La police prédictive

Margot Chambon

Aix-Marseille Université
Faculté de Droit et Sciences politiques

Master 2 Recherche sciences criminelles
Parcours sciences criminologiques

Mémoire

La police prédictive

Présenté par
Madame Margot Chambon

Directeur de recherche : Monsieur Nicolas Catelan,
Professeur, Maître de conférence

Juin 2018

La faculté n'entend donner aucune appropriation ou improbation aux opinions contenues dans ce mémoire de recherche qui doivent être considérées comme propres à son auteur.

Remerciements

Je remercie le Professeur Nicolas Catelan, pour ses précieux conseils et de m'avoir permis de travailler sur ce sujet.
Je tiens aussi à remercier mes proches pour leur patience et leur aide inconditionnelles.

Sommaire

Liste d'abréviations

ADN : acide désoxyribonucléique

Aff. : affaire

API : Advance Passenger Information

Ass. : assemblée

Cass. crim. : Chambre criminelle de la Cour de cassation

CE : Conseil européen

CEDH : Cour européenne des droits de l'Homme

CESDH : Convention européenne de sauvegarde des droits de l'Homme

CIA : Central Intelligence Agency

CJCE : Cour de justice des Communautés européennes

CJUE : Cour de justice de l'Union européenne

CNIL : Commission nationale de l'informatique et des libertés

Cons. constit. : Conseil constitutionnel

DDHC : Déclaration des droits de l'Homme et du citoyen

DGSI : Direction générale de la Sécurité intérieure

ECPN : European crime prevention network

EDVIGE : Exploitation documentaire et valorisation de l'information générale

Eurojust : Unité de coopération judiciaire de l'Union européenne

Europol : European police office

FAED : Fichier automatisé des empreintes digitales

FBI : Federal Bureau of Investigation

Fichier S : fichier atteinte à la sûreté de l'État

FIJAIS : Fichier judicaire automatisé des auteurs d'infractions sexuelles

FIJAISV : Fichier automatisé des auteurs d'infractions sexuelles ou violentes

FIJAIT : fichier judicaire national automatisé des auteurs d'infractions terroristes

FNAEG : Fichier national automatisé des empreintes génétiques

FPR : fichier des personnes recherchées

FSPRT : fichier des signalements pour la prévention de la radicalisation à caractère terroriste

GPS : Global Positioning System

IA : intelligence artificielle

Ibid. : ibidem

Interpol : Organisation internationale de police criminelle

JAI : Justice et Affaires intérieures

JLD : Juge des libertés et de la détention

JO : Journal officiel

JUDEX : système judiciaire de documentation et d'exploitation

LSI-R : Level of Service Inventory-Revised

LSJ : liberté, sécurité, justice (espace)

NSA : National Security Agency

OCDE : Organisation de coopération et de développement économiques

ONU : Organisation des Nations Unies

OPJ : officier de police judiciaire

Op. cit. : opus citatum

PCL-R : Psychopathy Checklist-Revised

PDG : président directeur général

PET : Privacy Enhancing Technologies

PNR : Passenger Name Record

QPC : Question prioritaire de constitutionnalité

RGPD : Règlement général sur la protection des données

SIS : Système d'information Schengen

STIC : système de traitement des infractions constatées

SWIFT : Society for Worldwide Interbank Financial Telecommunication

TAJ : fichier de traitement des antécédents judiciaires

TFTP : Terrorist Finance Tracking Program

TFUE : Traité sur le fonctionnement de l'Union européenne

TGI : Tribunal de grande instance

UE : Union européenne

U.S. : United-States

« *The past and the present are within my field of inquiry, but what a man may do in the future is a hard question to answer* »

« *Le passé et le présent sont mes terrains d'enquête, mais ce qu'un homme peut faire dans le futur est une question à laquelle il est difficile de répondre* »

Sherlock Holmes, *The Hound of the Baskervilles*, Arthur Conan Doyle, 1905

Introduction

1. Intelligence artificielle - « *Réussir à créer une intelligence artificielle serait le plus grand événement de l'histoire de l'humanité. Malheureusement, il pourrait être l'ultime* ». S'il fallait retenir une mise en garde du scientifique Stephen Hawking, ce serait peut-être celle-ci. Stephen Hawking faisait partie de cette communauté de scientifiques qui s'alarme de l'engouement autour de ce projet, plus si chimérique aujourd'hui, de créer une intelligence artificielle (IA).

