données et cela est une de leurs caractéristiques. En revanche, l'idée que cette quantité de données puisse légitimer le raisonnement de ces outils de calcul est souvent avancée à défaut[188].

Par ailleurs, le fait que le nombre de données soit élevé ne garantit pas un meilleur résultat, ni une meilleure efficacité de l'algorithme[189]. Le problème est souvent issu d'une tendance combinatoire infinie créant ainsi des possibilités de résultats et de corrélations infinis, n'ayant parfois plus de sens. Le professeur Muller emploi le terme d'« explosion de possibilités » et le rapproche au domaine des jeux de société, comme les échecs ou le morpion. Ce domaine permet en effet de toujours retrouver dans une base de données une corrélation plausible et légitime « toute "base de données" (ensemble de nombres) suffisamment grande (avec au moins m éléments), même produite au hasard (des lancements de dés), contient des régularités avec les caractéristiques demandées – dans énormément de nombres on trouve donc ‘‘n'importe quoi’’, mieux : ‘‘ce que vous vouliez, a priori’’ »[190].

En revanche, reprendre en matière pénale une combinaison infinie entre les données représente un danger pour tout individu suspect ou prévenu. En effet, une mauvaise corrélation pourrait conduire un individu à être suspecté ou condamné pour une infraction qu'il n'a pas commise. Plusieurs défaillances au sein de dispositifs d'IA ont déjà été constatées, en matière de reconnaissance visuelle notamment.

Une étude de l'Université de Cornell [191] a testé l'efficacité d'un algorithme en matière de reconnaissance visuelle, en intégrant des images réelles et non modifiées, ainsi que des images volontairement altérées afin de tester sa fiabilité. L'algorithme en question est intitulé « DenseNet-121 ». Le résultat de l'expérience démontre que l'algorithme n'a réussi à reconnaître que 2% des

---

[186] Dominique Cardon, « *A quoi rêvent les algorithmes ? Nos vies à l'heure des big data* », La république des idées, Ed. Seuil Paris, 2015.
[187] Tyler Vigen, « Spurious correlations – correlation does not equal causation », Ed. Hachette Books, 2015.
[188] Chris Anderson, « *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete* », Wired Magazine, 2008 : « plus on a de données, plus les corrélations, que seule une machine peut trouver, permettront d'agir – point besoin de comprendre ».
[189] Yannick Meneceur, « *Quel avenir pour la justice prédictive* », la Semaine Juridique, Ed. Lexis Nexis, n°7, le 12 février 2018, p.318.
[190] Calude, C., Longo, G. « *The deluge of Spurious Correlations in Big Data* ». In Foundations of Science, 2017, vol. 22, 3, pp 595–612.
[191] Dan Hendrycks, Kevin Zhao, Steven Basart, Jacob Steinhardt, Dawn Song, « *Natural Adversarial Examples* », Univerisity of Cornell, 16 juillet 2019.

éléments demandés en ayant une baisse de précision de 90%. Cette expérience permet de comprendre que les algorithmes présents au sein des dispositifs d'IA utilisés, dont ceux utilisés en matière de répression pénale, pourraient en raison de lacunes importantes de précision, confondre deux individus par exemple.

Effectivement, une étude concernant les risques de corrélations erronées a été menée aux Etats-Unis et une exposition à des fins de préventions contre ces risques a été présentée aux membres du Congrès[192]. Cette étude a notamment explicité les risques de confusion d'individus ayant la même couleur de peau. Par ailleurs en Europe, 81% des personnes interpellées lors de l'expérience menée par les autorités londoniennes[193], étaient innocentes et leur visage a été confondu avec ceux de personnes réellement recherchées. En outre, l'intégrité des données peut se voir altérée par des causes extérieures au fonctionnement de l'algorithme.

§2. Les difficultés tierces à l'algorithme : « *Garbage in, garbage out* »

Il existe plusieurs causes de nuisances à l'intégrité des données au sein d'un dispositif d'IA. Il convient de reprendre l'adage utilisé en matière de science informatique : « *garbage in, garbage out* », selon lequel si les données intégrées au sein de l'algorithme sont de mauvaise qualité ou déjà erronées, le résultat ne sera meilleur. Il s'agit d'étudier quelques exemples de causes pouvant nuire à la qualité des données introduites dans l'algorithme, pouvant ensuite compromettre le résultat d'un dispositif d'IA en matière de répression pénale.

Dans le cas des dispositifs de reconnaissance visuelle, notamment par le cas de la perception des couleurs des vêtements des personnes au comportement déviant[194], si la qualité des images introduites au sein de l'algorithme est médiocre, il est possible que la personne soit confondue avec d'autres individus. Par ailleurs, les autorités de police ou de gendarmerie peuvent parfois saisir des données provenant des réseaux sociaux au sein de leurs bases de données, pour plus tard traiter ces informations en matière de cartographie infractionnelle. En revanche, il existe sur les réseaux sociaux plusieurs personnes possédant les mêmes noms et prénoms. Ainsi, un risque de confusion subsiste.

L'aspect probabiliste de la reconnaissance faciale demeure un enjeu lié à l'intégrité de la donnée également. En effet, les images collectées sont ensuite transformées en gabarits par la suite comparés avec un niveau de certitude. Il existe notamment des possibilités de remplacer le visage d'une personne par celui d'une autre grâce à la méthode de *deep learning*, le « *deep fake* ». Aussi, une

[192] Neema Giuliani (Union américaine pour les libertés civiles) et Claire Garvie (Chercheuse à l'Université de Georgetown), dans le reportage « Tous surveillés : 7 milliards de suspects », diffusé sur la chaîne Arte, le 21 avril 2020.
[193] Cf. Partie 1, Titre 1, Chap. 3.
[194] Ibid.

technique de création d'un visage inexistant en réalité est également déjà possible[195]. Face à autant de techniques nuisibles à l'intégrité des données, il convient de s'intéresser aux garanties normatives permettant un équilibre entre l'intérêt de la prévention et la répression des infractions par l'utilisation de l'IA et le droit à l'intégrité des données personnelles.

Section 2 : Les limites aux garanties normatives de protection de l'intégrité des données

En réponse à ces risques nuisibles à l'intégrité des données un cadre normatif national et européen est érigé. En revanche, il est incontestable que ces droits présents au sein de la protection générale des données à caractère personnel, sont limités en matière pénale, puisqu'il convient de conserver l'efficacité de la justice pénale. Pour ce faire, des limites à cette protection des données personnelles sont instaurées, au sein même des garanties individuelles du respect de l'intégrité des données (§1) et du droit d'accès aux données collectées (§2).

§1. L'impuissance de la garantie du respect de l'intégrité des données

Le droit à l'intégrité des données personnelles des personnes faisant l'objet d'une répression pénale est légèrement mentionnée au sein de la directive Police-Justice[196]. Elle est présente à l'article relatif au principe de sécurité du traitement automatisé, au sein duquel, la protection de l'intégrité est mise en exergue par la garantie que les « données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système »[197]. En revanche, il est incontestable qu'une marge de manœuvre est laissée aux Etats membres[198] et cela contribue d'une part à une hétérogénéité normative et d'autre part à l'insécurité du traitement automatisé des données des personnes en situation de répression pénale.

Effectivement, on assisterait au risque que l'intégrité des données soit placée au second plan lorsque sont concernées les données d'un suspect ou d'un prévenu, par application stricte de l'obligation étatique de protection et prévention des infractions. C'est l'idée qu'énonce Olivier De Schutter lorsqu'il estime que « la notion d'obligation sert précisément à intégrer cette notion d'aléa »[199]. Professeure Geneviève Giudicelli-Delage prend l'exemple des mesures carcérales afin de démontrer le déploiement massif de mesures à l'encontre de l'intégrité tant physique de l'individu détenu, que celle de ses données : « un ensemble plus vaste où se développent […], une radicalisation des mesures

---

[195] Le site internet « This person does not exist » génère à chaque rafraichissement de la page un nouveau visage totalement fictif, https://thispersondoesnotexist.com/.
[196] Cons. 59 : le responsable de traitement doit être capable de prouver le respect de l'intégrité des données.
[197] Art. 29, 2, j. Directive Police-Justice.
[198] Considérants 33 Directive Police-Justice : Les dispositions des Etats membres doivent contenir des précisions au sujet des modalités de traitement, notamment l'intégrité des données.
[199] Olivier de Schutter, « *Fonctions de juger et droits fondamentaux. Transformation du contrôle juridictionnel dans les ordres juridiques américains et européens* », Bruylant, Bruxelles, 1999, p. 383.

de surveillance, un maillage de plus en plus étroit des fichiers de bases de données personnelles permettant une traçabilité individuelle, au nom de la dangerosité et du risque »[200]. En ce qui concerne les personnes suspectes ou prévenues, il convient de comprendre l'étendue du droit d'accès aux données personnelles et ses limites.

§2. Les limites du droit à d'accès aux données personnelles

Les données personnelles utilisées, lorsqu'elles sont sujettes à un traitement automatisé, font l'objet de certains critères de qualité[201] et de mesures de sécurité[202]. Elles doivent être assorties de garanties particulières si elles sont sensibles[203], et assurent aux personnes concernées par l'existence de ces fichiers l'accès à ces derniers, la rectification de leur données personnelles et un recours effectif[204].

Le droit d'accès aux données personnelles permet à la personne suspecte ou prévenue, concernée par une collecte de ses données personnelles, de pouvoir avoir connaissance de leur nature, et ainsi de pouvoir par la suite, contester une décision prise sur la base de ces données par exemple. Ce droit est prévu au sein de la directive Police-Justice[205] et une limite à ce droit est également prévue[206]. Cette limite constitue une ingérence au sein de la vie privée de l'individu – dont fait partie la protection des données personnelles – telle que définie par l'art. 8§1 de la ConvEDH, et peut être justifiée par des éléments dont l'intérêt est supérieur au droit d'accès[207]. En effet, la personne concernée par la collecte et le traitement des données peut voir son droit d'accès aux données collectées disparaître. Deux raisons principales s'opposent légitimement à ce droit. D'une part, lorsqu'une « telle limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique »[208]. D'autre part, afin de ne pas nuire aux travaux des autorités répressives et ainsi procéder à un équilibre entre le bon déroulement de ces travaux et la sauvegarde du droit fondamental à la protection des données.

L'art. 8§2 de la ConvEDH dispose qu'une ingérence est justifiée si elle est prévue par la loi[209], qu'elle poursuit un but légitime[210] et que la mesure en question est nécessaire dans une société démocratique.

---

[200] Geneviève Giudicelli-Delage, « *La dangerosité saisie par le droit pénal* », PUF, IRJS Éditions, Paris, 201.
Voir aussi : Anne Simon, « *Les atteintes à l'intégrité des personnes détenues imputables à l'Etat : contribution à la théorie des obligations conventionnelles européennes : l'exemple de la France* », Thèse universitaire, Université Panthéon Sorbonne, le 4 décembre 2013, pp. 140-141.
[201] Art. 5 Convention 108.
[202] Art. 7 Ibid.
[203] Art. 6 Ibid.
[204] Art. 8 Ibid.
[205] Art. 14 Directive Police-Justice.
[206] Art. 15 Ibid.
[207] Art. 8§2 ConvEDH.
[208] Ibid.
[209] CEDH, *Malone c. Royaume-Uni*, le 2 août 1984, req.n° 8691/79, §66 ; CEDH, M*agyar Ketfakru Kutya Part c. Hongrie* [GC], req. n°201/17, 20 janvier 2020. §93.
[210] CEDH, *Mozer c. République de Moldova et Russie* [GC], req. n° 11138/10, 23 février 2016. §193.

Il convient d'admettre que la base légale et le but légitime en matière de répression pénale sont majoritairement rencontrés, notamment en vertu de la place significative des concepts de dangerosité et de risque, développé dans le paragraphe précédent.

En revanche, afin que l'ingérence réponde à une « nécessité dans une société démocratique », les motifs invoqués doivent être « pertinents et suffisants »[211]. Le caractère de ces motifs est subjectif et ainsi, complexe à interpréter.

La CEDH, reconnait que le droit d'accès aux données n'est pas absolu[212]. Ce raisonnement est notamment repris et justifié par une protection contre toute duperie de l'algorithme, si l'individu a accès aux données traitées, puisqu'il pourrait avoir accès au fonctionnement de ce dernier[213]. L'opacité des algorithmes présents au sein des dispositifs d'IA utilisés par les autorités répressives constitue un risque pour la protection des données personnelles. D'une part, de manière directe, du fait que la personne suspecte, n'a pas connaissance du fonctionnement de l'algorithme, et n'est pas consciente des données réellement collectées. D'autre part, de manière indirecte, au vu de la limitation des recours à la disposition des personnes concernées par une décision prise à l'aide de dispositifs d'IA.

[211] *S. et Marper c. Royaume-Uni* [GC], §101 ; CEDH, *M.K c. France, req. n° 19522/09, 18 avril 2013.*, §33.
[212] CEDH, *Godelli c. Italie*, req. n°33783/09, 25 septembre 2012, §47 : notamment lorsqu'il existe des intérêts concurrents ; CEDH, *Odièvre c. France [GC]*, req. n°42326/98, 13 février 2003, §40 ; CEDH, *Leander c. Suède*, n°9248/81, 26 mars 1987, §67.
[213] Jesse Beatson, « AI-supported adjudicators : should artificial intelligence have a role in tribunal adjudiction », Canadian Journal of Administrative Law & Practice, Ed. Carswell, vol. 31-3, Toronto, 2018, pp. 25-26.

Chapitre 3 : L'exploitation des données et l'utilisation du résultat fourni par l'IA

Lorsque les données traitées par un dispositif d'IA au sein d'une autorité répressive sont utilisées à des fins décisionnelles, l'individu concerné est confronté à l'opacité du dispositif d'une part et à la difficulté de contestation de cet outil d'autre part. Ces dispositifs conçus et développés par des sociétés privées et non par des professionnels du droit s'introduisent au sein de la justice. Le risque est alors « une privatisation de la justice, et ainsi une déjudiciarisation. On parle de choc de souveraineté, car le citoyen n'a pas de corps représentant au sein de cette situation où ses données sont collectées »[214]. Il est intéressant de comprendre quels sont les enjeux de l'opacité d'un dispositif d'IA au sein d'une autorité répressive susceptible de prendre une décision basée partiellement sur le résultat de l'algorithme (Section 1). Afin d'étudier les possibilités pour l'individu concerné, de s'opposer à une telle décision (Section 2).

Section 1 : Les enjeux de l'opacité des dispositifs entraînant une décision de répression

Il convient d'appréhender les risques issus d'une prise de décision répressive par ces dispositifs d'IA (§1) afin d'étudier l'importance et la complexité de mise en place du droit à l'explication du fonctionnement de l'algorithme utilisé (§2).

§1. Les risques des dispositifs d'IA participant aux décisions à caractère répressif

Des dispositifs d'IA utilisés lors des patrouilles et d'enquêtes judiciaire émane la possibilité d'interpellation d'individus suspects et d'autres formes de décisions privatives de liberté. Les risques des décisions à caractère répressif proviendraient de plusieurs erreurs de programmation de l'algorithme que certains auteurs nomment *miscodes*[215]. Il s'agit d'un terme large couvrant « les erreurs, les biais ou les manipulations dans les algorithmes qui ont un impact sur le résultat en termes de précision, de validité et de légalité »[216].

Des situations entraînant d'importants risques sont d'ores et déjà présentes en Europe. En 2019, un logiciel développé par une entreprise privée et vendu à l'Etat italien, en tant qu'aide aux enquêtes criminelles, a participé à l'interpellation erronée de plus de 1000 italiens[217]. Des chercheurs ont étudié d'où pouvait provenir la faille du logiciel appelé « Exodus ». L'étude démontre qu'il manquait à « Exodus » une procédure de validation de la cible à cause d'un problème de programmation[218].

---

[214] Adrien Basdevant, « Les données, la nouvelle ingénierie du pouvoir », op. cit.
[215] Francesca Palmiotto, « *The Black Box on trial : The impact of Algorithmic Transparency on Fair Trial Rights in Criminal Proceedings* », dans Martin Ebers and Marta Cantero-Gamito (eds.) *Algorithmic Governance and Governance of Algorithms*, Ed. Springer, à paraître en octobre 2020.
[216] Ibid.
[217] 'Più di mille italiani intercettati sul cellulare, per errore, da un hacker di Stato' La Repubblica, 30 mars 2019.
[218] Francesca Palmiotto, op. cit., p.3.

Concrètement, le logiciel n'a pas vérifié si le téléphone mobile dans lequel il devait être installé allait être légalement interpelé. En effet, en Italie, l'intrusion au sein d'un dispositif personnel est illégale, sauf autorisation par le juge. Le résultat de l'algorithme a alors autorisé les autorités de police d'interpeller des citoyens de manière totalement illégale, dont certains étaient innocents.

Au niveau international, plusieurs Etats fédérés des Etats-Unis utilisent le logiciel COMPAS[219], permettant de déterminer la susceptibilité pour un prévenu de récidiver, pour assister le juge dans la détermination du *quantum* de la peine. En revanche, des chercheurs de la société ProPublica[220] ont étudié les biais de cet algorithme, utilisé notamment lors d'une décision phare en matière d'aide algorithmique à la décision, *Loomis c. Wisconsin*[221]. En 2016, l'étude de ProPublica démontre que les résultats analysant la probabilité de récidive par l'algorithme COMPAS sont discriminants envers les personnes de couleurs. L'algorithme n'ayant évidemment pas le sens des discriminations, il est important de rappeler qu'il peut reproduire les discriminations déjà préexistantes, voir les généraliser[222]. Il convient pour cela, de renvoyer le lecteur au raisonnement « *garbage in, garbage out* » du chapitre précédent. En revanche, ces biais peuvent être issus de la phase d'apprentissage de l'algorithme, soit, lors de sa programmation. L'algorithme du logiciel COMPAS fût entraîné avec un jeu de données du comté de Broward en Floride, dont le taux de discrimination est particulièrement élevé. Lorsque le juge d'un autre Etat l'utilise, les données initialement intégrées dans COMPAS lors de son apprentissage peut biaiser son raisonnement et augmenter le taux de discrimination au sein de l'Etat[223].

Ainsi, il est important de ne pas occulter la présence de risque au sein des algorithmes assistant une prise de décision, afin de garantir une meilleure administration de la justice. En revanche, il conviendrait de permettre une meilleure visibilité du fonctionnement de ces derniers et une supervision plus prononcée face aux risques inhérents à ces logiciels. Seulement, des limites à ce droit à l'explication du fonctionnement de l'algorithme subsistent.

Voir aussi : Security without Borders, « *Exodus: New Android Spyware Made in Italy* », 2019.

[219] « Correctional Offender Management Profiling for Alternative Sanctions », Profilage des délinquants en milieu correctionnel pour les sanctions alternatives.

[220] Julia Angwin et Jeff Larson, « *How We Analyzed the COMPAS Recidivism Algorithm* », ProPublica, 23 Mai 2016.

[221] Cour Suprême des Etats-Unis, *Loomis c. Wisconsin*, op. cit.

Voir aussi : Sabine Gless, Wolfgang Wohlers, *Subsumstionsautomat 2.0 – Künstliche Intelligenz statt menschlicher Richter ?*, dans Böse Martin, Schuman Kay H., Toepel Friedrich, Festschrift für Urs Kindhäuser, Ed. Nomos, 2019.

[222] Institut Montaigne, « Algorithmes : contrôle de biais S.V.P », Mars 2020, p.18.

[223] Ibid., p. 23.

§2. La complexité de mise en place du droit à l'explication du fonctionnement de l'algorithme

Les algorithmes utilisés au sein de décisions à caractère répressif, sont de véritables boîtes noires, venant du terme *black box* repris par Franck Pasquale notamment. Ce dernier décrit le concept de *black box* comme une « situation où l'on peut observer les inputs (entrées) et outputs (sorties) d'un algorithme, mais on ne peut pas savoir comment l'un devient l'autre »[224]. Le concept de *black box* correspond alors au terme d'opacité algorithmique.

Cette opacité est un obstacle à la compréhension du fonctionnement de l'algorithme par le suspect ou prévenu dont les données ont été collectées et perturbe le droit à un procès équitable, certes. En outre, en matière de données personnelles, cette opacité algorithmique va à l'encontre du principe de transparence du traitement des données, concept clé du droit à la protection des données personnelles[225] et lié à la limitation de la finalité du traitement étudiée au premier chapitre de ce deuxième titre.

L'Union européenne démontre avoir pris conscience des risques de la décision *Loomis* précitée, prenant la forme d'un traitement inapproprié des données, pouvant aller jusqu'à la discrimination de l'individu concerné. En effet, l'organisation mentionne au sein du considérant 38 : *« La personne concernée devrait avoir le droit de ne pas faire l'objet d'une décision impliquant l'évaluation de certains aspects personnels la concernant, qui est prise sur le seul fondement d'un traitement automatisé […] un traitement de ce type devrait être assorti de garanties appropriées, y compris la fourniture d'informations spécifiques à la personne concernée et le droit d'obtenir une intervention humaine, en particulier d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation ou de contester la décision »*. L'article 11 de la directive Police-Justice interdit également tout type de prise de décision exclusivement fondée sur un traitement automatisé des données. Les prises de décisions fondées uniquement partiellement sur un traitement automatisé seraient-elles alors admises, notamment si elles sont « autorisées par le droit d'un Etat membre »[226] ?

L'UE entend ainsi expliquer le risque d'une décision automatisée produisant des effets juridiques défavorables à l'individu concerné. En revanche, par le respect de la souveraineté des Etats membres, une marge de manœuvre leur est laissée. Cette dernière pourrait être une porte ouverte aux expérimentations de « justice prédictive »[227], dans le domaine pénal. La Commission européenne est

---

[224] Franck Pasquale, « *The Black Box Society : the secret algorithms that control money and information* », Harvard University Press, 2015, p. 5.
[225] Art. 5, para. 1, point a) RGPD.
Art. 5, para. 4, point a), et art. 8, Convention 108+.
[226] Art. 11, Directive Police-Justice.
[227] Cf. Partie I, Titre II, Chap. 2.

consciente qu'une décision automatisée comporte des enjeux beaucoup plus importants que celle prise par un être humain[228]. Notamment, puisqu'elle est plus complexe à contester.