Le terme est devenu, en 2018, presque commun et ce même chez les « profanes » de l'informatique. Car inconsciemment, chacun accueille de plus en plus l'intelligence artificielle dans son quotidien. En lui faisant une place dans tous les appareils connectés, dans tous les systèmes informatiques, dans le cadre de la profession, au quotidien dans nos actes de consommation, de communication, l'utilisation des services publics, le monde intègre pleinement l'idée d'une intelligence artificielle. Un concept tellement utilisé, qu'on en oublie sa réelle signification. Il faut comprendre les termes séparément pour réaliser ce qu'ils impliquent une fois réunis.

2. Définitions - La notion d'intelligence ne fait pas l'unanimité. Du latin *intelligentia*, dérivé du mot *intellegere*, le terme est composé du préfixe -*inter*, « entre », et du verbe *legere* : « cueillir, choisir, lire » et renvoie à la notion de faire un choix, une sélection. Étymologiquement, l'*intelligentia*, déclinaison d'*intelligo*, est la faculté, de comprendre, de percevoir, de discerner ; donc de savoir faire un choix réfléchi. Le dictionnaire Larousse semble lui-même être tiraillé entre différentes définitions : « *aptitude d'un être humain à s'adapter à une situation, à choisir des moyens d'action en fonction des circonstances* » ; « *ensemble des fonctions mentales ayant pour objet la connaissance conceptuelle et rationnelle* » ; « *personne considérée dans ses aptitudes intellectuelles, en tant qu'être pensant* » ; « *qualité de quelqu'un qui manifeste dans un domaine donné un souci de comprendre, de réfléchir, de connaître et qui adapte facilement son comportement à ces finalités* » ; « *capacité de saisir une chose par la pensée* ».

Réduire toutes ces caractéristiques à une seule capacité, qualité, est difficile. Un point commun ressort néanmoins parmi toutes ces définitions : il est fait référence à l'être humain, à la personne, à quelqu'un. L'intelligence est donc attribuée avant tout, si ce n'est uniquement, à l'Homme. Bien que les animaux aient pu nous prouver plus d'une fois leur

capacité à réfléchir et d'adaptation, il est fait ici référence à la réflexion et à des émotions bel et bien humaines. L'intelligence est donc cette faculté rationnelle et naturelle de l'être humain de pouvoir faire un choix réfléchi à travers l'observation et la conception du monde qui l'entoure. Ce qui est artificiel à l'inverse est « *produit par le travail de l'Homme et non par la nature* », « *qui n'est pas conforme à la réalité* »[1].

Du latin *artificialis*, qui signifie fait avec art, l'artificiel renvoie directement à son étymologie, l'artifice : qui sert à déguiser, à tromper. L'artifice sert à masquer. Ce qui est artificiel est donc faussement naturel ; c'est une ruse créée par l'Homme afin de palier à une création que la nature n'a pu lui offrir.

Pris ensemble, les termes « d'intelligence artificielle » prennent tout leur sens. C'est donc une volonté de l'Homme de recréer une intelligence humaine, le corps et les caractéristiques biologiques en moins. Or, cette résolution impliquerait nécessairement un cerveau. De quoi dispose-t-on aujourd'hui pour atteindre un tel objectif ? De la machine, de la science informatique, en fait de l'ordinateur. Les prémices de ce dernier sont apparues dès le début du XXème siècle.

3. Origines de l'intelligence artificielle - C'est au Royaume-Uni, dans les années 1920, que sont nées les premières références à l'intelligence artificielle. Alan Turing, alors étudiant en mathématiques, « *parvint à établir une limite entre ce qui est calculable et ce qui ne l'est pas* »[2].