En revanche, aucune disposition quant à la possibilité d'avoir accès à une explication du fonctionnement du système de traitement automatisé, n'est précisée. L'argument nécessaire d'avancer quant à ce manque de transparence au sein des dispositifs d'IA serait qu'un accès total aux données de l'algorithme doit être évité afin d'éviter toute duperie du logiciel qui pourrait affaiblir la sécurité de la justice[229]. La complexité de mise en place du droit d'accès au fonctionnement est également avancée pour des raisons commerciales et concurrentielles entre les fabricants de tels dispositifs.

Il convient de comprendre les moyens pour l'individu concerné, de s'opposer à une décision prise par ce type de dispositifs.

Section 2 : Les recours disponibles en cas de décision issue d'un mauvais traitement

En matière pénale, la motivation d'une décision a un double intérêt. Elle permet d'abord à la personne qui se voit imposer une peine de se la faire expliquer et de la comprendre, mais elle oblige également la personne qui prend la décision à la rigueur d'un raisonnement et à la pertinence de motifs dont elle doit pouvoir rendre compte. C'est ce dernier point qui nous intéresse ici. Un magistrat, un policier ou tout intervenant prenant une décision ayant des conséquences sur les libertés individuelles d'une personne se doit d'être en capacité d'expliquer les raisons qui l'ont poussé à prendre cette décision.

L'article 11 de la directive Police-Justice mentionne l'obtention d'une décision défavorable à l'issu d'un traitement automatisé des données. En revanche, cette disposition ne concerne que les délibérations exclusivement automatisées sans présence humaine. La présence humaine lors de la prise de décision rend le contexte décisionnel différent et surement moins absurde. En revanche, outre le fait que le terme « décision défavorable » soit subjectif, le terme « présence humaine » désigne-t-il un juge, une personne chargée de supervisée techniquement l'algorithme ou d'autres professionnels ? Partons du fait qu'il s'agisse d'un juge.

La présence humaine lors de cette décision n'est pas une garantie suffisante. D'une part, du fait que le juge possèderait une place secondaire au sein de la décision. D'autre part, puisqu'il n'est pas explicitement fait référence au droit de recours de l'individu concerné par cette décision.

---

[228] Commission européenne, Livre blanc, op. cit., p. 13.
[229] Jesse Beatson, « AI-supported adjudicators : should artificial intelligence have a role in tribunal adjudiction », op. cit., pp. 25-26.

Il est nécessaire pour cet individu de pouvoir exercer un recours lui permettant une réponse autre qu'un renvoi devant une autre juridiction par exemple. Il s'agirait de réaliser son droit de refuser de faire l'objet d'une décision lorsque l'algorithme du dispositif d'IA est complètement opaque. Cette question nous renvoi à la réflexion du consentement. Le consentement ayant été requis par les autorités françaises pour les traitements des données biométriques, il serait contradictoire de ne pas accorder de l'importance aux conséquences d'une décision automatisée. Il convient également de renvoyer ces réflexions aux raisonnements relatifs à la justice prédictive[230].

Titre II : Les risques liés à la publication et conservation des données personnelles

La circulation d'un flux de données à caractère personnelle figure à plusieurs reprises au sein du RGPD et de la directive Police-Justice. Ce terme apparaît à premier abord comme abstrait et en émane une crainte liée à sa sémantique qui laisserait penser que les données circuleraient à travers les frontières et entre tout organisme sans réel contrôle et protection. Les dispositifs d'IA permettant une réelle accélération du transfert des informations pourraient être en ce sens perçus en tant que dangers. En revanche, le concept de transfert de flux de données personnelles est issu du cumul des principes européens de « transferts des données personnelles »[231] et de la « libre circulation des données à caractère personnel »[232]. En matière pénale, il appelle à la coopération pénale transfrontalière. Ainsi, le besoin d'échanger des données entre autorités pénales d'Etats membres de l'UE en l'occurrence devient primordial à une meilleure appréhension des infractions transfrontalières. Les dispositifs d'IA utilisés par les autorités pénales nationales étudiées en première partie s'uniformisent et permettent une meilleure collaboration.

En outre, les données personnelles contemporaines ne connaissent également pas de frontières, notamment en matière de divulgation des données sur les réseaux sociaux pouvant ensuite être traitées par les services de police ou de gendarmerie comme étudié précédemment. Mais également par l'accès du public à ces données et à leur traitement par les sociétés privées dont le profit est tiré de cette publication. La protection des données, matière première de ces sociétés privées serait parfois insuffisante. Il est incontestable que les fondements du droit à la protection des données personnelles soient mis en danger par les notions de publication (Chapitre 1) et de conservation (Chapitre 2) des données.

---

[230] Cf. Partie I, Titre II, Chap. 2.
[231] Art. 44 du RGPD ; Art. 14, §1-2 de la convention 108+.
[232] Art. 1, 3 et cons. 170 du RGPD ; Art. 14§1 de la convention 108+.

Chapitre 1 : La publication des données et les enjeux de l'*open data* des décisions judiciaires

La diffusion au public des décisions de justice, bien que déjà existante, s'est accrue depuis l'entrée en vigueur de la loi pour une république numérique du 7 octobre 2016, précisant l'accès au public des décisions des juridictions en ses articles 20 et 21. Dans un but d'amélioration de l'accès à la jurisprudence aux justiciables. Cependant, il faut que ces outils rediffusant des décisions garantissent une objectivité et une qualité de service.

A la suite de la mise en œuvre de *l'open data* des décisions de justice, de belles perspectives au profit d'une accélération et d'une amélioration de la préparation à du procès sont à envisager. D'un point de vue économique également. Le rapport Cadiet[233], consacre une section entière aux perspectives économiques, dans laquelle l'*open data* des décisions de justice sont présentées comme la perfection de la prévisibilité de la justice, cela notamment par l'utilisation de cette banque de données enrichie par des dispositifs d'IA étudiés en première partie. En revanche, il s'agit de ne pas oublier les répercussions de cet afflux de données sur le principe rare, si non obsolète, de l'anonymisation. La réidentification des décisions rendues publiques est difficile à prévenir (Section 1). Il s'agira également de comprendre quels peuvent être les risques engendrés par l'utilisation de ces données personnelles, par les *legaltechs*, en tant que sociétés privées (Section 2).

Section 1 : La difficulté à prévenir la réidentification des décisions rendues publiques

L'anonymisation des données assure la protection des données personnelles au sein du phénomène d'*open data* des décisions de justice. Au grand dam d'une partie de la doctrine nostalgique d'un temps où les décisions de justice publiées et non anonymisées faisait partie intégrante du concept de la Justice. Plusieurs auteurs estiment que les décisions se doivent d'être publiques et regrettent de « déplorer que [des *legaltechts*] soient obligées de se battre pour des décisions qui devraient être publiques »[234]. Les professeurs Nathalie Blanc et Pierre-Yves Gautier déclarent qu'« en réalité, derrière cette protection de façade de la vie privée, c'est un coup porté à l'utilisation de la jurisprudence par la doctrine et les praticiens, juges et avocats. Celle-ci n'est faite ni pour les réseaux sociaux ni pour les entreprises qui se servent du droit comme d'une marchandise, « à vendre » par tous moyens au public juriste. D'un mal de fait, est ainsi produit un mal de droit, ce qui n'est guère admissible »[235].

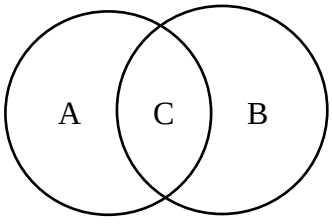
---

[233] Rapport Loïc Cadiet, « L'open data des décisions de justice », novembre 2017.
[234] Oussama Ammar, « La guerre s'intensifie entre Doctrine et les avocats », Les Echos Entrepreneurs, le 27 juin 2019.
[235] Nathalie Blanc, Pierre-Yves Gautier, « Contre « l'anonymisation » des arrêts publiés : décadence des références de jurisprudence », dans Dalloz actu., 6 septembre 2019.

Il convient de distinguer les termes « anonymisation » et « pseudonymisation » pouvant porter à confusion notamment selon leur caractère réversible et ainsi l'applicabilité du RGPD aux données concernées par l'un ou l'autre. La CNIL a défini ces deux concepts[236]. L'anonymisation « vise à rendre impossible toute identification des individus au sein de jeux de données. Il s'agit donc d'un processus irréversible. Lorsque cette anonymisation est effective, les données ne sont plus considérées comme des données personnelles et les exigences du RGPD ne sont plus applicables. [La pseudonymisation] se réfère à un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans avoir recours à des informations supplémentaires »[237]. Cette distinction se veut rassurante en ce que l'anonymisation des données semble plus protectrice des données issues de documents rendus publics.

Outre cette caractéristique d'attraction marketing des données pour les outils les manipulant, il s'agit de comprendre pour quelle raison, les efforts d'anonymisation des décisions et le renfort des textes en cette faveur pourraient ne pas être suffisants. En effet, les données des décisions une fois rendues publiques peuvent et pourront de plus en plus (au vu de l'évolution technique) être facilement réutilisées. La réidentification intervient cependant à la suite de « croisements de données et métadonnées »[238] du fait de l'augmentation du nombre de données en ligne et le perfectionnement des outils recensant ces dernières. Les métadonnées[239] possèdent pour rôle en effet, la corrélation sémantique et technique entre les différentes données.

Ci-après une représentation schématique du croisement des données, dans laquelle, les données A représentent les données anonymisées, les données B sont à lire comme étant celles possédées par un tiers ou le responsable de traitement, et les données C sont les données au départ anonymisées au sein des données A, mais réidentifiées par la conjugaison des données A et B.



[236] CNIL, « Identifier les données personnelles », 27 janvier 2020.
[237] Définitions de « l'anonymisation » et de « la pseudonymisation » par la CNIL.
[238] Rapport Loïc Cadiet, « L'open data des décisions de justice », novembre 2017, p.26.
Voir aussi : Antoinette Rouvroy et Anne Debet, op. cit.
[239] La métadonnée est une donnée servant à caractériser une autre donnée, physique ou numérique, https://www.larousse.fr/dictionnaires/francais/métadonnée/186919.

Ainsi, d'un point de vue pratique, si les données comme le nom et prénom son occultées, notamment par le renforcement du principe d'anonymisation en l'article 33 de la loi du 23 mars 2019[240], une personne peut être reconnue dans une décision, par les détails des faits, la date ou encore la ville. Le croisement de ces données permet une réidentification de plus en plus plausible, et l'interdiction seule de mentionner les noms et prénoms ne suffit pas, un décret encadrant une meilleure anonymisation est actuellement attendu. Cependant, cela pourrait au contraire, compliquer le process de publication des décisions et serait contre-productif vis-à-vis d'une tendance à vouloir davantage rendre les décisions accessibles aux professions de droit ainsi qu'aux justiciables.

Antoinette Rouvroy, étudie la possibilité d'établir une analyse de risques de réidentification étant cependant, insuffisante et très difficile à mettre en œuvre, puisqu'il s'agirait d'assurer une « réévaluation régulière, ou d'un « monitoring » constant, ce qui est d'autant plus difficile qu'est difficilement envisageable la réalisation d'un « inventaire » de toutes les données, actuelles et futures, susceptibles d'être « croisées » avec les données anonymes en la possession du responsable du traitement »[241]. Il convient de comprendre comment les sociétés participant au traitement des données gèrent-elles le respect de la protection des données.

Section 2 : L'utilisation des décisions judiciaires par des sociétés privées

Il convient de rappeler qu'au sein de cette étude, les dispositifs d'IA sont appréhendés en tant qu'outils développés parallèlement à l'émergence d'une vague sécuritaire et une volonté de toujours mieux renforcer la prévention des comportements déviants. La société est perçue comme un ensemble de comportements à prévenir et conditionner. Plusieurs auteurs et philosophes décrivent ce phénomène d'utilisation des outils statistiques comme une « gouvernance par les nombres »[242], « [une technique] de gouvernement »[243] et un « nouveau régime de vérité numérique s'incarnant dans une multitude de nouveaux systèmes automatiques de modélisation du « social » »[244] , notamment par une analyse des comportements rendue objective par les nombres.

A cet aspect se développe également la volonté de rendre accessible la connaissance juridique et le concept de justice au public. Des sociétés se développent en partie en ce sens et il s'agit de ne pas occulter le fait que derrière chacun de ces dispositifs, présentés en première partie, respire une volonté

---

[240] Cette disposition reprend notamment l'anonymisation des noms et prénoms des personnes physiques mentionnées dans la décision, lorsqu'elles sont parties ou tiers. Ce principe s'étend également aux noms des magistrats et greffiers.
[241] Antoinette Rouvroy, « Des données et des Hommes, Droits et libertés fondamentaux dans un monde de données massives », Bureau du comité consultatif de la Convention 108, Conseil de l'Europe, 11 janvier 2016, pp. 25-26.
[242] Alain Supiot, « La gouvernance par les nombres », Cours au collège de France (2012-2014), Ed. Fayard, 2015.
[243] Dominique Cardon, « A quoi rêvent les algorithmes ? Nos vies à l'heure des big data », op. cit., p.9.
[244] Antoinette Rouvroy, Thomas Berns, « Gouvernementalité algorithmique et perspectives d'émancipation – Le disparate comme condition d'individuation par la relation ? » Dans Réseaux 2013/1 (n° 177), pp 163-196.

légitime de profit. De ce fait, sont entendues comme « sociétés privées » dans cette étude, majoritairement les *legaltechs,* traitant des décisions de justice et les organismes liés de près ou de loin à ces dernières traitant des données personnelles et comprenant une équipe d'informaticiens et de *data scientists*. Ce titre peut rapidement servir d'appât aux critiques souvent facilement délivrées aux sociétés privées, se servant des données personnelles. Selon Christiane Féral-Schuhl, présidente du conseil national des barreaux, « l'*open data* des décisions de justice suppose un flux intègre et une base de données exhaustive qui ne peut pas être tenue par un acteur privé »[245]. En réponse à cette réticence, le domaine du droit se voit injustement étiqueté de « secteur technophobe »[246].

En l'occurrence les craintes des professionnels du droit sont principalement issues du fait que les données des décisions judiciaires, pourraient permettre d'identifier les personnes concernées par la décision. Le cadre juridique des *legaltechs* concernées et de l'*open data* des décisions de justice, ne serait pas encore suffisamment poli. Cette section est consacrée à la façon dont ces risques quant aux données personnelles, sont anticipés et gérés par ces sociétés privées accompagnées par des experts en informatiques et quelles sont les lacunes de cette gestion. Il convient d'étudier les différentes protections mises en œuvre (§1), pour en appréhender les lacunes et les besoins d'un cadre normatif renforcé (§2).

§1. La présence d'une volonté protectrice des données par les sociétés privées

La volonté de protection des données par les sociétés privées se traduit par des actes répondant à une éthique (a) et d'autres à un aspect technique (b) de cette protection.

a. La protection de nature éthique

Il convient premièrement de rappeler que plusieurs *legaltechs* mettent en lumière leur volonté de ne pas traiter des données et décisions judiciaires pénales, pour des raisons éthiques. C'est le cas de la l*egaltech «* Predictice » utilisée afin d'estimer le taux de succès d'une action contentieuse principalement en matière civile. Elle s'interdit d'exploiter ses compétences au sein de la matière pénale. Cette interdiction est surveillée par le comité éthique et scientifique de la justice prédictive, créé au sein même de cette *legaltech*. Les risques concernant les données, sont en revanche majoritairement liés au fonctionnement des algorithmes de ces *legaltechs,* et une protection de nature technique est alors nécessaire.

[245] Christiane Féral-Schuhl, « La guerre s'intensifie entre Doctrine et les avocats », op. cit.
[246] Guillaume Bregeras, « La start-up Doctrine attaquée par l'Ordre des avocats de Paris », Les Echos, le 27 septembre 2018.

b. La protection de nature technique

Selon Antoinette Rouvroy, une des approches protectrices des données personnelles les plus praticables serait de « contraindre les entités qui souhaitent anonymiser des données à procéder à l'évaluation préalable des risques de réidentification (en fonction de la quantité, de la variété et du temps de conservation envisagée pour les données récoltées), et à en communiquer les résultats aux individus préalablement au recueil de leur consentement mais aussi, à tout moment, en cas d'accroissement du risque de réidentification. »[247].

Le RGPD, s'appliquant aux sociétés privées traitant des données personnelles[248], elles doivent en respecter les dispositions. Le RGPD préconise la pseudonymisation afin de conserver les données sous une forme ne permettant pas d'identifier directement un individu sans information complémentaire. Pour ce faire, il s'agit de mettre en place une sécurité sous forme de *blockchain*, littéralement traduite par « chaîne de blocks ». La *blockchain* est définie par le ministère de l'économie en 2018 comme étant : « Un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie »[249].

Cette technique permet d'assurer une sécurité quant aux conséquences du traitement de ces données par des acteurs privés. En revanche, quelques lacunes sont à constater et à anticiper.

§2. Les lacunes provenant d'une mauvaise gestion des données par des sociétés privées

D'une part, la pseudonymisation est une méthode permettant d'évincer l'identité des personnes concernées par les décisions utilisées. Il convient de rappeler que cette méthode n'est pas sans risque. La notion de risque est mentionnée à 78 reprises au sein du RGPD. Antoinette Rouvroy rappelle l'importance de « sensibiliser tant les personnes concernées que les responsables de traitement au fait que l'anonymat n'est jamais garanti et de les inciter des lors à la prudence lorsque, pour les premiers, ils émettent un consentement, et, pour les seconds, ils rendent possible le croisement des données anonymes en leur possession avec d'autres jeux de données en leur possession également ou en la possession de tiers »[250] Ces lacunes quant à la protection des données proviendraient d'autre part d'un malentendu lié à la finalité du phénomène d'open data des décisions judiciaires. Ce risque est cumulé

[247] Antoinette Rouvroy, « Des données et des Hommes, Droits et libertés fondamentaux dans un monde de données massives », op. cit., p. 25.
[248] Art. 2, RGPD.
[249] Rapport d'information par la mission d'information commune sur les chaînes de blocks (blockchains), Laure de la Raudière et Jean-Michel Mis, le 12 décembre 2018, p. 119.
[250] Antoinette Rouvroy, « Des données et des Hommes, Droits et libertés fondamentaux dans un monde de données massives », op. cit., p. 25.

à un cadre normatif du principe de l'open data judiciaire, perméable à une interprétation de la publication confondu avec le principe de publicité des données. L'affaire médiatisée de 2018 concernant la legaltech « Doctrine » permet de mieux appréhender les risques et dangers ayant vu le jour il y a deux ans.

La *legaltech*, a récupéré des données par des pratiques de *typosquatting*[251], un type d'usurpation d'identité informatique, concrètement en utilisant des adresses e-mail inventées mais similaires à celles de professionnels du droit, comme des avocats connus, des universités, l'Ecole du barreau de Paris, ainsi que celles de *legaltechs* concurrentes. Le barreau parisien a porté plainte contre la *legaltech* pour « usurpation du titre d'avocat, usurpation d'identité, escroquerie, vol et maintien frauduleux dans un système informatique et recel »[252]. En outre, afin de pérenniser le rapport que les entreprises privées peuvent avoir avec la protection des données personnelles, il conviendrait d'établir une sécurité juridique. Au niveau français, le nombre de lois issues du récent projet d'*open data* des décisions judiciaires sont déjà au nombre de deux, dont une faisant partie d'un programme s'étendant jusqu'à 2022. Un décret d'application est également attendu.

Or, de futurs risques liés à une incertitude juridique ont également vu le jour le 16 juillet dernier, lors de la décision dite « Schrems II »[253], rendue par la cour de justice de l'UE (CJUE). En l'espèce, la cour a souhaité supprimer l'accord de bouclier de protection des données dit « privacy shield » entre l'UE et les Etats-Unis, permettant aux entreprises européennes de transférer de manière légale les données personnelles de leurs clients vers les Etats-Unis[254]. Le motif de cette suppression est notamment lié au niveau insuffisant de protection des données personnelles sur le territoire américain.

Bien que cette décision ne concerne pas directement les risques liés aux données traitées par des dispositifs d'IA servant la matière pénale, elle est importante en ce qu'elle rappelle les fondements du droit à la protection des données personnelles notamment en matière de transfert international des données personnelles. Quid du transfert et de la conservation transfrontières des données non-anonymisées, notamment en matière de coopération pénale ?

---

[251] Le typosquatting est une forme de piratage informatique se fondant principalement sur les fautes de frappe et d'orthographe commises par l'internaute au moment de saisir une adresse web dans un navigateur, https://fr.wikipedia.org/wiki/Typosquattage.

[252] Paul Gonzales, « L'accès en ligne aux décisions de justice est fragilisé », Le figaro, le 2 octobre 2018.

[253] CJUE, *Data Protection Commissioner c. Facebook Ireland Ltd, M. Schrems*, 16 juillet 2020, n° C-311/18.

[254] Ibid., §203, n°3, p. 51.

Chapitre 2 : La conservation des données et les enjeux du transfert transfrontière

Il convient de s'intéresser aux données conservées sous une forme permettant l'identification[255]. La conservation des données représente des risques d'une ampleur différente en fonction du type de données et du type de traitement. En l'occurrence, la conservation de données biométriques est sujet à débat et à une protection stricte de la part des juridictions européennes. Par ailleurs, la conservation des données peut résulter en une crainte vis-à-vis lorsque ces dernières sont sauvegardées à l'étranger à la suite d'un transfert dans le cadre de la coopération pénale transfrontalière. Nous délimiterons cette étude au cadre européen de collaboration pénale. Il s'agira dans ce chapitre d'étudier les risques et enjeux d'une conservation de données plus ou moins sensibles, d'une part au niveau national (Section 1) et d'autre part, en matière de coopération pénale transfrontalière à la suite d'un transfert des données (Section 2).

Section 1 : La conservation des données par les autorités compétentes au niveau national

La conservation des données à caractère personnel, à la suite de leur utilisation en matière de répression pénale, doit répondre à plusieurs principes protecteurs des données. En outre, la matière pénale est également comprise dans les exceptions aux règles strictes, dans la mesure où la conservation respecte cependant un niveau minimum de protection. La conservation des données en la matière fait face à deux principes non négligeables.

D'une part, la raisonnabilité de la conservation des données est subjectivement appréciable (§1). D'autre part, le principe du droit à l'oubli est remis en cause dans un contexte du big data et en matière pénale (§2).

§1. La raisonnabilité de la conservation des données dépendante de facteurs subjectifs

La conservation des données doit répondre à une finalité et la CJUE dans sa décision « Schrems »[256] rappelle notamment des principes généraux concernant cette finalité : « la conservation des données doit toujours correspondre à des critères objectifs établissant un rapport entre les données à caractère personnel à conserver et l'objectif poursuivi. Une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée » [257].

---

[255] Art. 4§1, e) Directive Police Justice : les données sont conservées sous une forme permettant l'identification des personnes.
[256] CJUE, 6 octobre 2015, *Data Protection Commissionner of Ireland c. M. Schrems*, C-362/14.
[257] Ibid., §§93-94.

En outre, le niveau de sensibilité des données personnelles est à appréhender afin d'évaluer la raisonnabilité de sa conservation. Ainsi, à titre d'exemple, la CEDH dans sa décision « S. et Marper »[258], a jugé disproportionné et inutile « dans une société démocratique »[259], la conservation par des autorités de police des empreintes digitales, échantillons cellulaires et de profils ADN des deux requérants, alors même que le premier avait été acquitté et que le second a vu son affaire être classée sans suite. Le sens du terme société démocratique est à comprendre comme un « besoin social pressant et proportionnel au but légitime poursuivi »[260]. C'est ainsi au titre de cette forme de démocratie que la conservation des données doit être établie. Outre la sensibilité des données concernées par la matière pénale, le délai de conservation est à prendre en compte. En effet, la conservation des données sensibles, dont font partie les données génétiques[261] est davantage encadrée par les juridictions européennes.

Par ailleurs le principe général de la conservation des données requiert la suppression ou l'anonymisation des données dont le traitement n'est plus nécessaire à la finalité pour lesquelles elles ont été employées[262]. En revanche, en matière policière, la conservation de ces données au-delà de l'utilisation convenue est possible seulement si une limite temporelle a été précisée. Ce délai de conservation se doit d'être raisonnable et proportionnel à l'objet de la collecte. En revanche, le caractère raisonnable du délai de conservation, comme le concept de finalité du traitement, n'est pas clairement défini et dépend de plusieurs facteurs.

A titre d'exemple, le délai de conservation dans des fichiers de police. En 2013, la CNIL rédige un rapport à destination des autorités de police et de gendarmerie pour leur fichiers respectifs STIC et JUDEX. Elle y dénonce à répétition des problèmes de gestion des données personnelles et s'inquiète du manque d'améliorations depuis son précédent contrôle 5 ans plus tôt. Parmi les difficultés rencontrées par les services de police et de gendarmerie, un besoin de « mise à jour massive d'antécédents par rectification ou effacement »[263]. En effet, les personnes relaxées, voyant leur affaire classée sans suite ou recevant une décision favorable au sein de leur procès pénal, voient leurs données personnelles non mises à jour, et perdent ainsi la possibilité de bénéficier de l'arrêt de la

---

[258] CEDH, *S et Marper c. Royaume-Uni*, n° 30562/04 et nº 30566/04, 4 décembre 2008, §70.
Voir aussi : CEDH, *Breyer c. Allemagne*, n° 50001/12, 30 janvier 2020, §88.

[259] Ibid.

[260] CEDH, Olsson c. Suède, n°10465/83, 24 mars 1988, §67.
Voir aussi : CEDH, *Leander c. Suède*, op, cit., §58.

[261] Cons. 23, Directive Police-Justice : « Compte tenu du caractère complexe et sensible des informations génétiques ».

[262] Art. 5§1, e. RGPD ; Art. 5§4, e. Convention 108.

[263] Rapport de la CNIL, « Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur », le 13 juin 2013, p. 23.

conservation de leurs informations au sein du fichier. Cette mauvaise gestion de leurs données personnelles peut entrainer une discrimination à l'emploi, certains employeurs ayant accès au STIC.

C'est ainsi que par sa décision « Brunet » de 2014, la CEDH condamne la France pour violation du droit au respect de la vie privée – incluant la protection des données à caractère personnel – au motif que la conservation pendant 20 ans de données à caractère personnel issues d'une affaire classée sans suite au sein du fichier de police STIC (Système de traitement des infractions constatées) était « disproportionnée »[264]. Les données du fichier STIC sont désormais disponibles au sein du fichier TAJ (Traitement d'antécédent judiciaire).

Bien que les données entrées au sein de ces fichiers de police s'effectuent manuellement, il convient de rappeler que les données du TAJ sont potentiellement recueillies par des algorithmes, comme celui de reconnaissance faciale combinant les informations policières à une banque d'images de vidéosurveillance précédemment étudié[265]. D'autre part, les magistrats ont accès aux données issues de ces fichiers, notamment afin de connaître des détails plus fournis au sujet des infractions dont ils sont saisis[266]. Ainsi, les informations personnelles, par exemple conservées au sein d'un fichier de police, comme il en est le cas pour les victimes d'infractions au sein du TAJ, anciennement STIC, doivent pouvoir être supprimées. Notamment pour des raisons de consentement d'utilisation des données au sein de ces dispositifs d'IA, cependant il est important d'étudier cet enjeu au regard du principe fondamental du droit à l'oubli.

§2. Le droit à l'oubli en matière de recueil pénal des données personnelles à l'ère du big data

Le droit à l'oubli est communément appelé « droit à l'effacement » au sein des régulations du droit à la protection des données personnelles en Europe, comme le RGPD et la convention 108[267]. Il s'agit pour un intéressé dont les données personnelles sont recueillies, de demander au responsable de traitement de les effacer. Le droit à l'oubli n'est pas absolu. La CJUE a pu le rappeler en 2014, dans son arrêt *Google Spain*[268], ainsi qu'en 2017 par une décision dans laquelle *Salvatore Manni*, ressortissant italien, souhaitait effacer la mention de la faillite de sa société sur internet lorsque l'on cherche son nom sur Google [269]. La Cour considère qu'en l'espèce, la publicité légale des données prime sur le droit à l'oubli[270]. Le droit à l'oubli n'étant pas absolu dans certaines matières, il doit tout

---

[264] CEDH, *Brunet c. France*, n°21010/10, 8 septembre 2014, §8.
[265] Cf. Partie I, Titre I, Chap. 3, S1 : voir les développements quant au logiciel G.A.S.P.A.R.D.
[266] Cf. Partie I, Titre II, Chap. 1.
[267] Art. 9§1, e) convention 108 ; art. 17 RGPD.
[268] CJUE, 13 mai 2014, aff. C-131/12, Google Spain c/ Agencia Española de Protección de Datos, AJDA 2014. 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère.
[269] CJUE, 9 mars 2017, aff. C-398/15, Camera di Commercio c/ Salvatore Manni.
[270] Géraldine Péronne, Emmanuel Daoud, « *Droit à l'oubli contre publicité légale des données : la publicité prime !* », Observations sous Cour de justice de l'Union européenne, 9 mars 2017, aff. C-398/15, Camera di Commercio c/ Salvatore Manni, Dalloz IP/IT 2017, p.345.

de même prévaloir sur la conservation abusive des données, notamment en matière pénale dans certains cas.

Si les données personnelles d'un individu sont collectées et conservées au sein d'un fichier, leur sauvegarde doit répondre à un but légitime et à un fondement juridique. En revanche, une liste de situations dans lesquelles cet effacement peut être refusé est dressée par la directive Police-Justice[271].

La CEDH vient cependant garantir que les données ne soient pas stockées trop longtemps et vérifie le réel intérêt de sécurité nationale de la préservation de ces données pour cette durée. Ce fût le cas notamment dans sa décision « Brunet ». Un an plus tôt, dans sa décision « M.K »[272], la Cour condamne la France au sujet de la conservation irrégulière par les services de police, des données biométriques, à savoir des empreintes digitales, au sein du fichier français FAED (Fichier automatisé des empreintes digitales), créé en 1987.

En l'espèce, le requérant a fait l'objet d'une relève d'empreintes digitales en 2004, puis en 2005 il est relaxé des enquêtes pour vols de livre ouvertes à son encontre. En 2006, il exerça une demande d'effacement des données au sein du FAED auprès du procureur de la République. Sa demande est refusée, et cette décision est confirmée par les juridictions de première instance, d'appel et de cassation. Ce refus est motivé du fait que la conservation des données était d'une part, dans l'intérêt du requérant – afin de prouver son innocence –, d'autre part, dans l'intérêt des services de police, nécessitant de remplir la base de données du fichier afin de garantir l'efficacité des enquêtes futures. Il convient de rappeler ici encore une fois, l'enjeu de produire de la donnée pour permettre d'augmenter l'efficacité des dispositifs de traitement des données.

Ce refus d'accès aux données est valablement reçu par la CEDH quand l'État parvient à « ménager un juste équilibre entre l'intérêt général et les intérêts de l'individu »[273]. Notamment, en procédant à l'évaluation de la justification de l'ingérence et à un contrôle de proportionnalité.

Afin de répondre à la requête de l'intéressé, et de prononcé une violation de la convention européenne des droits de l'Homme (ConvEDH) du fait du refus de l'effacement, la Cour, tout d'abord évalue la justification de l'ingérence au sein de la vie privée du requérant, selon les dispositions concernées, au sein de l'art. 8 paragraphe 2 de la ConvEDH. Elle procède ainsi : le prélèvement des empreintes digitales du requérant en tant que données biométriques constitue bien entendu, une ingérence au sein

[271] Art. 16§§3-4. Directive Police-Justice.
[272] CEDH, *M.K c. France*, 18 avril 2013.
[273] CEDH, *Stjerna c. Finlande*, Op. cit., Concordante de M. le Juge WILDHABER, p. 15.

de sa vie privée[274]. Cette ingérence est justifiée par l'art. 55-1 du code de procédure pénale français, encadrant le relevé de données personnelles afin d'alimenter une base de données policières.

La Cour effectue un contrôle de proportionnalité en contrôlant si la mesure de saisie des données au sein dudit fichier de police est une mesure « nécessaire dans une société démocratique ». Pour des raisons de fluidification de lecture, il convient de renvoyer le lecteur à la définition de cette notion à la section 1 du présent chapitre. La durée de conservation des données pendant vingt-cinq années au sein du FAED est jugée non seulement longue, mais surtout « indéfinie »[275] par la Cour. Les juges de Strasbourg relèvent également le peu de chance pour un requérant dans cette situation, de voir sa demande d'effacement aboutir positivement. Ce manque de possibilité d'effacement provient notamment du fait que la demande doive être formulée au procureur de la République, considérés par la Cour comme non indépendants, à savoir : « du fait de leur statut ainsi rappelé, les membres du ministère public, en France, ne remplissent pas l'exigence d'indépendance à l'égard de l'exécutif »[276].

Enfin, la Cour regrette l'incertitude des finalités des fichiers. En effet, le FAED a pour finalité de « faciliter la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie »[277]. La Cour considère que cette finalité englobe tout type d'infractions et constitue ainsi une disproportion, cela quand bien même un décret a été adopté en 2005, pour restreindre aux crimes et délits, l'enregistrement des empreintes digitales. Par ailleurs, la Cour condamne le fait que ce fichier conserve les données d'un innocent, puisqu'en l'espèce M. K. a été relaxé. La Cour a alors considéré « que retenir l'argument tiré d'une prétendue garantie de protection contre les agissements des tiers susceptibles d'usurper une identité reviendrait, en pratique, à justifier le fichage de l'intégralité de la population présente sur le sol français, ce qui serait assurément excessif et non pertinent »[278].

Ainsi cette conservation constitue une violation de l'article 8 de la convention car elle ne traduit pas « un juste équilibre entre les intérêts publics et privés concurrents en jeu. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit du requérant au respect de sa vie privée et ne peut passer pour nécessaire dans une société démocratique »[279]. Quid de la société démocratique sous l'égide de l'utilisation des données personnelles dans un contexte d'augmentation de l'utilisation de dispositifs d'IA au sein même de la matière pénale.

---

[274] CEDH, *S et Marper c. Royaume-Uni*, op. cit.
[275] CEDH, *M.K c. France*, op. cit., §45.
[276] CEDH, *Moulin c. France*, n°37104/06, 23 novembre 2010, §57.
[277] Art. 3 al. 2 du décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'Intérieur.
[278] CEDH, *M.K c. France*, op. cit. §40.
[279] Ibid., §§46-47.

A l'ère du big data, les dispositifs d'IA en matière pénale seraient-ils à appréhender en tant que garantie de la démocratie ou de destruction de cette dernière ? Alors que ces dispositifs sont « gages de modernité »[280], y compris au sein des autorités pénales, sa tendance destructrice de la démocratie est présente au sein de plus en plus d'écrits[281].

La récente directive Police-Justice garantit la possibilité de demander l'effacement des données détenues par les autorités compétentes à la répression pénale[282], ainsi que l'obligation de fixer une durée limite de conservation des données[283]. Le 13 février dernier, la CEDH, a en ce sens condamné le Royaume-Uni au sujet d'une conservation illimitée dans le temps par les services de police des données biométriques, notamment du profil ADN, des empreintes digitales et de la photographie d'un homme condamné pour conduite en état d'ivresse, a enfreint son droit au respect de la vie privée[284], d'autant plus qu'il s'agissait de données vouées à être utilisées pour des techniques de reconnaissance faciale, et de cartographie faciale[285].

Cependant, cette obligation figure uniquement au sein d'un considérant, n'ayant pas de force exécutoire. Par ailleurs, il n'est techniquement pas possible de garantir à 100% l'effacement de données, renseignées au sein de dispositifs d'IA – notamment comme précédemment cité, les informations du TAJ au sein de l'algorithme G.A.S.P.A.R.D – du fait que lorsque sont supprimées ces données, elles « ne disparaissent pas comme par enchantement. Au lieu de cela, le morceau de mémoire est placé sur une "liste liée" qui est traitée tôt ou tard et insérée dans une mémoire logicielle disponible en vue d'une réutilisation éventuelle »[286]. Cette procédure est appelée « ramasse-miettes »[287].

Par ailleurs, d'autres enjeux liés à la conservation surviennent du transfert des données au sein de l'Europe, dans le cadre de la coopération pénale transfrontalière notamment.

---

[280] Joseph Righenzi de Villers « *L'IA sauvera-t-elle la démocratie ?* », Assas Legal Innovation, le 8 avril 2020.
[281] « *L'IA va-t-elle aussi tuer la démocratie* », Jean-François Copé et Laurent Alexandre.
[282] Art. 13, §1, e), directive Police-Justice.
[283] Considérant 26, directive Police-Justice.
[284] CEDH, *Gaughran c. Royaume-Uni*, n° 45245/15, 13 février 2020, §§87-96.
[285] Ibid., §70 :
« In the present case, given that the applicant's custody photograph was taken on his arrest and will be held indefinitely on a local database for use by the police and that the police may also apply facial recognition and facial mapping techniques to the photograph, the Court has no doubt that the taking and retention of the applicant's photograph amounts to an interference with his right to private life within the meaning of Article 8 § 1 ».

[286] Christophe Badot, « *Le défi du droit à l'oubli face à l'intelligence artificielle* », Les Echos, le 10 novembre 2017.
[287] Ibid.

Section 2 : La conservation des données en matière de coopération pénale transfrontalière

Depuis la suppression des contrôles aux frontières au sein de l'espace Schengen, une augmentation des risques de fraudes a été observée, et les Etats membres se doivent ainsi d'augmenter leur coopération en la matière, notamment en s'échangeant des données. L'échange des données dans le cadre de cette collaboration est encadrée par plusieurs textes[288]. La nature des données personnelles échangées dans ce domaine et intéressant les services de police et judiciaire, concerne majoritairement des données sur l'immigration ainsi que celles liées aux produits exportés depuis l'UE ou importé vers l'UE.

En 2005, le traité de Prüm, signé par plusieurs Etats membres de l'UE, vise à approfondir la coopération transfrontalière en matière de police, notamment dans les domaines de la lutte contre le terrorisme, la criminalité organisée et l'immigration illégale. Il est établi à la suite des attentats espagnols de 2005, et permet au niveau de l'UE, de réfléchir et de mettre en œuvre le principe de disponibilité[289]. Ce dernier recommande aux services répressifs d'un État membre de fournir spontanément à un agent d'un autre État membre toute information disponible susceptible de présenter un intérêt communautaire. Le Conseil de l'UE intègre au droit communautaire en 2008 dans sa décision Prüm[290], les dispositions dudit traité. Par ailleurs, en 2011, la Commission européenne rappelle que « le monde a connu une augmentation du terrorisme et de la criminalité grave et organisée, ce qui peut impliquer des déplacements sur le plan international et a mis en évidence la nécessité de renforcer la coopération transfrontalière entre autorités policières et répressives dans de nombreuses affaires »[291]. Il convient d'étudier les difficultés de la politique du libre flux des données à l'ère du big data (§1), afin d'appréhender les enjeux liés à la protection des données personnelles et l'harmonisation de cette protection (§2).

---

[288] Décision-cadre 2009/315/JAI du Conseil concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres. Décision 2000/642/JAI du Conseil relative aux modalités de coopération entre les cellules de renseignement financier des États membres en ce qui concerne l'échange d'informations.

Voir aussi : « Autres instruments juridiques spécifiques en matière de protection des données dans le domaine répressif », Manuel sur la protection des données, op. cit., p. 326.

[289] Principe encadré par la décision-cadre 2006/960/JAI du Conseil relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne.

[290] Décision 2008/615/JAI.

[291] Commission européenne (2011), Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière de la Commission, COM(2011) 32 final, Bruxelles, 2 février 2011, p. 1.

§1. Les libres flux de données en matière de coopération pénale à l'ère du big data

Il a longtemps été pensé que les organisations policières supranationales comme « Europol, le réseau judiciaire européen, Eurojust, fonctionneront d'autant mieux que les droits pénaux procéduraux des Etats membres seront semblables : la compréhension, le climat de confiance et donc les contacts entre les personnes travaillant au sein de ces enceintes ou équipes seront naturellement plus aisés si les règles qu'ils connaissent sont proches »[292]. Quid de ces relations aujourd'hui, observons-nous une communauté d'exercice entre les autorités répressives nationales et européennes ? Le transfert des données personnelles traitées par les IA d'organisations policières supranationales, utilisent des dispositifs similaires à ceux utilisés au niveau national.

Europol met en place un budget consacré à l'intelligence artificielle[293]. L'organisation rappelle notamment le besoin de développer ces techniques : « les services répressifs doivent investir dans la compréhension de la technologie de l'IA et de ses implications pour détecter et contenir correctement ces nouvelles menaces »[294]. D'autant plus au sein du contexte de l'émergence de nouvelles formes des infractions comme le « *deepfake* »[295]. Philippe Ammann, directeur de l'unité stratégie et développement d'Europol, souligne que dans un contexte où l'information peut être manipulée et rendue fausse, alors il est primordial de réagir par des technologies basées sur une « approche humano centrée »[296]. Europol évoque également la nécessité du transfert des données au sein de son organisme[297]. Cela n'est pas sans risque de confusion, face à une volonté émergente de la part des institutions européennes et du Conseil de l'Europe de renforcer la protection des données personnelles.

§2. Les enjeux et risques envers les données personnelles et l'harmonisation de leur protection

La conservation des données au sein des serveurs pénaux étrangers peut être source de crainte liée au niveau de sécurité sur le territoire d'un autre Etat membre de l'UE ou au sein d'une organisation policière supranationale. Les Etats membres de l'UE étant les acteurs initiaux de la sauvegarde des droits fondamentaux, il est précisé dans plusieurs textes, que les Etats doivent donner leur accord avant toute transmission et collecte d'informations, à des fins d'enquête, notamment. Plusieurs règles, précédemment étudiées concernant la finalité du traitement et les conditions de conservation sont

[292] Anne Weyembergh, « L'harmonisation des procédures pénales au sein de l'Union européenne », Archives de politique criminelle, éditions A. Pédone, 2004/1 n° 26, pp. 37-70.
[293] Europol programming document 2019-2021, le 29 janvier 2019, pp. 28-40.
[294] « *Do criminals dream of electric sheep* ? », How technology shapes the future of crime and law enforcement, Europol, 2019, p.10.
[295] Cf. Partie II, Titre I, Chap. 2.
[296] Philippe Ammann, Session parlementaire européenne du 20.02.2020 sur « L'intelligence artificielle au sein de la justice pénale et son utilisation par la police et les autorités judiciaires en matière pénale ».
[297] Europol programming document 2019-2021, le 29 janvier 2019, p. 37.

mentionnées de manière importante au sein de la récente directive. En outre, en plus des services de police, la douane est également davantage concernée par la répression transfrontalière. La directive « PNR »[298] traitant des données des passagers, régit les transferts de données entre autorités compétentes à des fins d'aide aux services répressifs à l'identification de suspects connus ou potentiels, en traçant leur itinéraire notamment. En revanche, l'un des aléas à la conservation à l'étranger des données utilisées en matière de répression pénale, est le fait qu'une harmonisation et standardisation de la protection des données personnelles n'est pas encore d'actualité.

L'harmonisation d'une protection des données en matière de coopération pénale transfrontalière appelle à étudier les enjeux liés à la collecte, le transfert et la conservation des données. Ces enjeux sont nombreux et il s'agira de s'intéresser à ceux propres aux Etats membres (a) pour mieux comprendre les enjeux provenant de la réaction et du fonctionnement de l'UE, en tant qu'organisation supranationale (b).

a. Les enjeux d'harmonisation liés aux Etats-membres

La directive Police-Justice, rappelle que l'échange d'informations aux fins de « prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces » prévaut sur la protection des données personnelles, dans le sens où ce droit fondamental ne doit être limité ou interdit face à cette nécessité[299]. En outre, ces textes laissent une marge de manœuvre considérable aux Etats membres dans la retranscription et l'interprétation des mesures, par exemple, le terme « délais appropriés »[300] de conservation. Par ailleurs, la collecte de données sur le territoire d'un Etat possède des règles relatives à la souveraineté étatique.