Ce qui est calculable est prédictible, ce qui ne l'est pas résiste donc à ce déterminisme, et est imprévisible. Ses premiers travaux tendent à montrer qu'une machine pourrait effectuer chaque étape d'un long calcul, seule. Ces recherches ne sont alors qu'au stade théorique, des suppositions.

Recruté par le gouvernement britannique pour décrypter les messages radios nazis pendant la Seconde Guerre mondiale, Alan Turing a pu confirmer ses premières approches de la machine. Mais c'est après la guerre, dans les années 1940, qu'il va concrétiser son projet en matérialisant enfin ce qu'il appellera l'*Automatic Computing Engine (ACE)*, le premier ordinateur capable non pas uniquement d'effectuer des calculs, mais de traiter tous types de données. Bien que l'ACE soit un exploit, le mathématicien ne s'arrête pas là, son ambition étant bien plus grande. En 1950, il publie son ouvrage

[1] Dictionnaire Larousse électronique
[2] Jean Lassègue dans CNRS Le Journal, « L'héritage d'Alan Turing », Hors-série mai 2012

Computing Machinery and Intelligence, dans lequel il décrit cette pensée conceptuelle d'attribuer une intelligence à la machine. Sa théorie *The Imitation Game*[3] fait référence à une capacité qu'aurait la machine à se faire passer pour l'être humain. L'allégorie de l'intelligence artificielle est née.

4. Big Data - Aujourd'hui, le projet se concrétise : l'intelligence artificielle doit pouvoir désormais se rapprocher le plus possible du fonctionnement du cerveau humain. Ainsi comme tout cerveau, elle a besoin, pour fonctionner, de s'alimenter : les matières premières de l'intelligence artificielle sont les données. Comme tout cerveau, si elle est sous-nourrie, sa capacité est réduite. Or, les progrès fulgurants de l'intelligence artificielle au XXIème siècle, au-delà des progrès technologiques, ne sont pas un hasard. Elle est le corollaire d'un nouveau phénomène relatif à la multiplication des données : le Big Data.

Ce flux permanent et monumental des données est intimement lié à l'essor de l'IA. Le Big Data, littéralement, « grosses » « données », est aussi désigné sous les termes de méga données, ou de données massives. On comprend que cet ensemble extrêmement conséquent de données, est impossible à exploiter ou organiser. Du moins pour l'être humain et les outils existant jusqu'alors. Cet ensemble massif de données d'origine virtuelle, allant de l'adresse mail, aux photos, vidéos, jusqu'aux publications textuelles a grossi de façon exponentielle grâce aux capacités de stockage toujours plus puissantes des serveurs. Un rapport de recherche du META Group de 2001 a posé trois règles, qui sont désormais acceptées comme propres à définir le Big Data : volume, vélocité et variété[4]. Ces « 3V » renvoient donc au volume conséquent de données, à la vitesse à laquelle elles sont mises à jour, ajoutées ou modifiées, et à la variété de sources alimentant cet ensemble.

Comment donc agréger et analyser une telle masse de données ? L'utilisation de l'intelligence artificielle, qui dispose d'une puissance informatique et d'une capacité technologique particulièrement développées, s'est imposée tout naturellement. Parce que le Big Data présente un potentiel d'amélioration et d'efficience pour beaucoup de secteurs, l'Homme a dû trouver un moyen de traiter artificiellement ces données, incapable qu'il est de le faire lui-même. La traitement automatisé et l'analyse de données, appelé *datamining*, est ainsi apparu. Ce processus permet d'extraire des informations

[3] A.M. TURING, « Computing Machinery and Intelligence », *Mind*, 1950
[4] META Group, « Controlling Data Volume, Velocity and Variety », 2001

discriminantes de ces groupes de données et faire émerger, constater, de nouveaux savoirs pour l'opérateur (… et de nouvelles données).

Le secteur commercial se sert par exemple sur internet des « *cookies* », traceurs de données et de préférences de l'utilisateur afin d'adapter la communication aux profils des clients. La première caractéristique de l'intelligence artificielle est donc cette capacité à l'exploration et l'exploitation de données, dans un univers numérique extrêmement vaste.