Le transfert de données entre différents Etats tiers à l'UE en matière d'entraide pénale internationale, peut se voir encadrer par des conventions prévues à ce titre, comme la convention Schengen, ou la Convention sur l'entraide pénale internationale. C'est le cas de l'arrêt rendu le 15 novembre 2019 par la première cour de droit public du Tribunal fédéral suisse[301], au sujet du transfert des données, pendant une enquête concernant un réseau de trafiquants de drogue transférant des substances illicites d'Espagne à la Suisse en passant par la France en voiture : les forces de police suisses ont placé un

---

[298] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

[299] Art. 1§2, b. Directive Police-Justice : « [Les Etats membres] veillent à ce que l'échange de données à caractère personnel par les autorités compétentes au sein de l'Union, lorsque cet échange est requis par le droit de l'Union ou le droit d'un État membre, ne soit ni limité ni interdit pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ».

[300] Art. 5 et 36 Directive Police-Justice.

[301] Tribunal fédéral suisse, A c. Ministère public de l'arrondissement de l'Est vaudois, n°1B_164/2019, 15 novembre 2019.

GPS sous ladite voiture et ont utilisé ses données pour arrêter les trafiquants en traçant leur situation géographique. La question de l'ingérence dans le transfert des données entre Etats en matière d'entraide judiciaire internationale s'est posée puisque la Suisse n'a pas eu l'accord de l'Espagne, ni de la France.

L'harmonisation d'un droit à la protection des données sur le territoire de l'ensemble des Etats participant à la coopération pénale transfrontalière fait également face à un différent degré d'implantation de l'intelligence artificielle. Il est à noter également, les divergences entre les droits procéduraux pénaux des Etats membres. Il convient d'appréhender comment ces enjeux découlent sur le fonctionnement de l'UE en matière de coopération pénale.

b. Les enjeux d'harmonisation liés au fonctionnement de l'UE

La protection des données à caractère personnel a fait l'objet de plusieurs textes au niveau européen participant à un cadre et une structuration au transfert et traitement transfrontaliers des données. Cela peut paraître contradictoire face à une réelle politique de « libre flux des données » et un devoir de concorder à la protection des droits. Par ailleurs, le concept de protection des données n'est pas encore appliqué de manière homogène au sein de l'UE. En matière de l'harmonisation des droits dans le cadre pénal, Anne Weyembergh décrit dès 2004, un principe de « reconnaissance mutuelle en matière pénale »[302], par l'ensemble de décisions-cadres adoptées en la matière, et nous démontre une tendance à « se contenter du plus petit commun dénominateur et entraîne de la sorte un nivellement par le bas des droits et garanties procédurales dont jouissent les personnes concernées par le procès pénal »[303]. Selon elle, dans un contexte de divergence procédurales pénales, afin de « rétablir l'équilibre nécessaire à l'établissement d'un espace de liberté, de sécurité et de justice, il s'agit donc de rapprocher les procédures pénales des Etats, et en particulier de tirer vers le haut les garanties judiciaires reconnues aux individus », notamment en instaurant un niveau de protection exigeant.

Après avoir étudiés l'évolution de la place des dispositifs d'IA en matière de répression pénale, et les risques vis-à-vis des données personnelles que cela engendre ; il convient, dans une troisième partie, d'étudier la façon dont l'utilisation de dispositifs d'IA de traitement des données personnelles en matière pénale, a été régulée en Europe, et vers quel type d'encadrement juridique nous dirigeons-nous.

[302] Anne Weyembergh, « L'harmonisation des procédures pénales au sein de l'Union européenne », op. cit., pp. 37-70.
[303] Ibid.

Conclusion de la Partie II

Il est souvent soutenu que l'IA permet une meilleure administration de la justice pénale tant en matière de prévention que de répression des infractions, en passant par son utilité à rendre accessible le concept même de justice. Selon le philosophe autrichien Karl Popper, une théorie est scientifique si elle est réfutable[304]. La réfutabilité de la théorie selon laquelle l'IA participe au perfectionnement de la justice pénale est tenue dans les risques que cette technologie engendre. Cette théorie est alors scientifiquement admise.

Il est certain que l'IA puisse dans plusieurs domaines apporter une amélioration inédite, en revanche. Il convient de s'assurer que notre société est capable de contourner les risques et enjeux envers la protection des données, posés par l'utilisation de l'IA en matière pénale.

« Le passé ne manque pas d'avenir »[305]. Pour comprendre les capacités de notre société à protéger les droits fondamentaux face à une menace technologique, il est nécessaire n'appréhender le chemin parcouru par notre société depuis l'introduction même du droit à la protection des données lors d'une époque où l'IA, déjà conçue, ne constituait pas encore les risques présents aujourd'hui.

[304] Patrick Juignet, « Karl Popper et les critères de la scientificité », Philosciences.com, 6 mai 2015.
[305] Vincent Vigneau, « Le passé ne manque pas d'avenir - Libres propos d'un juge sur la justice prédictive », Recueil Dalloz, 2018, p. 1095.

Partie III : Le cadre normatif européen des données en matière de justice pénale et en matière d'IA

Il convient de reprendre la citation de Professeur Dino Pedreschi « la technologie n'est pas une fin, mais un moyen. Nous avons la tâche de définir les principes démocratiques d'une société digitale, différents de ceux que nous avons posés dans le passé »[306]. Le professeur prononçait ces mots lors d'une conférence en relation avec les technologies de traçage au profit de la lutte contre le coronavirus évoqué en introduction. Notre société digitale est en constante évolution et a besoin de principes démocratiques. Cependant, il est important de nuancer les propos de cette citation. Nos principes démocratiques ne sont pas différents de ceux posés dans le passé. Par ailleurs, il s'agit de construire autour de ces derniers, les dispositifs technologiques de demain. En effet, occulter nos droits fondamentaux au profit d'une idéologie sécuritaire viendrait créer l'effet inverse à celui souhaité, une réelle « dictature du chiffre »[307].

Il est question de comprendre les fils directeurs de l'évolution de la protection des données afin d'appréhender la régulation tant nationale qu'européenne de cette protection notamment en matière pénale. Les dispositifs d'IA étant présents au sein des autorités répressives des trois Etats étudiés, il s'agit également d'analyser la montée de cette technologie, dans leurs cadres normatifs nationaux. Il conviendra d'étudier l'évolution du cadre normatif de protection des données en matière pénale et au regard de l'IA, à travers l'Allemagne et la France, en tant qu'Etats-membres de l'UE. L'étude du cas de la Suisse est également pertinent du fait de son appartenance au Conseil de l'Europe.

Cette étude se divisera en deux axes temporels. D'une part, il convient de s'intéresser à l'évolution du cadre normatif du traitement automatisé des données en Europe, de 1970 – époque des premiers textes nationaux en faveur d'une protection des données – à 2016 (Titre 1). Dans un second temps, il s'agira d'étudier les nouveaux enjeux et cadres normatifs introduits en Europe depuis 2016, année consacrée à la protection des données personnelles (Titre 2). Cela permettra d'appréhender l'encadrement du traitement des données par des dispositifs d'IA au sein de la justice pénale dans un futur plus ou moins proche.

---

[306] Dino Pedreschi, professeur de Sciences informatiques, Université de Pise, « *Myths and realities of tracking applications* », Webinaire IA and Law Breakfasts, organisé par le Conseil de l'Europe, le 13 avril 2020.
[307] Mark Hunyadi, « La dictature des chiffres », comm. Alain Supiot, La gouvernance par les nombres, LeTemps.ch, le 12 février 2016.

Titre I : L'évolution de l'encadrement européen liée à celle du traitement automatisé des données (de 1970 à 2016)

La protection des données à caractère personnel survient dans les années 1970 au niveau national, notamment en France et en Allemagne et le premier texte international faisant allusion à ce droit apparaît au Conseil de l'Europe en 1981, par la convention dite « 108 ». Le droit à la protection des données personnelles s'est développé initialement au niveau national. Il s'agit dans un premier chapitre d'en étudier les sources nationales (Chapitre 1). Il conviendra d'étudier les cas de l'Allemagne et de la France, en tant qu'Etats membres de l'UE, pour ensuite comprendre la façon dont s'est développé ce droit en Suisse, Etat non-membre de l'UE mais étant partie au Conseil de l'Europe. Le cadre normatif ayant suivi cette démarche nationale appartient au Conseil de l'Europe, concerné avant tout par la protection des données personnelles en tant que droit humain (Chapitre 2). Il sera alors question d'analyser l'état normatif de ce droit au sein de l'UE (Chapitre 3).

Chapitre 1 : La protection des données personnelles au niveau national

Bien qu'il existe aujourd'hui une certaine harmonisation européenne du droit à la protection des données personnelles, l'idée même de protéger ce droit est provenu d'évènements nationaux, ayant mené à la mise en place de telles dispositions, comme ce fut le cas en Allemagne et en France. Par ailleurs, la protection des données personnelles au niveau national peut émaner d'un texte rédigé par une organisation supranationale. C'est le cas de la Suisse. Il convient d'étudier l'introduction de la protection des données personnelles au niveau national au sein de l'UE (Section 1) en comparaison à la situation d'un Etat non-membre de l'UE (Section 2).

Section 1 : Le cas de deux Etats membres de l'UE : l'Allemagne et la France

Il convient dans un premier temps de comprendre les éléments nationaux ayant participé à l'introduction des dispositions allemande et française relatives à la protection des données personnelles (§1), avant d'étudier les divergences et similarités présentes au sein de ces textes (§2).

§1. Les cadres normatifs précurseurs en matière de protection des données

Les textes « précurseurs »[308] allemand et français relatifs à la protection des données sont intervenus avant toute disposition européenne en la matière. En Allemagne, dès 1970, plusieurs dispositions relatives à cette protection sont présentes au sein des *Länder*, Etats fédérés, c'est le cas du *Land* de Hesse. La *Bundesdatenschutzgesetz* (BDSG), littéralement traduite par la « loi fédérale allemande de

[308] Olivia Tambou, Manuel de droit européen de la protection des données à caractère personnel, Ed. Bruylant, 2020, p.1.

protection des données » a été adoptée en janvier 1977, il s'agit de la première loi nationale pour la protection des données personnelles en Europe.

Par une décision du 15 décembre 1983[309], la Cour constitutionnelle fédérale allemande déclare inconstitutionnels certains des articles d'une loi relative au recensement permettant au gouvernement allemand de recueillir des informations personnelles et de les partager aux collectivités territoriales et aux *Länder*. La Cour instaure alors le *Informationelle Selbstbestimmungsrecht,* littéralement traduit par « le droit à l'autodétermination informationnelle » pour toute personne dont les données ont été recueillies. Ce droit est interprété par la Cour fédérale comme une extension de la liberté individuelle présente dans la constitution fédérale[310].

La Cour est déjà consciente qu'il est « possible de créer une image complète et détaillée de la personne concernée - un profil de personnalité »[311], à travers un croisement de données, même anonymisées. Le législateur a dès lors, l'obligation de contrôler si un tel traitement des données entraîne l'étiquetage social[312] de la personne concernée et permet de classer les individus malades mentaux, délinquants, toxicomanes, etc. La Cour rappelle cependant que ce droit n'est pas absolu face aux intérêts publics notamment[313]. La Cour veille régulièrement à la constitutionnalité des lois relatives à un traitement des données.

En 2008[314], la Cour fédérale constitutionnelle déclare inconstitutionnelle une pratique de perquisition secrète en ligne, et institue un « droit fondamental à la confidentialité et l'intégrité des informations et des systèmes technologiques »[315] dans le cadre des droits généraux individuels consacrés par la constitution allemande. Les fichiers de police sont régis par les dispositions du *Bundeskriminalamt* (BKA), l'Office fédéral de la police judiciaire. En revanche, certaines dispositions de la BDSG s'appliquent, comme le droit d'accès aux données recueillies par les services de police judiciaire, sauf exceptions d'un intérêt public ou d'un intérêt tiers supérieur[316]. Alors qu'en Allemagne, le droit à la protection des données personnelles est issu d'un droit fondamentalement garanti par la constitution, en France, ce droit provient d'une affaire vivement contestée par l'opinion publique : l'affaire SAFARI. L'affaire SAFARI[317] a été le déclenchement d'un droit à la protection des données personnelles.

---

[309] Cour fédérale constitutionnelle (BVerfG), 1 BvR 209/83, le 15 décembre 1983, §2.
[310] Art.2 Constitution fédérale allemande (Grundgesetz) : « Chaque personne a le droit au libre développement de sa personnalité ».
[311] Cour fédérale constitutionnelle (BVerfG), 1 BvR 209/83, op. cit., §§93,108.
[312] Ibid., §160.
[313] Ibid., §148.
[314] BVerfG, 1 BvR 370/07, le 27 février 2008.
[315] Ibid., §166.
[316] §19 BDSG.
[317] L'acronyme SAFARI désigne « Système automatisé pour les fichiers administratifs et le répertoire des individus ».

L'administration française, lors du passage à l'informatique, met au point un fichier reposant sur le numéro de sécurité sociale du citoyen, permettant l'accès à tout un ensemble d'informations sur lui. Le 21 mars 1974, un article publié dans *Le Monde* rédigé par Philippe Boucher et intitulé « SAFARI ou la chasse aux français »[318] vient dévoiler ladite idée de fichier automatisé et provoque une polémique telle, que le projet fut stoppé. En réponse à la vive réaction du public, le 27 juin 1975, Bernard Tricot, conseiller d'Etat, écrit le rapport « de la Commission Informatique et Libertés » qui servira de base à la loi du 6 janvier 1978 « Informatique et libertés » créant la CNIL actuelle. Cette institution, prenant sa source à la suite d'une opinion publique majoritairement défavorable à un type de fichage des citoyens, devient la gardienne des libertés individuelles mises en danger par des systèmes informatiques en France.

Malgré une différence de contexte introductif de la notion de protection des données personnelles entre les deux Etats, le concept de protection des données à caractère personnel apparaît tout de même tôt.

§2. Les divergences et similarités au sein des deux cadres normatifs nationaux

La BDSG et la loi informatique et libertés sont appliquées respectivement au niveau national. Les deux lois sont entrées en vigueur uniquement à une année d'intervalle. Cependant, des différences de développement de la protection des données entre les dispositions allemande et française sont observables.

La BDSG utilise le terme *Daten*, signifiant littéralement « données », tel qu'actuellement omniprésent au sein des textes modernes de protection des données. En revanche au sein des dispositions françaises, elles sont nommées « informations ». Cette différence de terminologie démontre une certaine avance de la part de l'Allemagne. En effet, la différence entre le terme donnée et information réside dans le fait que par une donnée il est possible de créer de l'information. En informatique, la donnée est une « représentation de l'information dans un programme »[319]. Bien qu'au sein des situations factuelles régulées par ces dispositions, les termes « données » et « informations » soient synonymes, il est important de noter le souci de précision présent au sein de la BDSG.

Le traitement des données dont il est question au sein de l'ancienne loi allemande de protection des données, s'applique à n'importe quelle méthode de traitement des données prenant en compte « la conservation, le transfert, la modification, et la suppression des données »[320]. Le paragraphe 2 est

[318] L'article se situe en annexe du mémoire.
[319] Définition de la donnée informatique, https://fr.wikipedia.org/wiki/Donnée_(informatique).
[320] Ancien §2, BDSG.

applicable à ces traitements « quelles que soient les procédures utilisées »[321]. Cette expression démontre la volonté du législateur de couvrir un maximum de situations menant à un traitement abusif des données.

En France, le terme traitement automatisé des données est présent au sein de la loi informatique et libertés. Il s'étend à « la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements consultations ou communications d'info normatives »[322]. La description française du traitement automatisé des données, fait majoritairement allusion aux traitements informatiques du fait de la proximité temporelle de l'entrée en vigueur de la loi de 1978 à l'affaire « SAFARI » de 1974.

Ci-après un tableau comparatif des deux anciennes dispositions quant à la définition de traitement automatisé des données. En caractère gras figurent les termes similaires.

Allemagne	France
Ancienne *Bundesdatenschutzgesetz* (BDSG) 1977	Ancienne loi informatique et libertés 1978
Conservation, transfert, modification et **suppression.**	Collecte, enregistrement, élaboration, modification, **conservation** et **destruction.**

Outre les quelques divergences de forme, les droits protégés sont de même nature. En effet, les deux lois prévoient un droit à l'information du traitement des données, ainsi qu'une exception à ce droit lorsqu'il contrevient à un intérêt public supérieur ou lorsque le traitement des données est nécessaire au constat des infractions pénales[323]. Le droit à l'intégrité des données ainsi que leurs correction et suppression sont également régis par ces deux lois[324]. Des exceptions au droit de correction des données de nature pénales sont également prévues. En effet, la vérification et la correction des données sont effectués par l'intermédiaire de membres habilités et non directement par la personne concernée par des mesures pénales[325]. Les traitements automatisés des données par la justice ne sont autorisés, seulement s'ils possèdent une base légale[326], en matière d'informations renseignant des infractions, condamnations et mesures de suretés notamment[327].

[321] Ibid.: « Ungeachtet der dabei angewendeten Verfahren ».
[322] Ancien art. 5 Loi informatique et libertés.
[323] Ancien art. 27 Loi informatique et libertés ; Ancien §4 BDSG.
[324] Ancien art. 36 Loi informatique et libertés ; Ancien §4 BDSG.
[325] Anciens art. 29 et 39 Loi informatique et libertés ; §20 BDSG.
[326] Ancien art. 2 Loi informatique et libertés.
[327] Ancien art. 30 Loi informatique et libertés.

La loi française de 1978 prévoit d'ores et déjà au sein de la CNIL, une équipe pluridisciplinaire chargée de vérifier la protection des données personnelles[328]. L'Allemagne prévoit également une autorité de contrôle[329], mais n'en précise pas la qualité des membres la composant.

Les dispositifs d'IA tels qu'étudiés en première partie ne sont pas encore présents en matière pénale. Les traitements automatisés des données en la matière s'étendent concrètement à l'utilisation de fichiers de police. Les dispositifs de police prédictive tels que les outils prédictifs à disposition des policiers, sous forme de cartographies mises à jour régulièrement et utilisant des données de géolocalisation, sont apparus en Europe dans les années 1990[330]. Il est alors trop tôt dans les années 1970, d'inclure au sein d'un cadre normatif, des instruments couvrant la protection des données traitées par des technologies modernes. En revanche, il est intéressant d'observer une certaine concordance normative entre ces deux Etats, voisins certes, mais également membres de l'UE. Il convient d'étudier le cas de la Suisse, également voisin de l'Allemagne et la France, mais non membre de l'UE.

Section 2 : Le cas d'un Etat non-membre de l'UE : la Suisse

Les données personnelles sont protégées en Suisse initialement via l'article 13 de la constitution suisse relatif à la protection de la sphère privée. Avant 1993, il n'existe pas de loi relative à la protection des données ou informations personnelles en Suisse.

La loi fédérale suisse relative à la protection des données (LPD) est débattue par le parlement fédéral entre 1988 et 1992, puis entre en vigueur en 1993. Le terme de « données personnelles » ne figure pas dans le titre ni dans le champ d'application de la LPD, mais figure ensuite dans le corps du texte. En revanche la loi se prévaut dans le titre de protéger la « personnalité et les droits fondamentaux d'une personne ». Ce terme fort, est utilisé puisque l'entrée en vigueur de la loi intervient après la rédaction en 1981 de la Convention 108 par le Conseil de l'Europe, dont il sera question dans les développements suivants.

La LPD protège les personnes physiques et morales contre le traitement de leurs données par des personnes privées ou organes fédéraux. En revanche, le terme « organes fédéraux » n'inclut pas les autorités pénales traitant ces données en matière de procédure pénale ou d'entraide judiciaire internationale par exemple. La loi suisse définit le traitement des données comme « toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment

---

[328] Anciens art. 6 - 13 Loi informatique et libertés.
[329] Ancien §30 BDSG, « Aufsichtsbehörde ».
[330] Alexander Babuta, Session parlementaire européenne sur « L'intelligence artificielle au sein de la justice pénale et son utilisation par la police et les autorités judiciaires en matière pénale », le 20 février 2020, op. cit.

la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données »[331]. Cette définition est modernisée et fusionne les définitions initialement émises par l'Allemagne et la France. Cette disposition démontre la volonté du législateur de couvrir un maximum de situations faisant preuve d'un traitement abusif des données d'une part, et d'autre part, d'offrir une définition la plus moderne possible, dans les années 1990, période charnière pour les dispositifs informatiques de traitement des données[332].

Les droits protégés sont similaires à ceux prévus au sein des dispositions allemande et française. La LPD rajoute cependant avec pertinence les notions de bonne foi et de proportionnalité du traitement des données[333]. Ces principes sont à interpréter comme une limite « aux développements de certaines technologies pouvant porter atteinte à la dignité humaine »[334].

La loi suisse distingue les traitements provenant de personnes privées et ceux issus des organes fédéraux. Les traitements issus des autorités fédérales sous-entendent l'utilisation des données par les juridictions et institutions étatiques, elles sont licites si elles sont prévues par la loi[335]. La LPD prévoit également une autorité de contrôle du bon traitement des données personnelles[336], le préposé à la protection des données personnelles. Il est contrôlé par la Commission fédérale de la protection des données[337]. En revanche la qualité de ses membres n'est pas précisée.

En Suisse, le traitement automatisé des données en matière pénale est intrinsèquement lié à la coopération pénale transfrontalière, le « transfert » et la « communication » de données faisant partie intégrante de la définition du traitement en Suisse et en Allemagne. La confédération suisse se doit de posséder un niveau de protection « adéquat » à celui de ses voisins afin de continuer à bénéficier des avantages de la coopération judiciaire transfrontalière, à savoir le libre transfert des données et le traitement de données étrangères dans le cadre d'enquêtes judiciaires notamment.

Les législateurs des trois Etats dirigent ainsi l'idée d'une protection des données personnelles en matière de coopération judiciaire internationale, qu'il serait question de mettre en place au niveau supranational. Se fait ressentir alors un besoin d'harmonie continentale d'une telle protection des données.

---

[331] Art. 3, e. LPD.
[332] Voir Partie 1, Titre 1, Chapitre 1, section 1.
[333] Art. 4§2 LPD.
[334] Olivia Tambou, op. cit. p. 119.
[335] Art. 17 LPD.
[336] Ibid., Art. 26-32.
[337] Ibid., Art. 33.

Chapitre 2 : Le Conseil de l'Europe axé sur les droits de l'Homme

Le Conseil de l'Europe a publié en 1981 la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, que l'on citera « convention 108 ». Il s'agit du premier texte européen traitant de la protection des données personnelles. La convention 108 est ouverte en ce qu'elle permet à tout Etat ayant une législation conforme d'y adhérer. En outre, elle emploie le terme « traitement automatisé des données à caractère personnel », ce qui révèle une prise de conscience de la part du Conseil de l'Europe de l'incidence que l'informatique et les technologies a sur ce droit à la protection des données personnelles.

Ce texte est une harmonisation du droit à la protection des données personnelles au niveau européen. Par ailleurs, la sauvegarde des droits de l'Homme étant le fil rouge de cette organisation internationale, la protection des données à caractère personnel devient un droit fondamental. Il convient d'étudier la dimension fondamentale apportée à la protection des données personnelles (Section 1) afin d'en appréhender les limites face au contexte digital prenant de plus en plus de place au sein de la justice pénale notamment (Section 2).

Section 1 : La dimension fondamentale de la protection des données personnelles

La Convention 108 est présentée aux parties en 1981 et est entrée en vigueur le 1er octobre 1985. Via ce texte, le Conseil de l'Europe a souhaité s'assurer de la bonne mise en place d'un droit universel à la protection des données personnelles, pour « favoriser un espace démocratique et juridique commun organisé autour de la Convention en ce compris, le droit au respect de la vie privée »[338]. Le fait que cette convention puisse être invoquée devant la CEDH permet aux individus de saisir la Cour en exerçant leur droit à un recours individuel qu'ils n'auraient pas pu épuiser devant une autre juridiction internationale.

La convention 108 devient pour certains Etats membres du Conseil de l'Europe, le seul texte réellement contraignant en matière de la protection des données. Ce fut le cas de la Suisse[339]. La CEDH affirme plus tard que la notion de données à caractère personnel est issue du concept de vie privée prévu par l'article 8 de la ConvEDH, mais ne doit en revanche pas être limité à la sphère privée[340]. La convention 108 reprend des principes nationaux de la protection des données – tels que les principes de loyauté, de licéité, de finalité, de qualité et de proportionnalité[341] – et les harmonise

---

[338] Catherine Forget, « La protection des données dans le secteur de la police et de la justice », dans Le règlement général sur la protection des données (RGPD/GDPR), Ed. Larcier, 2018, p. 870.
[339] Office fédéral de la Justice (Suisse), « Esquisse d'acte normatif relative à la révision de la loi sur la protection des données », 29 octobre 2014, p.4
[340] CEDH, *Amann c. Suisse*, 16 février 2000, n° 27798/95, §65.
[341] Art. 5, convention 108.

à la protection européenne des données lors d'un traitement automatisé. Des exceptions à ces principes dans le cadre de la lutte contre « la répression des infractions pénales »[342].

Le Conseil de l'Europe demeure tout de même conscient des risques que les exceptions au principe fondamental de la protection des données peuvent avoir sur les individus faisant l'objet d'une répression pénale. Afin de garantir à ces individus un niveau minimum de protection, le comité des ministres du Conseil de l'Europe rédige la recommandation R(87)15, visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police[343], s'inspirant de la convention 108. Cette recommandation permet d'éviter tout abus de traitement des données à caractère personnel des personnes concernées par une enquête ou répression pénale, sur la seule base de l'article 9 de la Convention 108.

Dès le préambule de cette recommandation, le Conseil de l'Europe rappelle que « c'est dans ce secteur, en effet, que les conséquences d'une violation des principes de base énoncés dans la convention 108 pourraient peser le plus lourdement sur l'individu »[344] et que l'équilibre entre la prévention, la répression d'infractions et la protection des données personnelles de l'individu est « difficile à obtenir dans le secteur de la police »[345]. Les points forts de cette recommandation résident dans la prise de conscience par le comité des ministres de l'étendue des données personnelles, au-delà de l'article 8 de la ConvEDH disposant de la vie privée au sens stricte[346]. L'ensemble des données permettant l'identification de l'individu est concerné.

Il convient cependant d'étudier les limites propres à ce texte et les enjeux émergents à l'époque, c'est-à-dire dans les années 1990.

Section 2 : Les limites de ce cadre normatif

Deux limites sont visibles. La première est formelle, elle concerne l'absence de caractère contraignant de la recommandation pourtant nécessaire en ce qu'elle aurait pu être le point de départ de textes nationaux relatifs au traitement automatisé des données par les autorités de police. La seconde est matérielle, en ce qu'elle emploie des termes larges. La première phrase du préambule fait l'éloge d'une technologie facilitant le travail de la police[347].

---

[342] Ibid., art. 9.
[343] Comité des ministres du Conseil de l'Europe, Recommandation (87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, le 15 septembre 1987.
[344] Ibid., préambule.
[345] Ibid.
[346] CEDH, *Malone c. Royaume-Uni*, op. cit., §64 : les écoutes téléphoniques font partie de la sphère privée au sens strict de l'article 8 de la ConvEDH.
[347] Préambule R(87)15 : « La technologie facilite à l'évidence l'action de la police ».

En revanche, la recommandation R(87)15 puise sa matière dans l'interprétation de l'article 9 de la Convention 108, excluant certains droit de la protection des données personnelles lors de mesures nécessaire à la « répression d'infractions pénales »[348], mais ne vise uniquement les « autorités de police » alors que la répression pénale est également effectuée par l'ordre judiciaire. Cette occultation peut s'expliquer par le fait que les « technologies » des années 1980-1990, au sens de celles sous-entendues dans le préambule, ne concernaient pas encore les juridictions pénales.

Il est pertinent de s'intéresser à la façon dont l'UE, une autre organisation supranationale européenne, organise la protection des données face à un traitement automatisé en matière pénale.

Chapitre 3 : L'UE : conciliatrice de deux idéologies communautaires

Contrairement au Conseil de l'Europe, dont les droits de l'Homme sont la ligne directrice, l'UE est « tiraillée entre le besoin d'assurer les flux transfrontières dans le cadre de la coopération policière et judiciaire tout en garantissant la protection des données »[349]. Il est nécessaire d'appréhender les textes encadrant la protection des données dans un contexte de transfert des données en matière de coopération pénale transfrontalière notamment (Section 1), avant d'en distinguer les limites et les enjeux de modernité (Section 2).

Section 1 : L'équilibre nécessaire entre le transfert et la protection des données

Entre 1992 et 2007[350], la protection des données à caractère personnel au sein de l'UE est répartie parmi les trois piliers de l'organisation, à savoir, le marché intérieur, la politique étrangère et de sécurité commune (PESC) et la coopération policière et judiciaire. La directive relative à la protection des données à l'égard du traitement des données personnelles et à la libre circulation de ces données, dite « directive 95/46/CE »[351], est applicable uniquement au domaine du marché intérieur. Ainsi, la protection des donnés dans le domaine pénal demeurait alors la prérogative de puissance publique des Etats membres[352]. Le début des années 2000 représente un contexte propice au développement d'une « vague sécuritaire »[353] entrainant une multitude de traitements des données personnelles par les autorités de police. La situation ne s'améliore pas lorsque des Etats membres de l'UE sont également touchés par des attentats terroristes, notamment à Londres et Madrid en 2004 et 2005.

---

[348] Art. 9§2, a. Convention 108.
[349] Catherine Forget, op. cit., p. 870.
[350] De l'entrée en vigueur du traité de Maastricht, mettant en place les trois piliers, au traité de Lisbonne.
[351] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[352] Art. 3, Dir 95/46/CE.
[353] Voir Partie I, Titre 1, p.12 : Alex Türk.

Il était alors nécessaire de recourir à un texte permettant de protéger les données personnelles contre un traitement abusif de la part des autorités de police. Cette protection ne figurait uniquement au sein de la recommandation R(87)15 du Conseil de l'Europe, datant de 1987 et était dépourvue d'effet juridique contraignant. En 2004, le contrôleur européen à la protection des données (CEPD) est créé, il permet de protéger les personnes physiques contre tout traitement abusif de leurs données personnelles de la part des institutions et organes de l'UE. En revanche, le traitement des données en matière pénale demeure de la compétence des Etats membres. En 2008, le Conseil de l'UE rédige une décision-cadre relative à la protection des données personnelles traitées dans le cadre de la coopération policière et judiciaire en matière pénale, dite « décision-cadre 2008/977/JAI »[354]. Des limites à ce cadre normatif subsistent.

Section 2 : Les limites de ce cadre normatif

Au regard de la décision-cadre 2008/977/JAI, des limites formelles et matérielles sont présentes. Du point de vue formel, il est prévu par le Traité de l'UE (TUE) que « les décisions-cadres lient les États membres quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens. Elles ne peuvent entraîner d'effet direct »[355]. Ce sont des « instruments de la coopération intergouvernementale et non de la méthode communautaire »[356]. Ainsi, cela consiste en pratique à laisser une marge de manœuvre dans l'application de la décision au niveau national contrevenant à l'efficacité et à la finalité de cette décision visant une protection harmonieuse des données personnelles traitées en matière de coopération pénale par l'ensemble des Etats membres.

D'autre part, sur le fond de la décision-cadre, le CEPD regrette avant même l'entrée en vigueur de cette décision-cadre « un déséquilibre patent en faveur des impératifs de sécurité publique et au détriment de la protection des droits fondamentaux »[357]. En outre, le CEPD reproche également l'absence des traitements de données effectués sur le territoire des Etats membres dans le champ d'application de la décision-cadre pourtant souhaité par « le Parlement européen, la Conférence des autorités européennes de protection des données, et même le Comité consultatif T-PD du Conseil de l'Europe »[358].

---

[354] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.
[355] Art. 34§2, Traité de l'Union Européenne.
[356] Monika Szwarc, « Le caractère juridique de la coopération judiciaire en matière pénale et de la coopération policière (IIIe pilier) à la lumière du Traité constitutionnel pour l'Europe », Revue Electronique Nice, le 15 mars 2006, p.6.
[357] Catherine Forget, op. cit., pp. 869-870. Voir aussi : CEPD, avis du 27 avril 2007.
[358] Journal Officiel de l'UE, avis du CEPD n°C139/1 du 23 juin 2007, §§16-17.

La protection des données personnelles était déjà encadrée de manière générale, par la directive 95/46/CE ainsi que constitutionnalisée et garantie par la Cour de Justice de l'UE (CJUE)[359]. Ainsi, un cadre normatif relatif à la protection des données expressément prévu pour la matière tant policière et judicaire qu'en matière de coopération pénale provenant de l'UE en tant qu'organisation supranationale, était nécessaire, dans un but d'harmonisation de cette matière.

Titre II : L'évolution des normes et un besoin d'anticipation (à partir de 2016)

L'année 2016 marque le tournant de la protection des données personnelles au niveau européen. La protection des données personnelles est au centre de l'intérêt normatif européen. Le marché de l'IA s'étend dans la décennie 2000-2010 et la confiance envers les dispositifs d'IA devient nécessaire. L'année 2016 symbolise ainsi le point de départ de l'éclosion d'un débat « ouvert et éclairé sur l'éthique numérique, qui permet à l'Union européenne de concrétiser les avantages de la technologie pour la société et l'économie, tout en renforçant les droits et libertés des personnes, en particulier leurs droits au respect de la vie privée et à la protection des données »[360]. Il convient dans ce titre de saluer cette « vague éthique » dont nous sommes témoins, afin d'en tirer les conséquences et la réalité des limites toujours présentes dans l'encadrement des données personnelles au sein de l'utilisation de l'IA en matière répressive. A ce titre, l'évolution normative depuis 2016 s'est proliférée depuis l'UE (Chapitre 1) puis s'est développée au sein du Conseil de l'Europe (Chapitre 2) avant de réellement s'ancrer au niveau national (Chapitre 3).

Chapitre 1 : 2016, l'année phare de la protection des données pour l'UE

Le traitement automatisé des données personnelles par l'IA devient évident dans plusieurs domaines, tant au sein des stratégies commerciales qu'en matière médicale. La matière pénale n'y échappe pas et les dispositifs d'IA tendent à s'installer dans le marché de la prévention et de la répression d'infractions pénales. Il devient alors nécessaire de gagner la confiance des dispositifs d'IA afin de ne pas contrevenir au renforcement de la protection des données personnelles (Section 1). Ce cadre normatif possède cependant des limites face aux enjeux d'un futur proche (Section 2).

[359] Sylvie Peyrou, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la C.J.U.E », in Protection des droits fondamentaux dans l'Union européenne, Ed. Bruylant, 2015 p. 229.
[360] CEPD, décision du 3 décembre 2015 instituant un groupe consultatif externe sur les dimensions éthiques de la protection des données, cons. 5.

Section 1 : Le renforcement de la protection des données traitées par l'IA

L'UE renforce la protection des données à caractère personnel tel qu'un concept général et répond à un besoin de sécurité juridique en matière de traitement automatisé des données au sein du domaine de prévention et de répression pénale (§1). Parallèlement à cette montée en puissance de la protection des données, l'UE entreprend plusieurs projets permettant de garantir l'éthique de l'IA (§2).

§1. La solidification de la protection des données personnelles en matière pénale

Le 27 avril 2016, le règlement général relatif à la protection des données à caractère personnel (RGPD) est présenté par l'UE. Il remplace la directive 95/46/CE évoquée et est accompagné par la directive dite « Police-Justice », également mentionnée, remplaçant la décision-cadre 2008/977/JAI. La directive doit être transposée au sein des dispositions nationales des Etats membres pour le 6 mai 2018 et le RGPD entre en vigueur le 25 mai 2018. Ces deux textes fondent le « paquet européen de protection des données personnelles »[361].

Le RGPD ne s'applique pas au domaine du traitement des données personnelles en matière de prévention et de répression pénale. Cependant, dès les considérants du RGPD, il est fait état des exceptions aux droits découlant de la protection des données en matière de prévention et de répression pénale[362]. Par ailleurs, la directive calque la structure et la logique du RGPD[363], cependant, elle ajuste ses dispositions à la matière pénale. A titre d'information, le principe de transparence, n'apparaît pas au sein de la directive. Une telle adaptation permet de ne pas contrevenir à la garantie de libre flux transfrontières des données en matière de coopération pénale, notamment.

Le champ d'application de la directive Police-Justice, possède une étendue plus large que celle de la décision-cadre de 2008 précédemment étudiée. Alors que la décision-cadre concernait les « autorités de répression », la nouvelle directive emploie le terme « autorités compétentes » et couvre ainsi les activités des autorités policières, judiciaires[364] ainsi que tout organisme disposant de prérogatives de puissance publique[365]. Par le terme « prévention des infractions pénales » présent dans le titre de la directive, sont sous entendues les enquêtes judiciaires, ainsi que toute activités allant « au-delà de ce cadre pour acquérir une meilleure compréhension de certains phénomènes »[366]. La directive concerne également le traitement des données personnelles lors de prévention des infractions pénales, liée à la prérogative de maintien de l'ordre public, lors de rassemblements évènementiels notamment. De tels

---

[361] CNIL, « Le cadre européen », https://www.cnil.fr/en/node/114099.
[362] A titre d'exemple, voir considérant 73 : exceptions aux droits à l'information, d'accès aux données, de rectification, etc.
[363] Catherine Forget, op. cit., p.872.
[364] Cons. 20 Directive Police-Justice.
[365] Cons. 11 Directive Police-Justice.
[366] Cons. 27 Directive Police-Justice.

traitements de données renvoient à l'idée de surveillance publique ayant eu lieu dans plusieurs projets de « smart cities » en France, étudiés en première partie. Cette disposition pourrait être interprétée comme l'ouverture au développement d'expérimentations impliquant l'IA telles que l'expérience de reconnaissance faciale entreprise par la ville de Nice lors du carnaval de 2019. La directive Police-Justice concerne les traitements automatisés utilisés pour anticiper les comportements déviants de profils particuliers[367]. L'UE est consciente de l'utilisation de dispositifs d'IA par les autorités compétentes à la prévention et la répression pénale. En effet, le parlement européen a consacré une session parlementaire à ce sujet[368].

Il est important de saluer la pluridisciplinarité des intervenants, et l'émergence au sein du débat des règles éthiques à respecter lors de la conception des dispositifs d'IA en question.

§2. La nécessité d'éthique pour une IA digne de confiance

Les dispositifs d'IA peuvent être utiles à la prévention et à la répression pénale. En revanche, l'opacité de l'IA fait débat et entraîne une réticence. Certaines formes d'IA peuvent difficilement être évaluées comme compatibles aux règlementations européennes. La Commission rappelle les dangers de l'opacité, la complexité, l'imprévisibilité et le comportement partiellement autonome. De ce fait, « les particuliers et les entités juridiques peuvent se heurter à des difficultés en ce qui concerne l'accès effectif à la justice lorsque ces décisions sont susceptibles d'avoir des effets négatifs pour eux »[369].

Afin d'instaurer une certaine confiance envers les instruments d'IA de manière générale et de déterminer les critères déterminants d'une IA « *trustworthy* »[370] soit, digne de confiance, l'UE crée de nombreux projets visant à renforcer le caractère éthique de l'IA. Selon le groupe d'experts de haut niveau de l'UE, une IA digne de confiance doit respecter sept caractéristiques éthiques[371] à inclure au sein même de la conception de dispositifs d'IA. En ce qui concerne les dispositifs utilisés en matière pénale, sont retenus des caractéristiques de nature pluridisciplinaire – parfois empiétant sur des thèmes philosophiques et sociaux.

L'agentivité représente l'inclusion des droits fondamentaux et une certaine résistance humaine aux opportunités et choix disponibles nous étant imposés. **La transparence et la protection des données personnelles** via la garantie de l'intégrité et la qualité des données doivent être inclues lors du

[367] Catherine Forget, op. cit., p. 28.
[368] Session parlementaire européenne du 20.02.2020 sur « L'intelligence artificielle au sein de la justice pénale et son utilisation par la police et les autorités judiciaires en matière pénale ».
[369] Commission européenne, Livre blanc sur l'intelligence artificielle, le 19 février 2020, p. 14.
[370] Commission européenne, HLEU Group, « Ethics guidelines for trustworthy AI », avril 2019.
[371] Ibid., pp. 14-15.

processus de développement des dispositifs d'IA. Enfin, **la responsabilité, de l'anglais « *accountability* »** devrait également figurer au sein même de la création de l'IA.

En revanche, de tels projets sont critiquables et ne peuvent à eux seuls suffire de garanties face à l'utilisation de l'IA en matière de prévention et de répression pénale.

Section 2 : Les limites de ce cadre normatif

Plusieurs limites de la directive Police-Justice ont été soulevées, à savoir des termes étant parfois vagues et pouvant laisser une trop grande marge de manœuvre aux Etats membres dans leurs interprétations des dispositions. C'est le cas du terme « menace » n'étant pas expressément défini au sein de la directive.

Professeur Catherine Forget craint qu'une absence de définition claire des termes compris dans le champ d'application de la directive ne dérive en une interprétation extensive de la part de certains Etats membres, qui pourraient inclure la protection de la sécurité nationale sous l'égide de cette directive[372]. La directive exclut pourtant de son champ d'application les questions de sécurité nationale[373]. Cependant, le terme « sécurité nationale » n'est pas clairement définie ni par les traités de l'UE, ni par la jurisprudence de la CJUE. En revanche, une limite à la flexibilité de ce terme est reconnue par la CEDH[374].

Par ailleurs, il est toujours difficile de maintenir l'équilibre entre les intérêts individuels de protection des données et le besoin d'efficacité des autorités de répression pénale par la technologie, cela est en partie lié à l'opacité des dispositifs d'IA. La notion de transparence n'est d'ailleurs pas évoquée au sein de la directive.

Enfin, les directions d'une IA éthique de manière générale sont à saluer. En revanche, il convient également d'en appréhender les enjeux de manière spécifique. Le Conseil de l'Europe en a également pris conscience.

---

[372] Catherine Forget, op. cit., pp. 876-877.
[373] Cons. 14 Directive Police-Justice.
[374] CEDH, *Esbester c. Royaume-Uni*, n° 18601/91, 2 avril 1993, pp. 10-11 : « L'expression "sécurité nationale" ne se prête pas à une définition exhaustive et étant donné que l'étendue et les modalités d'exercice des fonctions du service de sécurité sont suffisamment indiquées ».

Chapitre 2 : Les enjeux de l'IA : renforcement de la protection des données personnelles

L'éthique est également présente au sein du Conseil de l'Europe. En tant qu'organisation travaillant sur les nouveaux enjeux sociétaux pouvant affecter les droits de l'Homme, le Conseil de l'Europe ne pouvait passer outre une étude de l'IA liée à la protection des données à caractère personnel. Le conseil de l'Europe est conscient des avantages de l'IA dans plusieurs domaines, y compris dans le domaine de la prévention des infractions[375]. Les nouveaux enjeux issus de l'utilisation de dispositifs d'IA sont pris en compte au sein de nouveaux textes et projets (Section 1). Cependant, il demeure des limites à ces évolutions (Section 2).

Section 1 : Les nouveaux risques nécessitant d'un nouvel encadrement

En mai 2018, le Conseil de l'Europe a présenté une version modernisée de la convention 108, intitulée « convention 108+ »[376]. La nouvelle convention reprend les principes de la convention 108. Elle préserve son aspect « général et technologiquement neutre »[377] et sa nature universelle. Elle se donne en effet pour objectif de répondre aux nouveaux défis « nés de l'usage de nouvelles technologies de l'information »[378] sans pour autant citer le terme d'IA au sein de ses dispositions. Le Conseil de l'Europe rappelle cependant que l'IA est concernée par cette nouvelle convention[379].

Par ailleurs, la convention 108+ est également créée afin de renforcer le contrôle de la mise en œuvre des mesures prévues pour une meilleure prise en compte des droits des individus concernés par le traitement. À titre d'exemple, le responsable de traitement doit prévoir « un examen de l'impact potentiel du traitement »[380] et les autorités de contrôle se voient accorder un renforcement de leur indépendance[381]. En outre, un nouveau chapitre concernant la coopération et l'entraide entre les parties est introduit afin de renforcer la mise en œuvre efficace de la Convention. Ce texte demeure un aperçu général de la protection des données traitées par les nouvelles technologies.