5. Apprentissage autonome - Mais l'un des plus grands progrès à ce jour en matière d'intelligence artificielle, toujours dans cette optique de la rapprocher des capacités humaines, est l'apprentissage autonome, aussi appelé *machine learning*. Cette technique repose sur l'idée selon laquelle la machine (l'algorithme en fait), à partir de millions de données de base, va apprendre elle-même par l'exemple. Cette « instruction » procède en deux temps : une phase d'entraînement (apprentissage sur certaines données), puis une phase de vérification (contrôler le « savoir » sur d'autres données). Au point qu'elle aurait, seule, appris à effectuer une tâche et à s'améliorer dans celle-ci.

Les premiers exploits se sont illustrés en matière de jeu d'échecs, puis de jeu de go. En octobre 2017, l'intelligence artificielle *AlphaGo* a battu à plusieurs reprises le champion du monde en la matière. La machine, qui avait été équipée peu de jours avant, de seulement quelques données de base relatives au jeu, a composé ses propres parties, jouant contre elle-même et apprenant seule des coups que même l'Homme jusqu'ici n'avait pu jouer. L'apprentissage autonome fait donc des progrès considérables. Et si le Big Data est le carburant du *machine learning*, on peut dire que ce dernier profite totalement des possibilités offertes par le Big Data.

A tel point que le concept d'intelligence artificielle est quelques fois réduit à celui de *machine learning*. Pourtant si cette dernière surpasse l'Homme dans certains domaines, par l'extraction de modèles et la réalisation de prédiction, elle n'est qu'un sous-domaine de l'IA. Et l'intelligence artificielle fait ses preuves dans bien d'autres domaines que le jeu. Les GAFA tels que Google ou Apple disposent de leurs propres algorithmes commerciaux, intégrés aux appareils, comme la technologie SIRI de direction vocale. La technologie atteint aussi la sphère publique et notamment le domaine judiciaire et juridique. L'intelligence artificielle commence à faire sa place dans les tribunaux et les postes de police et de gendarmerie.

6. Déterminisme – Dans le domaine de l'IA il existe par ailleurs deux grandes familles : l'approche statistiques (dont fait partie la technologie de *machine learning*) et l'approche déterministe qui procède de l'utilisation d'algorithmes capables de modifier leurs réponses ou les données traitées en fonction de l'évolution de leur environnement. Alan Turing se heurtait ainsi, dans l'avancée de ses théories, à une réalité : l'opposition entre le déterminisme et le biologisme. Une différence doit être faite entre ce qui est prédictible, car calculable et connu, et ce qui est imprévisible car non-mesurable mathématiquement. Or, un exemple de cette imprévisibilité est, en principe, le comportement humain.

Des courants de pensées anthropologiques et criminologiques qui s'opposent, ont en effet traversé les âges : la théorie du déterminisme, ou de l'Homme criminel, et celle du libre-arbitre. Les travaux sur le déterminisme ont notamment débuté avec la théorie de Cesare Lombroso : l'Homme criminel dispose de caractéristiques génétiques, physiques, physiologiques et psychiques de prédisposition à ce comportement délinquant. Ces théories ont mené à des politiques pénales qui ont été les plus dangereuses dans l'histoire de l'humanité, gouvernées par des lois univoques : eugénisme, théories des races, lois religieuses … A l'inverse, les théories du libre-arbitre sous-tendent l'idée selon laquelle l'Homme, en possession de ses moyens, agit en toute conscience et doit donc être tenu responsable de ses actes. Bien heureusement, le déterminisme n'est aujourd'hui plus d'actualité, le libre-arbitre et les théories socio-économiques ayant pris le dessus. Ces deux courants de pensées incitent à s'interroger sur l'utilisation des données du Big Data et plus largement sur son exploitation par l'intelligence artificielle.