---

[375] Comité consultatif de la Convention 108, « Guidelines on Artificial Intelligence and data protection », Conseil de l'Europe, 25 janvier 2019, T-PD(2019)01, p. 1.
[376] Comité des ministres du Conseil de l'Europe, « Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel », Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, adopté par le Comité des Ministres lors de sa 128e session à Elseneur, le 18 mai 2018.
[377] Comité des ministres du Conseil de l'Europe, Rapport explicatif de la Convention 108+, p.17.
[378] Ibid., p. 40.
[379] Comité consultatif de la Convention 108, « Lignes directrices sur l'Intelligence Artificielle et la protection des données à caractère personnel », 25 janvier 2019, p. 1 : « Un développement de l'IA reposant sur le traitement de données à caractère personnel devrait être fondé sur les principes figurant dans la Convention 108 + ».
[380] Art. 10 Convention 108+.
[381] Art. 15§5 Ibid.

Le Conseil de l'Europe est cependant conscient des nouveaux enjeux de l'utilisation des données personnelles par des dispositifs intelligents. Notamment dans le secteur de prévention et de répression des infractions en matières policière et judiciaire.

Le comité consultatif de la convention 108, précédemment mentionné, est conscient des risques de l'utilisation des données par la police. En 2018, il publie un guide pratique sur l'utilisation des données à caractère personnel dans le secteur de la police[382]. Ce guide permet finalement de comprendre l'ensemble des risques et enjeux, étudiés en deuxième partie, auxquels doivent faire face les autorités chargées d'appliquer la loi. Plusieurs directions sont émises, afin de permettre un traitement automatisé des données témoignant d'une fiabilité. Le terme « *privacy by design* »[383] est repris et sollicite une réelle prise de conscience par les gouvernements du besoin d'introduire le respect des droits fondamentaux, en l'occurrence, de la protection des données à caractère personnel, au sein des outils techniques utilisés par la police. Le terme d'IA n'est pas expressément employé.

La même année, le Conseil de l'Europe fonde la Commission européenne pour l'efficacité de la Justice (CEPEJ). Laquelle dresse une « charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement »[384]. Par cette charte, elle fait preuve d'un pragmatisme en ce qu'elle cite expressément l'usage de l'IA au sein du système judiciaire et évoque au sein de cette dernière, la présence de dispositifs de police prédictive notamment. Elle évoque également la volonté d'imposer la présence de personnes aux profils multidisciplinaires au sein des sociétés de conception d'IA, afin de sécuriser les données[385].

Ce droit souple fait état de cinq principes fondamentaux à la protection des droits en la matière. Les trois derniers principes, à savoir, la « qualité et sécurité », la « transparence, neutralité et intégrité intellectuelle » et la « maîtrise par l'utilisateur » viennent renforcer directement la protection des données personnelles utilisées par l'IA.

---

[382] Comité consultatif de la Convention 108, « Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police », Conseil de l'Europe, 15 février 2018.
[383] Ibid., p. 19.
[384] CEPEJ, Charte éthique européenne d'utilisation de l'IA dans les systèmes judiciaires et leur environnement, Conseil de l'Europe, 3-4 décembre 2018.
[385] Ibid., p. 10.

Section 2 : Les limites de cette évolution normative

Le cadre normatif du Conseil de l'Europe, concentré sur les droits de l'Homme, est pragmatique du fait d'une prise de conscience des risques pour la protection des données traitées par l'IA en matière pénale. Il est cependant encore tôt pour observer une réelle amélioration émanant de ce nouveau cadre. A titre d'exemple, la convention 108+ n'a obtenu que cinq ratifications pour l'instant[386]. De plus, la Cour Européenne des droits de l'Homme n'a pas encore eu l'opportunité de statuer sur un cas traitant de l'IA utilisée en matière pénale. Il convient d'étudier les conséquences nationales de ces nouveaux cadres normatifs européens.

Chapitre 3 : L'incidence du nouveau cadre normatif européen au niveau national

Face à ce nouveau panel normatif – tant au sein de l'UE que du Conseil de l'Europe – corrélé à l'usage croissant des dispositifs d'IA au sein de la matière pénale, les Etats se doivent d'appliquer ces principes protecteurs en droit interne. Il convient d'observer les mises en œuvre au niveau national du nouveau cadre normatif européen au sein de l'Allemagne et la France en tant qu'Etats membres de l'UE (Section 1), puis au sein du droit suisse (Section 2). Enfin, un constat sur les ambitions futures des trois Etats sera effectué (Section 3)

Section 1 : L'adaptation des droits allemand et français au nouveau cadre européen

Les dispositions nationales en adoptant ce nouveau panel juridique européen, adaptent leurs dispositions aux « réalités du monde en ligne et à certaines pratiques d'utilisation »[387]. Il convient d'étudier l'adaptation nationales des textes européens au sein d'Etats membres de l'UE (§1) et d'en comprendre les limites (§2).

§1. L'adaptation nationale des textes européens au sein d'Etats membres de l'UE

En 2017 et en 2019, l'Allemagne adopte deux lois d'adaptation de la BDSG aux dispositions de la directive Police-Justice. La transposition de la directive est prévue à la partie 3 de la BDSG, soit au sein de 38 articles. En 2018, la France adopte une ordonnance portant sur la modification de la loi informatique et liberté du 6 janvier 1978. Le titre III est consacré à la transposition de la directive Police-Justice, soit 27 articles reprenant l'ensemble des dispositions relatives aux obligation des autorités compétentes, aux droits des personnes concernées et au transfert des données vers un pays tiers.

---

[386] Etat des ratifications de la Convention 108+, au 10 août 2020.

[387] Yannick Meneceur, « Intelligence Artificielle et droits fondamentaux », dans Patrick Gielen et Marc Schmitz, Avoirs dématérialisés et exécution forcée, Novembre 2019, Ed. Bruylant, p. 121.

§2. Les limites à ces adaptations nationales

La directive Police-Justice laisse une importante marge de manœuvre aux Etats-membres et renforce l'hétérogénéité de la protection des données au niveau national. En revanche, la régulation de l'IA en matière pénale au niveau national, se voit limitée. Il s'agit de mettre en œuvre de nouvelles mesures pratiques et non uniquement théoriques afin de vérifier le fonctionnement des algorithmes. « On a tout à fait conscience des limites de ce que l'on peut faire actuellement. Il est absolument nécessaire de développer des contrôles plus automatisés qui permettent de vérifier la loyauté des algorithmes »[388]. C'est également dans une optique d'anticipation des risques pouvant découler de l'IA en matière de prévention des infractions notamment, qu'Anne Souvira, commissaire divisionnaire chargée de mission aux questions liées à la cybercriminalité au cabinet du préfet de police, rappelle que « ces outils sont indéfiniment développables. On aura toujours de plus en plus de choses si aujourd'hui on ne se mêle pas d'envisager par anticipation leur régulation »[389].

D'un point de vue d'anticipation pratique, Professeur Emmanuel Dreyer prend l'exemple de l'enquête de personnalité lors de la décision du quantum de la peine d'un individu. L'IA permettrait une meilleure individualisation de la peine, en ce que l'enquête de personnalité serait de meilleure qualité, à l'aide du procédé de recoupement d'informations, notamment. « Elles ne seront plus l'apanage des procès criminels, car automatisées, elles pourront être facilement obtenues des services pénitentiaires d'insertion et de probation qu'ils réaliseront par ordinateur »[390]. Cependant, le caractère qualitatif de ces procédés dépend de la « fiabilité des bases de données [factuelles] à partir desquels les recoupements pourront être effectués »[391]. Le professeur estime que le savoir criminologique français nécessaire à une telle qualité de traitement des données pour réaliser un processus intelligent de qualité n'est pas assez développé. Il regrette que le budget de l'Etat ne puisse être suffisant aux dépenses nécessaires. Ainsi, il en conclu que « c'est peut-être là que réside la véritable naïveté »[392].

Par ailleurs, l'efficacité de la protection des données utilisées par l'IA en matière pénale sur le territoire européen est également de faire en sorte que les Etats non-membres de l'UE puissent avoir un niveau de protection équivalent sur leur territoire.

---

[388] Laura Fernandez Rodriguez, « Algorithmes : la France se mobilise pour plus de transparence », Usbek et Rica, 21 février 2017.
[389] Anne Souvira, Séminaire « Intelligence artificielle et justice », Université Paris 5 Descartes, 2 avril 2019.
[390] Emmanuel Dreyer, « L'Intelligence artificielle et le droit pénal », dans Alexandra Bensamoun et Grégoire Loiseau, Le droit et l'intelligence artificielle, Ed. LGDJ, 219, pp. 230-231.
[391] Ibid., p. 231.
[392] Ibid.

Section 2 : L'adaptation du droit suisse au nouveau cadre européen

Il convient d'étudier l'adaptation du droit suisse aux nouvelles mesures européennes de protection des données en matière de coopération pénale notamment (§1), afin d'en comprendre les limites (§2).

§1. L'adaptation des textes nationaux et les nouvelles mesures nécessaires

Afin pour la Suisse d'appliquer les mesures issues du nouveau cadre protecteur des données adopté au sein de l'UE, la Commission européenne doit attester qu'il existe sur le territoire suisse un « niveau de protection substantiellement équivalent », le niveau ne pouvant être totalement identique[393]. Ce fut le cas en 2000[394]. La directive Police-Justice a été notifiée à la Suisse en tant que développement de l'Acquis de Schengen[395].

Depuis l'entrée en vigueur de la directive Police-Justice et du RGPD, la Suisse procède à une révision complète de la loi pour la protection des données (LPD). Cette dernière a pour projet de renforcer les dispositions légales fédérales relatives à la protection des données, afin de faire face au développement des nouvelles technologies et d'adopter ces mêmes dispositions aux références du Conseil de l'Europe et de l'UE. En revanche, cette loi ne concernera pas le traitement automatisé des données personnelles en matière pénale et de coopération judiciaire. La Suisse a décidé le 28 septembre 2018 de consacrer une loi à la transposition de la directive Police-Justice[396].

Cette loi entrée en vigueur le 1er mars 2019, se présente sous la forme de deux rubriques. Les principales modifications apportées par cette loi de transposition au droit suisse comprennent notamment le renforcement de l'indépendance du préposé fédéral à la protection des données personnelles (autorité de contrôle suisse pour la protection des données) et la préservation d'un niveau « équivalent » des règles de protection des données pour la communication d'informations entre les autorités compétentes suisses et d'Etats tiers liés à la Suisse par les accords Schengen[397]. En revanche, des lacunes en matière d'encadrement des dispositifs d'IA sont observées en Suisse. Il s'agit de comprendre d'où proviennent ces difficultés d'adaptation.

---

[393] Conclusions de l'avocat général à la décision *Schrems* de la CJUE op. cit., pt. 141, sur l'interprétation du terme de « niveau de protection adéquat » présent la directive 95/46/CE précédant le RGPD dans l'UE.
[394] Commission européenne, décision d'adéquation du 26 juillet 2000, n° 2000/518/CE, relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse.
[395] Cons. 102 et 103 Directive Police-Justice.
[396] Loi fédérale du 28 septembre 2018 mettant en œuvre la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (Développement de l'acquis de Schengen).
[397] Art. 349b code pénal suisse.

§2. Les limites à l'adaptation des dispositions suisses aux normes européennes

La révision de manière générale de la protection des données personnelles en Suisse est délicate et cela pourrait impacter la protection spéciale des données personnelles, à savoir en matière pénale. Les limites concernant l'adaptation du droit suisse au nouveau cadre européen de la protection des données résident dans une crainte de ne pas pouvoir transposer de manière optimale le RGPD en suisse. La Suisse se trouve actuellement dans une impasse en matière de droit à la protection des données. La LPD date de 1992 soit il y a près de trente ans. Le parlement de la confédération suisse travaille actuellement sur un projet de réforme de la LPD. Le préposé fédéral à la protection des données est dans l'attente de ce nouveau texte et espère que le projet aboutira en une « heureuse conclusion » [398] en automne 2020, pour entrer en vigueur au plus tard en début d'année 2022.

La révision du droit à la protection générale des données calquée sur le RGPD est problématique pour la Suisse. François Charlet cite quelques exemples de situations difficiles non mentionnées par le parlement européen. Notamment, dans une situation où une société privée ne respecte pas les règles de protection des données, « comment les amendes administratives et autres mesures correctives seront-elles appliquées si elles sont imposées à des organisations suisses qui n'ont pas d'établissement dans l'UE ? Afin de protéger la souveraineté suisse, des accords devront être signés (s'ils ne le sont pas déjà) avec la Commission européenne et les États membres. Il doit être clairement précisé que le préposé à la protection des données personnelles n'appliquera pas la RGPD aux organisations suisses » [399]. Dans cette situation, le RGPD pourrait-il ne pas être opposable aux sociétés suisses ? Si tel est le cas, la Suisse craint alors que ses dispositions relatives à la protection générale des données personnelles ne soient plus en adéquation avec celles de l'UE.

Par ailleurs, la confédération suisse est d'autant plus perturbée par l'invalidation par la CJUE, le 16 juillet dernier[400] du bouclier de la protection des données (privacy shiled) entre les Etats-Unis et l'UE, puisqu'elle possède un instrument similaire avec les Etats-Unis. En l'absence d'une base solide de protection des données de manière générale en Suisse, l'encadrement de l'IA est d'autant plus complexe. En effet, le concept même de « privacy by design » voudrait qu'une règlementation de la protection des données personnelles n'est efficace que si elle est complétée par des opérations de protection inhérentes à la fabrication de dispositifs d'IA.

[398] Yannick Chavanne, « Révision de la LPD : le préposé fédéral à la protection des données s'impatiente », le 30 juin 2020.
[399] François Charlet, « Data protection in Switzerland : a preview », dans Karen McCullagh, Olivia Tambou et Sam Bourton, National adaptation of the GDPR, coll. Open Access Book, Blogdroiteuropen, février 2019, pp. 120-121.
[400] CJUE, 16 juillet 2020, « Schrems II », op. cit.

Section 3 : La solution d'un cadre normatif consacré à l'IA au niveau national

Les autorités répressives de ces trois Etats utilisent des dispositifs d'IA en matière pénale. La France et l'Allemagne ont publié en 2018 des lignes directrices sur l'IA[401].

En Allemagne, le rapport sur la stratégie nationale pour l'IA est ancré dans une politique d'innovation et d'amélioration des performances technologiques. Le gouvernement fédéral est conscient des conséquences juridiques des décisions prises sur la base de dispositifs d'IA. Il soutient ne pas négliger les « valeurs démocratiques fondamentales de la République fédérale allemande ainsi qu'à la protection des droits fondamentaux ancrés dans la constitution, notamment [le droit à] l'autodétermination en matière d'informations »[402], soit l'*Informationelle Selbstbestimmungsrecht*[403].

En France, les dispositifs d'IA utilisé en matière de police prédictive notamment est étudiée au sein du rapport Villani, sous l'égide notamment de l'affaire *Loomis c. Wisconsin*, précédemment citée. Les solutions apportées à ces dérives de l'IA sont d'une part, la création d'un « comité consultatif national d'éthique pour les technologies et l'IA »[404]. Ce comité est créé en décembre 2019, dans la continuité des dispositions éthiques énoncées au niveau européen. D'autre part, le rapport Villani recommande l'information des citoyens « sur leurs droits »[405]. En janvier 2020, une proposition de loi constitutionnelle, sous forme de « Charte de l'intelligence artificielle et des algorithmes »[406] est portée devant le parlement. Ce texte prévoit un droit constitutionnel, dans la continuité de la déclaration universelle des droits de l'Homme de 1948, afin que les citoyens préservent leur choix éclairé d'avoir recours à de tels dispositifs.

En Suisse en revanche, l'académie des sciences considère qu'une solution éventuelle pour la confiance en l'IA de la part de services de police pour l'instant partiellement réticents, serait d'établir d'une « institution au niveau gouvernemental responsable de la vérification des exigences des systèmes d'IA »[407]. Bien plus qu'un comité éthique, cela permettra notamment d'instaurer une cadre normatif solide pour l'IA, à défaut d'avoir une base solide en adéquation avec le RGPD.

---

401 Allemagne : « *Nationale Strategie für Kunstliche Intelligenz* », Gouvernement fédéral, Novembre 2018, cité « Rapport allemand relatif à la stratégie nationale pour l'IA »
France : « *Donner un sens à l'intelligence artificielle – pour une stratégie nationale et européenne* », Rapport Cédric Villani, Mission parlementaire de septembre 2017 à mars 2018, cité « rapport Villani ».

402 Rapport allemand relatif à la stratégie nationale pour l'IA, p. 38.

403 Cour fédérale constitutionnelle (BVerfG), 1 BvR 209/83, op. cit.

404 Rapport Villani, p. 155.

405 Ibid., pp. 151-152.

406 Pierre-Alain Raphan, proposition de loi constitutionnelle relative à la Charte de l'intelligence artificielle et des algorithmes, n°2585, 15 janvier 2020.

407 Académie suisse des sciences, « Recommandation for an AI Strategy in Switzerland », 2018, pp. 10-11 : « we recommend defining an institution at the governmental level in Switzerland to assume responsibility for the requirements and verification of AI systems ».

Conclusion de la Partie III

La notion de vie privée a évolué au point de créer la protection des données à caractère personnel. L'IA au niveau européen est une technologie parmi d'autres et les textes s'y référant se veulent généraux et anticipateurs de toute autre technologie à venir. L'IA n'est pas expressément citée au sein des textes européens, en revanche les institutions européennes et les Etats membres sont conscients de sa présence en matière pénale et des conséquences de cette utilisation sur la protection des données.

L'ambition de renforcer l'éthique au sein des dispositifs d'IA est un premier pas et n'est pas négligeable, puisque cette initiative démontre une prise de conscience collective des dérives possibles de l'IA. Par ailleurs, Anne Bouverot rappelait que « l'éthique est profondément humaine et, bien sûr, nous n'avons pas attendu l'arrivée d'Internet ni de l'apprentissage automatique pour y réfléchir »[408]. L'application de l'éthique aux nouveaux enjeux sociétaux est alors inévitable.

Cependant, l'idée selon laquelle le caractère éthique suffirait au respect des droits fondamentaux, notamment de la protection des données est erronée. En effet, les développeurs d'IA s'ils instaurent des règles éthiques au sein de leurs dispositifs, pourraient justifier leur fiabilité et ainsi leur utilisation en masse. L'éthique demeure un outil souple, ne pouvant à elle seule constituer « un cadre et une sécurité juridique [constituant] des facteurs indispensables pour tout développement durable »[409]. Ainsi, une avancée normative partiellement inspirée par cette « vague éthique »[410] mais développant d'autres aspects d'une protection juridique stricte est vivement attendue.

Par analogie à la citation de Brian Solis, au sujet du darwinisme digital, appliquée au monde du marketing selon laquelle « **la technologie et le comportement des consommateurs** évoluent plus vite que la capacité **des entreprises** à s'adapter à ces nouvelles situations »[411], il convient d'en modifier les termes pour l'adapter à notre sujet :

Les dispositifs d'IA et la volonté des autorités pénales de s'en doter*, évoluent plus vite que la capacité* ***des institutions européennes et nationales à réguler*** *et s'adapter à ces nouvelles situations*.

[408] Anne Bouverot, « *Éthique de l'IA : quels enjeux après la création du Comité d'éthique du numérique* ? », Institut Montaigne », 19 décembre 2019.
[409] Yannick Meneceur, « L'éthique, insuffisante à réguler seule les technologies numériques et l'intelligence artificielle », Les temps électriques, 7 mai 2020.
[410] Yannick Meneceur, « IA, Algorithmes, Big Data, Data Science, Robotique : inventaire des cadres éthiques et politiques », Les temps électriques, 6 mai 2020.
[411] Brian Solis, Digital Transformation and the Race Against Digital Darwinism, Disruptive technology, le 9 septembre 2014.

Conclusion générale

Face à une atmosphère sécuritaire prenant de plus en plus de place au sein de notre inconscient collectif, se sont développés plusieurs discours favorables au « solutionnisme technologique »[412], soit, le fait de voir en chaque nouveau développement technologique, la solution parfaite à un problème préexistant. L'idée de devoir « combattre les dangers du 21e siècle avec les armes du 21e siècle »[413] semble alors justifier l'utilisation massive de dispositifs d'intelligence artificielle.

Ces discours sont utilisés à deux fins complémentaires. D'une part, afin d'attiser la crainte d'un danger finalement omniprésent et invisible. D'autre part, pour renforcer la confiance envers l'IA permettant de vivre dans une société sans infraction, une société parfaite. Une société dans laquelle la justice même est perfectionnée par des algorithmes recalibrant les décisions de manière plus juste, sans les préjugés discriminants présents au sein du cerveau des juges dotés d'une sensibilité humaine. Nous passons alors dans un nouveau monde. Antoinette Rouvroy décrit ce passage comme une transition « d'une civilisation du signe et du texte vers une civilisation du signal calculable et de l'algorithme »[414].

« L'effet performatif est l'une des limites majeures de l'outil prédictif actuel »[415], puisque nous ne connaissons pas les « codes d'intelligibilité »[416] de cette nouvelle civilisation ni la façon dont nous sommes perçus par ces algorithmes auto-apprenants. Il s'agit de « garder la main »[417] sur l'intelligence artificielle, afin de transformer ce qui pourrait devenir un cercle vicieux, en cercle vertueux. En effet, à la manière du concept philosophique d'agentivité, il est primordial que nous conservions la capacité d'agir et d'accepter de manière éclairée de faire l'objet d'une décision fondée exclusivement sur le traitement automatisé de nos données personnelles, ou non.

En définitive, une ingérence dans le droit à la protection des données est possible et peut être simplifiée voire encouragée en matière pénale. En revanche, l'utilisation de l'IA, pour des traitements de données de manière auto-apprenante en matière pénale, amplifie cette ingérence. L'urgence du contexte d'un besoin commun de règles strictes encadrant l'IA a été compris et est en cours.

---

[412] Evgeny Morozov, « *To Save Everything, Click Here* », Ed. Publicaffairs, 2013 : ouvrage traitant de l'aberration du solutionnisme technologique.
[413] Christian Estrosi, maire de Nice, dans le reportage « Tous surveillés : 7 milliards de suspects », diffusé sur la chaîne Arte le 21 avril 2020, op. cit.
[414] Antoinette Rouvroy et Anne Debet, op. cit.
[415] Olivier Chaduteau, intervention lors du colloque à la Cour de cassation, « Justice prédictive : perspectives et limites », le 12 février 2018.
[416] Ibid.
[417] CNIL, « *Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle* », 15 décembre 2017.

Il convient désormais de s'assurer de la prise de conscience de cette urgence par l'ensemble des corps professionnels liés à ces dispositifs d'IA, notamment en matière pénale. Il s'agit de leur laisser une marge de manœuvre équilibrée.

A titre d'exemple, la Cour d'appel de Londres a rappelé l'importance de maîtriser l'usage de dispositifs de reconnaissance faciale par des agents de police du Pays de Galles, ayant pour mission de placer des individus au sein d'une liste de personnes devant faire l'objet d'une surveillance[418]. Cette liste nourrit ensuite un dispositif de reconnaissance faciale. En l'espèce, l'appelant, Edward Brigdes a fait l'objet de plusieurs collectes d'images de son visage dans l'espace public, par reconnaissance faciale, alors qu'il n'était pas un individu à risque devant être surveillé et a été placé sur ladite liste sans fondement. Cet abus ravive la question du besoin constant de surveiller l'utilisation humaine des algorithmes, en plus de l'auto-développement de ces derniers.

Plus largement, le débat des limites des emprises humaines sur ces dispositifs est renforcé. Jan Kleijssen rappelait d'ailleurs cette question via l'histoire de l'algorithme ayant battu le champion du monde du jeu de go, évoqué en introduction : « A ce jour, les ingénieurs ayant développé cet algorithme ne peuvent pas réécrire le codage utilisé par la machine. C'est-à-dire qu'ils savent ce que la machine a fait mais ne savent pas comment elle l'a fait »[419].

Si ces dispositifs ne sont pas encadrés de manière stricte par des bases légales solides, ils ne pourront être maîtrisés et utilisés sous l'égide même du respect des droits de l'Homme. Il est pertinent de se questionner sur notre capacité à maintenir un cap vers une régulation stricte de ces dispositifs.

---

[418] Cour d'appel d'Angleterre et du Pays de Galles (EWCA), R (Bridges) c. Chief constable of South Wales, n°C1/20192670, 11 août 2020, §124.

[419] Conseil de l'Europe, Interview avec Jan Kleijssen sur l'Intelligence artificielle, 13 septembre 2018. Passage traduit et souligné par mes soins.

Annexes

Faculté de droit, de sciences politiques et de gestion
Université de Strasbourg

Interview de Madame Sandra Bertin
Directrice de la Police municipale de Nice

Je rédige mon mémoire de fin d'études au sujet de : « l'intelligence artificielle (IA), la justice pénale et la protection des données à caractère personnel ». Le fil rouge de cette étude est en partie de comprendre la place que possède l'IA au sein des métiers essentiels au maintien de l'ordre, à la prévention des infractions et à la résolution d'enquêtes.

S'en suit ensuite une analyse de ces dispositifs (instruments de police prédictive, traitement automatisé des données, recensement automatique des fichiers de police, etc.), sous l'égide de la protection des données à caractère personnel, afin de comprendre quelles évolutions sont nécessaires au sein du cadre normatif européen et national, sans que cela nuise à l'efficacité des métiers ci-dessus mentionnés.

D'avance merci pour le temps que vous accorderez à ce questionnaire.

I. Votre présentation

A quelles responsabilités répond votre profession. Quel est votre rôle au sein de votre « service ».

GRADE : DIRECTEUR DE POLICE MUNICIPALE

FONCTION EXERCEE : RESPONSABLE DE LA CONSTRUCTION DE L'HOTEL DES POLICES ET DES INNOVATIONS

RÔLE : MISE EN ŒUVRE DE L'ENSEMBLE DES MOYENS ET COORDINATION OPERATIONNELLE DES DIFFERENTS SERVICES VISANT A MENER A BIEN LES PROJETS DE SECURITE (INCLUANT LES APPELS A PROJET, NATIONAUX OU EUROPEENS)

II. La place des dispositifs d'IA au sein de votre profession

Votre service est-il concerné par des dispositifs informatiques de manière générale ? (*Ex : traitement des données, recueils informatiques, travail de renseignement sur des sites internet, réseaux sociaux, etc.*)

OUI

Avez-vous observé au fil du temps, un besoin de plus en plus présent d'utiliser ces dispositifs (*par l'augmentation des fichiers/données à traiter notamment*) ? Si oui, à quelle période (approximativement) et quels sont les changements visibles (*Ex : efficacité dans l'exécution des missions, de nouvelles difficultés rencontrées ou atténuées ?)*

A mesure que les technologies se sont développées, les outils déployés par les puissances publiques ont tenté de s'adapter à l'évolution technologique que l'on retrouvait particulièrement au sein des sphères privées.

Dans le domaine de la sécurité, de nouvelles menaces ont émergé, sans pour autant que les anciennes ne disparaissent. La ville de Nice a une politique de sécurité ambitieuse dont l'objectif est de garantir la sécurité de tous sur l'espace public.

La ville de Nice dispose à ce jour du premier complexe de supervision de France.

Les technologies, dans la dynamique des politiques de sécurité visées et dans le cadre d'un dispositif de sécurité global se sont développées afin de contribuer efficacement à la protection des espaces publics.

Aussi, la ville de Nice propose aujourd'hui des dispositifs toujours plus innovants :

- + de 3000 caméras
- Des caméras reliées au CSU en temps réel dans toutes les rames de tramway
- Des outils d'aide à la relecture
- Des boitiers d'alerte dans tous les bâtiments communaux, écoles, crèches, ainsi que tous les commerces qui en font la demande
- Bornes d'appel sur la voie publique dans des secteurs définis
- Caméras piéton
- Expérimentations
- …

La décennie 2000-2010 a joué un rôle crucial dans le développement, la démocratisation et l'acceptation des technologies.

Dans le domaine de la sécurité (comme dans le domaine de la santé, la défense, etc) les technologies occupent une place prépondérante dans le sens où elles permettent de venir en complément des actions des agents. A titre d'exemple, intégrer dans le parc de caméras de vidéoprotection des logiciels capables de détecter un colis ou un bagage abandonné aura pour effet de conduire à une réaction immédiate et à la mise en place du protocole adapté de manière quasi instantanée.

L'intelligence artificielle, doit pouvoir apporter aux agents l'aide dont ils ont besoin pour exécuter convenablement les tâches relevant de leur compétence, à savoir la protection des personnes et des biens.

Utilisez-vous des dispositifs d'automatisation du traitement des données de tout type au sein de votre métier ? Si oui, lesquels et pour quelle raison ?

(Exemples : traitement automatisé des données, recensement automatique des fichiers de police/gendarmerie, algorithme de cartographie interactive, recensement automatisé des plaintes, etc.)

Oui. A titre d'exemple, la gestion automatisée de la main courante, de la géolocalisation des patrouilles ou encore des effectifs.

La gestion automatisée des données a pour effet de faciliter le travail des agents et d'optimiser la qualité du travail fourni.

A quelle fréquence utilisez-vous ce genre de dispositifs ? Expliquez, s'il vous plaît.

Quotidiennement/régulièrement : Ces outils me permettent d'exercer des missions quotidiennes
Occasionnellement : J'utilise ces outils afin d'effectuer des recherches à l'occasion de missions particulières.
Rarement : Je n'utilise ces outils que très rarement.

Mon poste étant basé sur la conception de projet, j'ai évidemment recours à l'outil informatique mais pas spécifiquement au traitement automatisé des données ou encore à l'intelligence artificielle. Je ne m'en sers qu'à l'occasion d'expérimentations, dans un contexte très spécifique.

III. La place des données au sein des dispositifs

Des données à caractère personnel sont-elles recueillies par les dispositifs ci-dessus mentionnés ? (*Ex : données liées à l'identification de l'individu (nom, adresse, etc.), données biométriques (Ex : visage, iris, contour de la main, etc.).* Si non, dans quelle mesure votre profession est-elle amenée à traiter ce type de données.

La règlementation en vigueur actuellement ne permet de traiter les données personnelles seulement si les dispositions entrent dans l'une des bases de licéité du package européen de traitement de la donnée. Aussi, tout ce qui est autorisé à ce jour en France est déjà déployé à la ville de Nice, ce qui ne l'est pas encore fait régulièrement l'objet d'expérimentation, le but étant de démontrer, outre l'efficacité et l'intérêt des outils, qu'il est urgent de faire évoluer nos lois et règlements.

Observez-vous une restriction du traitement des données à caractère personnel du fait d'un cadre légal ? (*Loi informatique et liberté du 6 janvier 1978, modifiée par la loi du 20 juin 2018*). L'avez-vous observé depuis 2018 ? (*Moment d'entrée en vigueur du règlement européen relatif à la protection des données RGPD, directive « police-justice »).*

Cette loi a fait l'objet d'une modification en Juin 2018, sans qu'aucune des marges de manœuvre permises par l'UE ne soit prise en compte. Elle a simplement été modifiée pour coller au cadre européen et aux dispositions obligatoires. En 2020, disposer d'un texte de référence de 1978 auquel nous devons nous référer pour l'usage des données et des nouvelles technologies d'une manière générale n'est plus adapté au contexte actuel. Dans un monde où tout va toujours plus vite, il est temps que nous nous donnions les moyens d'aller plus loin et que nous soyons cohérents avec la société dans laquelle nous évoluons. Le cadre légal est nécessaire pour éviter les dérives et pour protéger les données personnelles, il doit simplement être réactualisé.

IV. Remarques générales au sujet de l'expérimentation de reconnaissance faciale lors du carnaval de Nice en 2019

Comment avez-vous réussi à mettre en œuvre cette expérimentation tout en veillant à l'équilibre protection des données personnelles/ sécurité publique, prévention des infractions ? Vous pouvez également me faire part de remarques plus générales non évoquées ci-dessus.

L'expérimentation de reconnaissance faciale a reposé sur la base de licéité du consentement. L'expérimentation mise en place à Nice à l'occasion de la 135ème édition de son carnaval est la première en Europe, en temps réel et sur la voie publique.

Pour ce faire, une étude d'impact a été élaborée et transmise à la CNIL. Le dispositif accepté par la CNIL a été plus restrictif que celui que nous avions initialement proposé. Nous avons mené une expérimentation sur 3 jours et à l'occasion de 4 sorties carnavalesques, au sein d'une entrée spécifiquement dédiée pour les spectateurs désireux de participer à l'expérimentation.

Pour en démontrer ou non la pertinence opérationnelle, nous avons mis en place des simulations de situation. L'expérimentation de reconnaissance faciale avait plusieurs objectifs :

- AUTHENTIFICATION
- DETECTION
- MESURE D'ACCEPTABILITE

S'agissant du premier point, nous avons créé une base de données dans laquelle figurait un certain nombre de volontaires et nous avons testé le système du fast-access. L'intérêt de l'authentification par la reconnaissance faciale s'est très rapidement manifesté et peut s'articuler autour de différents cas d'usage :

- Accès pour les employés
- Accès dans des zones réservées par des personnels habilités
- Accès rapide pour le public s'étant préalablement enregistré

S'agissant du second, nous avons élaboré de nombreuses simulations qui nous ont permis de conclure que l'appui d'un outil de ce type semblait essentiel pour augmenter encore l'efficacité des filières de la sécurité, au travers de mesures de prévention ou de répression. Aussi, la reconnaissance faciale sur la voie publique peut se révéler très pertinente dans les cas suivants :

- Disparition de mineurs
- Disparition d'adultes vulnérables
- Détection d'une personne recherchée
- Détection d'une personne dangereuse

Enfin, s'agissant de l'acceptabilité, au terme de l'expérimentation un questionnaire a été proposé à 821 personnes (spectateurs du carnaval choisis au hasard) et il en est ressorti que 97% d'entre eux étaient favorable à l'usage et l'utilisation par les autorités de ce type de technologies quand 67% d'entre eux préconisait tout de même un encadrement strict.

V. Publication de l'interview en annexe du mémoire

L'interview figurera en annexe de mon mémoire.

Fait le 29/07/2020 à NICE .

Le Monde

JUSTICE

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le Journal officiel *va publier un arrêté créant une* « division de l'informatique » *au ministère de la justice, celui de l'intérieur met la dernière main à la mise en route d'un ordinateur puissant destiné à rassembler la masse énorme des renseignements grapillés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à définir* chaque *Français par un « identifiant », qui ne définisse que lui, maintenant terminé, est l'objet de convoitises ardentes; le ministère de l'intérieur y souhaite jouer le premier rôle. En effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, une puissance sans égale.*

Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebattu : celui des rapports des libertés publiques et de l'informatique. Son importance exigerait qu'il en fût, au Parlement, publiquement débattu. Tel ne paraît pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministère de la justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

« Safari » ou la chasse aux Français

Rue Jules-Breton, à Paris-13e, dans des locaux du ministre de l'intérieur, un ordinateur Iris-80 avec bi-processeur est en cours de mise en marche. A travers la France, les différents services de police détiennent, selon la confidence faite par un très haut magistrat, 100 millions de fiches, réparties dans 400 fichiers. Ainsi se trouve posées — et, à terme, théoriquement résolues — les données d'un problème comprenant, d'une part, l'énormité des renseignements collectés ; de l'autre, la méthode à définir pour faire de cet ensemble une source unique, à tous égards, de renseignements.

L'histoire du très puissant appareil qu'est l'Iris-80 est exemplaire du secret qui entoure l'épanouissement de l'informatique dans les administrations, quelles que puissent être les informations qui filtrent ici et là.

Puissant, cet Iris-80, une comparaison le démontre sans contestation. L'appareil employé pour engranger les données de l'opération Safari, qui concerne l'identification individuelle de l'ensemble des 52 millions de Français, a une contenance de 2 milliards d'octets (1) ; celle de l'ordinateur du ministère de l'intérieur est de 3,2 milliards d'octets.

C'est dire que la mise en route d'Iris-80 — dont la location coûte 1 million de francs chaque mois — a été précédée d'études, de tests pour en éprouver les possibilités. D'autant qu'à lui seul, il doit remplacer les trois GE 400 et le 10070 de la C.I.I. qu'employait jusqu'alors la Place Beauvau.

C'est sur ce dernier ordinateur qu'ont eu lieu les essais. Pour 20 % de sa capacité, il a été consacré à la gestion du personnel communal de la Ville de Paris. Mais, pour le reste (80 %), il a servi à tester les programmes devant être fournis à l'Iris-80, afin de rendre cohérentes entre elles, les données contenues dans les 400 fichiers que possèdent les services de police : renseignements généraux, direction de la surveillance du territoire, police judiciaire, etc.

A titre d'anecdote, on peut rappeler que ce 10 070 de la C.I.I., à l'origine, budgétairement, n'était pas du tout prévu pour la tâche qu'il a finalement assurée, mais pour « traiter » les données administratives du Fichier national des constructeurs (F.N.C.). Il s'agit donc apparemment d'un détournement manifeste de crédits d'études, ce qui n'était sans doute pas le vœu du Parlement qui les vota.

De vastes ambitions

Il n'y a pas que cela. Le ministère de l'intérieur a d'encore plus vastes ambitions. Détenteurs, déjà, du fichier national du remembrement, les services de M. Jacques Chirac font de grands efforts pour, affirme-t-on, s'en adjoindre d'autres : le cadastre, le fichier de la direction nationale des impôts et, plus grave peut-être, celui du ministère du travail.

De telles visées comportent un danger qui saute aux yeux, et que M. Adolphe Touffait, procureur général de la Cour de cassation, avait parfaitement défini le 9 avril 1973 devant l'Académie des sciences morales et politiques, en disant : *« La dynamique du système qui tend à la centralisation des fichiers risque de porter gravement atteinte aux libertés, et même à l'équilibre des pouvoirs politiques. »*

C'est si vrai que la régie nationale des usines Renault, par exemple, dispose déjà d'une base de données établies à partir d'un fichier du personnel.

On admettra, dans ces conditions, que l'ouverture d'un débat public paraîtra particulièrement urgente pour définir les limites de l'emploi des banques de données. Or ce débat paraît, dans le principe, écarté par le premier ministre, qui, dans une lettre directive adressée voici quelques semaines à M. Jean Taittinger, avait écarté une telle procédure au profit de circulaires, voire de décrets, préservant en tout état de cause le secret de décision de l'administration. On connaît le peu d'efficacité immédiate que peut avoir devant le juge administratif le recours en annulation d'actes du gouvernement...

Ce n'est pas, pourtant, que les avertissements aient manqué. Le Conseil d'Etat en 1970, puis le ministère de la justice en 1972 (qui avait rappelé le rôle dévolu à l'autorité judiciaire de *« gardien des libertés individuelles »* et donc réclamé voix au chapitre) ont insisté sur la nécessité d'une intervention législative qui préciserait les quelques éléments essentiels de l'emploi de l'informatique appliquée aux particuliers : réglementation de l'acces des tiers aux fichiers, de l'intercommunication de ceux-ci, droit de rectification des personnes fichées si les renseignements retenus sont inexacts, etc.

De plus, tous les exemples étrangers incitent à ce débat sur une utilisation de l'informatique à laquelle, par définition, il ne s'agit pas de renoncer, mais à qui doivent être tracées des limites, si grand est le danger qu'elle implique. La désignation par le gouvernement d'une commission de « sachants » dans les semaines à venir ne saurait suffire à remplacer le débat parlementaire dont on se méfie si visiblement.

En fait de débats parlementaires, il y a d'ailleurs des précédents qui sont le fait, précisément, du ministère de la justice et n'ont pas compromis le développement des fichiers. Avec le casier judiciaire, depuis longtemps, la chancellerie a l'expérience de semblables fichiers. Quel que soit le jugement qui peut être porté sur le principe d'un tel outil, il n'apparaît pas — sauf erreurs négligeables, relativement — que l'accès des tiers ou le droit à contrôle des personnes visées — par demande d'un extrait — ait jamais provoqué des bavures préjudiciables à la légalité.

De même, le fichier national des conducteurs, dans sa partie judiciaire, est prévu par une loi, et il faut regretter que les textes d'application ait permis des illégalités injustifiables — mais connues (*le Monde* du 8 mars).

« A la hussarde »

Fort, pourtant, de ces avantages, le ministère de la justice paraît curieusement se laisser dépasser par des querelles internes peu compréhensibles. L'arrêté signé le 18 mars par M. Jean Taittinger le montre. La création d'une « division de l'informatique », place Vendôme, serait en soi une bonne chose, du point de vue de l'efficacité, si les conditions de sa création, engagée vraiment voici trois mois, ne prenait l'allure d'une peu élégante tentative d'élimination dirigée contre certains esprits novateurs ayant eu le mauvais goût de s'intéresser trop tôt à l'informatique.

Il serait, en effet, bien étonnant que les membres de la commission de l'informatique au ministère de la justice, que préside M. Adolphe Touffait, ne s'offusquent pas d'une décision qui, en soi, ne peut avoir pour but que de *« vider de sa substance »* ladite commission. D'autant qu'il est d'ores et déjà connu que M. Touffait a été rayé de la liste des « sachants ». Il semble d'ailleurs que les réactions vives qui sont enregistrées portent moins sur le renouvellement des structures, jugées inévitables, que sur la méthode *« à la hussarde »* employée par tel membre de l'entourage de M. Taittinger pour mener à bien ses projets de rénovation de la gestion dans le domaine judiciaire.

Est-ce à dire de plus que les choix que l'on entend promouvoir soient nécessairement les plus opportuns ? Tout indique, pour l'instant, que, si le ministère de l'intérieur a définitivement choisi le « matériel lourd » pour s'équiper, la chancellerie, au contraire, s'oriente vers un réseau de mini-ordinateurs placés auprès de chaque tribunal de grande instance important.

Dans cet ordre d'idée, le choix déjà décidé de M. Jean Malbec, vice-président à Bobigny (Seine-Saint-Denis), comme futur chef de la division de l'informatique (au point qu'il a, dès à présent, effectué des missions d'information à Lille, Nice, Lyon et Marseille dans les semaines passées), est significatif. Il est, en effet, à Bobigny l'apôtre d'un système *« mini »* qu'il souhaite étendre à l'ensemble de l'institution judiciaire. Ce n'est sans doute pas non plus par hasard si la télévision, lundi, après avoir donné des extraits du discours de M. Taittinger à Gap sur la justice civile et les nécessités d'un *aggiornamento* technique, a illustré son discours par un large reportage sur les équipements du tribunal de Bobigny — plus réduits, donc plus rapides à réaliser, ainsi plus vite source d'orgueil pour leurs créateurs.

C'est donc un doute global qui pèse sur les intentions du gouvernement, en général, et du ministère de la justice, en particulier : ce dernier département, qui rappelle à tous sa mission de protection des libertés individuelles, a apparemment accepté sans broncher la suppression d'un éventuel débat public, ce qui jette sur les déclarations « libérales » de M. Taittinger en d'autres domaines une suspicion qui n'est pas de bon aloi.

Mais, dans cette entreprise, le ministère de la justice, même s'il fait preuve d'une grande mollesse pour la défense de ses idéaux, car il ne s'agit pas seulement à présent de *« protéger des délinquants »*, n'est pas essentiellement en cause. Ce qui l'est, c'est une entreprise dont on a tout lieu de suspecter la pureté tant on prend soin de cacher sa réalisation.

PHILIPPE BOUCHER.

(1) L'octet, ensemble de huit « bits », est l'unité de mémoire de la plupart des ordinateurs. Quand on enregistre un texte dans la mémoire, chaque caractère du texte occupe un octet. Un milliard d'octets représente, en gros, la capacité de mémoire de cinquante bandes magnétiques.

Bibliographie

I. Ouvrages

BASDEVANT ADRIEN, MIGNARD JEAN-PIERRE, *L'Empire des données*, essai sur la société, les algorithmes et la loi, Ed. Don Quichotte, 2018.

CARDON DOMINIQUE, *A quoi rêvent les algorithmes ? Nos vies à l'heure des big data*, La république des idées, Ed. Seuil Paris, 2015.

CAZALS FRANÇOIS, CAZALS CHANTAL, *Intelligence artificielle : L'intelligence amplifiée par la technologie*, Ed. De Boeck Supérieur, à paraître le 31 décembre 2021.

FOUCAULT MICHEL, *Surveiller et punir, naissance de la prison*, Ed. Gallimard, 1975.

GARAPON ANTOINE, LASSEGUE JEAN, « *La justice digitale* », Ed. PUF, 2018.

GIUDICELLI-DELAGE GENEVIEVE, LAZERGES CHRISTINE, *La dangerosité saisie par le droit pénal*, PUF, Ed. IRJS, Paris, 2011.

MAYER-SCHÖNBERGER VIKTOR ET CUKIER KENNETH, *Big data : la révolution des données est en marche*, Ed. Robert Laffont, 2013.

MOROZOV EVGENY, *To Save Everything, Click Here*, Ed. Publicaffairs, 2013.

PASQUALE FRANCK, *The Black Box Society : the secret algorithms that control money and information*, Ed. Harvard University Press, 2015.

SUPIOT ALAIN, *La gouvernance par les nombres*, Cours au collège de France (2012-2014), Ed. Fayard, 2015.

TAMBOU OLIVIA, *Manuel de droit européen de la protection des données à caractère personnel*, Ed. Bruylant, 2020.

TAYEBI MOHAMMAD A., GLÄSSER UWE, *Social network analysis in predictive policing, Concepts, Models and Methods*, Ed. Springer Switzerland, 2016.

TURING ALAN, *Computing Machinery and Intelligence*, Mind, Ed. Oxford University Press, 1950.

VIGEN TYLER, *Spurious correlations – correlation does not equal causation*, Ed. Hachette Books, 2015.

II. Travaux académiques

SIMON ANNE, *Les atteintes à l'intégrité des personnes détenues imputables à l'Etat : contribution à la théorie des obligations conventionnelles européennes : l'exemple de la France*, Thèse universitaire, Université Panthéon Sorbonne, le 4 décembre 2013.

WALTER EMMANUELLE, *Evaluation de la dangerosité et du risque de récidive d'auteurs mineurs d'infraction à caractère sexuel : à partie de 64 expertises psychiatriques pénales*, Thèse universitaire, Université de Lorraine, 2015.

III. Articles

AMMAR OUSSAMA, *La guerre s'intensifie entre Doctrine et les avocats*, Lesechos.fr, 27 juin 2019.

ANDERSON CHRIS, *The End of Theory : The Data Deluge Makes the Scientific Method Obsolete*, Wired Magazine, 2008.

ANGWIN JULIA, LARSON JEFF, *How We Analyzed the COMPAS Recidivism Algorithm*, ProPublica.org, 23 Mai 2016.

BADOT CHRISTOPHE, *Le défi du droit à l'oubli face à l'intelligence artificielle*, Les Echos, 10 novembre 2017.

BEATSON JESSE, *AI-supported adjudicators : should artificial intelligence have a role in tribunal adjudiction*, Canadian Journal of Administrative Law & Practice, Ed. Carswell, vol. 31-3, Toronto, 2018.

BEELEN AXEL, *Directive œuvres orphelines : de l'importance des considérants*, Worldpress.com, 2012.

BLANC NATHALIE, GAUTIER PIERRE-YVES, *Contre « l'anonymisation » des arrêts publiés : décadence des références de jurisprudence*, Dalloz actu., 6 septembre 2019.

BORE LOUIS, intervention de Bruno Lasserre dans *Open data des décisions de justice : une régulation nécessaire des algorithmes*, Conseil-état.fr, 6 juillet 2020.

BOUVEROT ANNE, *Éthique de l'IA : quels enjeux après la création du Comité d'éthique du numérique ?*, Institut Montaigne, 19 décembre 2019.

BRAFMAN JULIE, *Justice prédictive, l'augure des procédures*, Liberation.fr, 23 février 2017.

BREGERAS GUILLAUME, *La start-up Doctrine attaquée par l'Ordre des avocats de Paris*, Lesechos.fr, 27 septembre 2018.

CALUDE CRISTIAN, LONGO GIUSEPPE, *The deluge of Spurious Correlations in Big Data*, dans Foundations of Science, vol. 22, 3, 7 mars 2016.

CARDON DOMINIQUE, COINTET JEAN-PHILIPPE, MAZIERES ANTOINE, *La revanche des neurones : l'invention des machines inductives et la controverse de l'intelligence artificielle*, Réseaux, La Découverte, vol. 5 (211), 2018.

CATHERINE FORGET, *La protection des données dans le secteur de la police et de la justice*, dans Le règlement général sur la protection des données (RGPD/GDPR), Ed. Larcier, 2018.

CEDRIC INGRAND, *Le data-mining : l'intelligence artificielle au service du fisc*, lci.fr, 02 juillet 2020.

CHARLET FRANÇOIS, *Data protection in Switzerland : a preview*, dans Karen McCullagh, Olivia Tambou et Sam Bourton, National adaptation of the GDPR, coll. Open Access Book, Blogdroiteuropen, février 2019.

CHAVANNE YANNICK, *Révision de la LPD : le préposé fédéral à la protection des données s'impatiente*, ictjournal.ch, 30 juin 2020.

CHERON ANTOINE, *Intelligence artificielle et enjeux juridiques*, Village-justice.com, 3 avril 2018.

COUSTET THOMAS, Interview d'Antoine Garapon, *le numérique est un remède à la lenteur de la justice*, Dalloz actualités, 4 mai 2018.

DE BRUYN FLORENCE, KENSEY ANNIE, *50 ans d'études quantitatives sur les récidives enregistrées*, Direction de l'administration pénitentiaire, Collection Travaux et Documents, Décembre 2017.

DE SCHUTTER OLIVIER, *Fonctions de juger et droits fondamentaux. Transformation du contrôle juridictionnel dans les ordres juridiques américains et européens*, Ed. Bruylant, Bruxelles, 1999.

DONDERO BRUNO, *Justice prédictive : la fin de l'aléa judiciaire* ?, Dalloz, n°10, 2017.

DREYER EMMANUEL, *L'Intelligence artificielle et le droit pénal*, dans Alexandra Bensamoun et Grégoire Loiseau, Le droit et l'intelligence artificielle, Ed. LGDJ, 2019.

FERNANDEZ RODRIGUEZ LAURA, *Algorithmes : la France se mobilise pour plus de transparence*, Usbek et Rica, 21 février 2017.

FLEURIOT CAROLINE, *Avec l'accès gratuit à toute la jurisprudence, des magistrats réclament l'anonymat*, Dalloz actu., 06 février 2017.

GARAPON ANTOINE, *Les enjeux de la justice prédictive*, La Semaine Juridique, Edition générale, n°1-2, Ed. Lexis Nexis, 9 janvier 2017.

GLESS SABINE, WOHLERS WOLFGANG, *Subsumtionsautomat 2.0 – Kunstliche Intelligenz statt menschlicher Richter ?*, dans Böse Martin, Schuman Kay H., Toepel Friedrich, Festschrift für Urs Kindhäuser, Ed. Nomos, 2019.

GONZALES PAUL, *L'accès en ligne aux décisions de justice est fragilisé*, Le figaro, 2 octobre 2018.

HENDRYCKS DAN, ZHAO KEVIN, BASART STEVEN, STEINHARDT JACOB, SONG DAWN, *Natural Adversarial Examples*, Univerisity of Cornell, 16 juillet 2019.

HUNYADI MARK, *La dictature des chiffres*, Comm. Alain Supiot, La gouvernance par les nombres, Le Temps.ch, le 12 février 2016.

JUIGNET PATRICK, *Karl Popper et les critères de la scientificité*, Philosciences.com, 6 mai 2015.

LE-BAS CHRISTOPHE., *Sous le capot de la police prédictive*, Courrier picard, 4 février 2018.

LEPINE BASTIEN, *La RATP transforme Châtelet en laboratoire de test pour la reconnaissance faciale*, LeBigdata.fr, 27 février 2020.

MENCEUR YANNICK, *Intelligence artificielle et droits fondamentaux*, dans Patrick Gielen et Marc Schmitz, Avoirs dématérialisés et exécution forcée, Ed. Bruylant, novembre 2019.

MENECEUR YANNICK, *IA, Algorithmes, Big Data, Data Science, Robotique : inventaire des cadres éthiques et politiques*, Les temps électriques, 6 mai 2020.

MENECEUR YANNICK, *L'éthique, insuffisante à réguler seule les technologies numériques et l'intelligence artificielle*, Les temps électriques, 7 mai 2020.

MENECEUR YANNICK, *Quel avenir pour la justice prédictive*, la Semaine Juridique, Edition générale, n°7, Ed. Lexis Nexis, 12 février 2018.

MOREAUX ANNE, *La procédure pénale et les nouvelles technologies*, Affiches-parisiennes.com, 21 décembre 2018.

MULLER PHILIPPE, *Intelligence artificielle et reconnaissance de formes*, Institut de recherche en informatique de Toulouse, 27 mars 2014.

PALMIOTTO FRANCESCA, *The Black Box on trial : The impact of Algorithmic Transparency on Fair Trial Rights in Criminal Proceedings*, dans Martin Ebers and Marta Cantero-Gamito, Algorithmic Governance and Governance of Algorithms, Ed. Springer, à paraître en octobre 2020.

PERONNE GERALDINE, DAOUD EMMANUEL, *Droit à l'oubli contre publicité légale des données : la publicité prime !*, Obs. sous Cour de justice de l'Union européenne, 9 mars 2017, aff. C-398/15, Camera di Commercio c/ Salvatore Manni, Dalloz IP/IT, juin 2017

PIAZZA PIERRE, *Alphonse Bertillon et l'identification des personnes (1880-1914)*, criminocorpus, 26 août 2016.

PIETT TODD, *How Law Enforcement Uses Social Media for Forensic Investigation*, Mashable.com, 13 février 2012.

RIGHENZI DE VILLERS JOSEPH, *L'IA sauvera-t-elle la démocratie ?*, Assas Legal Innovation, 8 avril 2020.

ROUVROY ANTOINETTE, BERNS THOMAS, *Gouvernementalité algorithmique et perspectives d'émancipation – Le disparate comme condition d'individuation par la relation ?*, dans Réseaux, n° 177, 2013.

ROUVROY ANTOINETTE, *Big data : l'enjeu est moins la donnée personnelle que la disparition de la personne*, propos recueillis par Serge Abiteboul et Christine Froidevaux, Le Monde, le 22 janvier 2016.

SOLIS BRIAN, *Digital Transformation and the Race Against Digital Darwinism*, 9 septembre 2014.

SZWARC MONIKA, *Le caractère juridique de la coopération judiciaire en matière pénale et de la coopération policière (IIIe pilier) à la lumière du Traité constitutionnel pour l'Europe*, Revue Electronique Nice, le 15 mars 2006.

THIERRY GABRIEL, *La Gendarmerie, de l'analyse prédictive à l'analyse décisionnelle*, L'Essor de la Gendarmerie nationale, 26 janvier 2018.

VIGNEAU VINCENT, *Le passé ne manque pas d'avenir - Libres propos d'un juge sur la justice prédictive*, Recueil Dalloz, 2018.

WEYEMBERGH ANNE, L'harmonisation des procédures pénales au sein de l'Union européenne, Archives de politique criminelle, Ed. A. Pédone, n°26, 2004.

ZOUBEIDI-DEFERT YANIS, *Fichier ELOI : Suite et fin*, Obs. sous Conseil d'État, 30 décembre 2009, *Association SOS Racisme – Groupe d'information et de soutien aux immigrés et autres*, Req. n^{os} 312051-313760, blogdroitadministratif.net, 19 mars 2010.

IV. Conférences et webinaires

- Session parlementaire européenne, Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 20 février 2020.

Disponible à l'adresse suivante : https://www.europarl.europa.eu/committees/en/hearing-on-artificial-intelligence-in-cr/product-details/20200211CHE07061, visionnée le 20 mars 2020.

- Souvira Anne, Séminaire « Intelligence artificielle et justice », Université Paris 5 Descartes, 2 avril 2019.
- Yannick Meneceur, *Quelle régulation pour l'intelligence artificielle ?,* Conférence enregistrée, Librairie Kléber Strasbourg, 4 juin 2020.
- Olivier Chaduteau, colloque à la Cour de cassation, *Justice prédictive : perspectives et limites*, 12 décembre 2018.
- Monsieur Bertrand Louvel, colloque par l'ordre des avocats au Conseil d'État et à la Cour de cassation, *La justice prédictive*, 12 février 2018.

Les petits déjeuners de l'Intelligence Artificielle (UMR DRES et Conseil de l'Europe)

- *Predictive policing and Rule of technology*, 2 juillet 2020.

Disponible à l'adresse suivante : https://www.coe.int/fr/web/human-rights-rule-of-law/-/sixth-edition-of-the-ai-breakfasts-predictive-policing-and-rule-of-technology, visionnée le 2 juillet 2020.

- *Covid-19 : Myths and realities of tracking applications*, 13 Avril 2020, visionnée le 27 avril 2020.

Disponible à l'adresse suivante : https://www.coe.int/en/web/artificial-intelligence/-/ai-breakfasts-5th-edition-covid-19-myths-and-realities-of-tracking-applications-.

- Adrien Basdevant, *Les données, la nouvelle ingénierie du pouvoir : quelles conséquences pour l'Etat de droit ?*, 2 décembre 2019.

V. Autres sources

A. Reportages

- *Tous surveillés : 7 miliards de suspects*, réalisé par Sylvain Louvet, Arte, 21 Avril 2020.

Disponible à l'adresse suivante : https://www.youtube.com/watch?v=8wN3emyA-ew, visionné le 25 Avril 2020.

- *Technologie : Anacrim, un puissant logiciel au service de la gendarmerie*, France 3 Provence-Alpes-Côte-d'Azur, 4 février 2018.

Disponible à l'adresse suivante : https://france3-regions.francetvinfo.fr/provence-alpes-cote-d-azur/alpes-maritimes/technologie-anacrim-puissant-logiciel-au-service-gendarmerie-1415201.html, visionné le 15 juin 2020.

B. Emissions de radio

- *22 v'là la police prédictive !*, Beauchamp Antoine, France Culture, 5 décembre 2018.

Disponible à l'adresse suivant : https://www.franceculture.fr/emissions/la-methode-scientifique/la-methode-scientifique-du-mercredi-05-decembre-2018, consulté le 5 juin 2020.

- Antoinette Rouvroy et Anne Debet, *Protection des données personnelles : souriez, vous être traqués*, émission la méthode scientifiques par Nicolas Martin sur France culture du 23 mai 2018.

Disponible à l'adresse suivante : https://www.franceculture.fr/emissions/la-methode-scientifique/la-methode-scientifique-du-mercredi-23-mai-2018, consulté le 15 juillet 2020.

Liste des matériaux

I. Documentation des organisations concernées par le sujet

A. France

CNIL

- Avis n°2020-056 sur le projet de décret relatif à l'application mobile dénommée « Stopcovid », 25 mai 2020.
- Identifier les données personnelles, 27 janvier 2020.
- Reconnaissance faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019.
- La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo, 19 septembre 2018.
- Le cadre européen, 2018.
- Comment permettre à l'homme de garder la main, rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, 15 décembre 2017.
- Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur, 13 juin 2013.
- Rapport d'activités 2006, La documentation française, Paris, 2007.
- Délibération n°2005-208 portant avis sur le projet de loi relatif à la lutte contre le terrorisme, 10 octobre 2005.

Rapports et missions parlementaires

- RAPHAN PIERRE-ALAIN, proposition de loi constitutionnelle relative à la Charte de l'intelligence artificielle et des algorithmes, n°2585, 15 janvier 2020.
- DE LA RAUDIERE LAURE, MIS JEAN-MICHEL, Rapport d'information par la mission d'information commune sur les chaînes de blocks (blockchains), n°1501, 12 décembre 2018.
- PARIS DIDIER, MOREL-A-L'HUISSIER PIERRE, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, sur les fichiers mis à la disposition des forces de sécurité, n°1335, 17 octobre 2018.
- VILLANI CEDRIC, « Donner un sens à l'Intelligence Artificielle - Pour une stratégie nationale et européenne », Septembre 2017 - Mars 2018.
- CADIET LOÏC, « L'open data des décisions de justice », Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, Novembre 2017.
- JEAN-YVES LE BOUILLONNEC ET DIDIER QUENTIN, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, sur la mesure statistique des délinquances et de leurs conséquences, n°988, 24 avril 2013.
- BATHO DELPHINE, BENISTI ALAIN, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police, n°4113, 21 décembre 2011.

Instituts français

- Institut Montaigne, *Algorithmes : contrôle de biais S.V.P*, Mars 2020.
- Institut d'aménagement et d'urbanisme d'Île de France, *La police prédictive - Enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique*, Camille Gosselin, Avril 2019.
- Institut Montaigne, *Justice : faîtes entrer le numérique* », Novembre 2017.

Autres

- Descriptif de l'application « Stopcovid », Site internet du ministère français de l'économie, des finances, de l'action et des comptes publics, 2 juin 2020.
- Ministère de la Justice, Les chiffres clés de la Justice 2019.
- Programme de sécurité de la campagne présidentielle d'Emmanuel Macron, 2017.
- Comité interministériel aux Archives de France, Pourquoi les archives sont-elles un atout de modernisation pour votre administration ?, Octobre 2013.

B. Conseil de l'Europe

- Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *Guidelines on Artificial Intelligence and data protection*, Conseil de l'Europe, T-PD(2019)01, 25 janvier 2019.
- Manuel de droit européen en matière de protection des données, Conseil de l'Europe, 2018.
- Comité des ministres du Conseil de l'Europe, Rapport explicatif de la Convention 108+,
- Rouvroy Antoinette, Rapport au bureau du comité consultatif de la convention 108, Conseil de l'Europe, *Des données et des Hommes, Droits et libertés fondamentaux dans un monde de données massives*, 11 janvier 2016.
- Algorithme et Droits humains, étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données et éventuelles implications réglementaires, Etude DGI(2017)12, Conseil de l'Europe, Mars 2018.
- Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel *Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police*, T-PD(2018)01, , 15 février 2018.
- Conseil de l'Europe, Interview avec Jan Kleijssen sur l'Intelligence artificielle, 13 septembre 2018

C. Union Européenne

- Commission européenne, *Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance* », 19 février 2020.
- Commission européenne, Groupe d'experts de haut niveau, *Ethics guidelines for trustworthy AI*, avril 2019.
- Comité Européen de la Protection des Données, institution un groupe consultatif externe sur les dimensions éthiques de la protection des données, 3 décembre 2015.

- Commission européenne, Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière de la Commission, 2 février 2011.
- Journal Officiel de l'UE, avis du CEPD n°C139/1 du 23 juin 2007.
- Commission européenne, décision d'adéquation du 26 juillet 2000, n° 2000/518/CE, relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse.

D. Autres matériaux pertinents

- The Law Society, Algorithms in the Criminal Justice System, Juin 2019.
- Europol programming document 2019-2021, 29 janvier 2019.
- Europol, *Do criminals dream of electric sheep ? - How technology shapes the future of crime and law enforcement,* 2019.
- Gouvernement fédéral allemand, « *Nationale Strategie für Kunstliche Intelligenz* », Novembre 2018.
- Académie suisse des sciences, « Recommandation for an AI Strategy in Switzerland », 2018.

II. Bases légales

A. Bases légales du Conseil de l'Europe

- Commission Européenne pour l'Efficacité de la Justice, Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires, 2018.
- Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel, dite « Convention 108+ », 2018.
- Comité des ministres du Conseil de l'Europe, Recommandation (87)15, visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police compte tenu des nouveaux développements en la matière, le 15 septembre 1987.
- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, dite « Convention 108 », 28 janvier 1981.
- Convention Européenne des Droits de l'Homme, 1950.

B. Bases légales de l'UE

- Directive (UE) 2016/680, dite « Directive police-justice », du parlement européen et du conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.
- Règlement général pour la protection des données (UE) 2016/679, dit « RGPD », du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
- Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.
- Décision-cadre 2009/315/JAI du Conseil concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres. Décision 2000/642/JAI du Conseil relative aux modalités de coopération entre les cellules de renseignement financier des États membres en ce qui concerne l'échange d'informations.
- Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.
- Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière
- Règlement « SIS II », Règlement (CE) nº 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), JO L 381.

- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- Traité de l'Union Européenne, 1992.

C. Bases légales nationales

France

- Décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives,
- Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
- Décret n° 2017-1224 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD), du 3 août 2017.
- Décret n° 2016-1480 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
- Arrêté modifiant l'arrêté du 23 décembre 2009 portant organisation de la direction générale de la gendarmerie nationale (NOR: IOCJ1020161A), 27 août 2010.
- Décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'Intérieur.
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (versions initiale et mise à jour)
- Code de procédure pénale.
- Code de l'organisation judiciaire.

Allemagne

- Loi allemande BGBl. I S. 201, du 27 janvier 1977 pour la protection contre toout abus des données personnelles par le traitement des données, dite « *Bundesdatenschutzgesetz* » ou « BDSG » (versions initiale et mise à jour).
- Constitution fédérale allemande « *Grundgesetz* », 1949.

Suisse

- Loi fédérale du 28 septembre 2018 mettant en œuvre la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (Développement de l'acquis de Schengen).

- Loi fédérale RS 235.1 relative à la protection des données, 1992.
- Code pénal

Liste des jurisprudences

I. Décisions de la Cour européenne des droits de l'Homme

II. Décisions de la Cour de justice de l'Union Européenne

- Data Protection Commissioner c. Facebook Ireland Ltd, M. Schrems, aff. C-311/18, 16 juillet 2020.
- Camera di Commercio c. Salvatore Manni aff. C-398/15, 9 mars 2017.
- Data Protection Commissionner of Ireland c. M. Schrems, aff. C-362/14, 6 octobre 2015.
- Google Spain c. Agencia Española de Protección de Datos, aff. C-131/12, 13 mai 2014.

III. Autres décisions pertinentes

- Cour d'appel d'Angleterre et du Pays de Galles (EWCA), *R (Bridges) c. Chief constable of South Wales,* n°C1/20192670, 11 août 2020.
- Tribunal Fédéral suisse, *A c. Ministère public de l'arrondissement de l'Est vaudois*, n°1B_164/2019, 15 novembre 2019.
- Conseil constitutionnel français, décision n° 2019-778 DC, sur la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice du 21 mars 2019.
- CE, 10ème - 9ème chambres réunies, Inédit au recueil Lebon, 18 octobre 2018, n°404996.
- Cour Suprême des Etats-Unis, *Loomis c. Etat du Wisconsin*, n° 16-6387, 26 juin 2017.
- Cour fédérale constitutionnelle (BVerfG), 1 BvR 370/07, 27 février 2008.
- Cour fédérale constitutionnelle (BVerfG), 1 BvR 209/83, 15 décembre 1983.