7. Prédictibilité – Les progrès en la matière ont fait ressurgir une interrogation souvent soulevée par les criminologues, sociologues et scientifiques en général : le crime est-il calculable ? Peut-on calculer le comportement humain, afin de prédire le crime ? Si l'on suit le raisonnement d'Alan Turing, et qu'on considère que la délinquance est un phénomène calculable, qu'il est donc issu de données récoltables, alors le crime serait prévisible, voire prédictible. Or, le crime est le produit du comportement humain qui, selon les théories actuelles, n'est pas déterminé, mais issu du libre-arbitre.

Le comportement peut bien évidemment être influencé par des facteurs entourant l'individu. Il n'en reste pas moins que ces facteurs ne sont pas déterminants pour le comportement, qui répond encore moins à des prédispositions génétiques ou internes à l'Homme. Ainsi la police, grâce aux recherches sociologiques et juridiques, dispose de

certains facteurs socio-économiques, environnementaux des populations, qui permettent parfois d'anticiper certains phénomènes délinquants. Jusqu'ici l'un des rôles principaux de la police est donc la prévention. Prévention qui se transformerait petit à petit en prédiction.

8. Prédiction et justice pénale - La prédiction dans la justice pénale n'est pas si récente : les techniques d'évaluation des risques par une approche statistique, notamment utilisées dans les assurances, ont été transposées au pénal, et initiées à Chicago, dès les années 1920, par Ernest Burgess. Elles étaient alors testées dans le cadre de la prédiction de la récidive, notamment chez les personnes en libération conditionnelle, aux États-Unis.

Les méthodes actuarielles ont traversé les théories criminologiques et sont d'ailleurs toujours d'actualité. Bien que ne dépassant pas les méthodes cliniques et psychiatriques de prévention de la criminalité, l'actuariat est toujours expérimenté et aurait même pour vocation de remplacer l'expertise au procès. L'idée de la prédiction de la criminalité existe donc depuis longtemps dans le système judiciaire et pénal. Mais depuis leurs débuts et jusqu'à maintenant, les recherches sur la prédiction n'étaient menées qu'à l'échelle des moyens purement humains. L'intelligence artificielle va permettre bien plus, poursuivant l'objectif d'atteindre la prédiction du crime au-delà de la simple probabilité fournie par l'actuariat.

L'utilisation d'algorithmes à des fins de prédiction de la criminalité a été envisagée avant tout dans le cadre de la police. Cette profession assurant entre autres la sécurité de la communauté, la prédiction ne pourrait pas mieux servir que dans ce secteur. L'intégration de l'intelligence artificielle au service du travail policier implique donc de conjuguer les domaines de la sécurité, du juridique et du technologique. La police elle-même, par expérience, sait établir certaines statistiques et probabilités sur la délinquance à l'échelle d'une agglomération ou d'un quartier par exemple. Empiriquement, les officiers savent adapter leurs moyens d'action. Cependant parfois, le travail policier peut être biaisé par les propres croyances de ses acteurs et dévier vers des comportements et arrestations discriminatoires. Les affrontements entre la police et certaines communautés de la population américaine sont peut-être aussi l'illustration malheureuse de ces jugements hostiles, erronés. La technologie a cet avantage d'être neutre dans ses calculs ; à l'inverse du cerveau, elle n'émet pas d'émotions ni d'idées, mais seulement des résultats. C'est en ce sens que la possibilité d'une police prédictive commence à être envisagée, imaginée par les acteurs de la sécurité publique.

Les mutations technologiques influencent les relations et interactions humaines, sociales, voire les facilitent. La communication virtuelle, les nouveaux espaces publics que sont les réseaux sociaux, sont des sources, parmi tant d'autres, de données transmises par les utilisateurs. Les flux et sources de données sont certes des opportunités pour le secteur commercial, mais le sont tout autant pour les autorités publiques. Ces données peuvent s'avérer d'une utilité précieuse dans la lutte contre la criminalité. C'est ce deuxième constat qui a servi à la théorisation de la police prédictive. Le monde change, les individus s'adaptent, échangent de plus en plus, le travail policier suit cette évolution et en tire parti.

9. Police prédictive – La prédiction en matière de sécurité s'impose donc elle-même, lorsque l'intelligence artificielle et le Big Data entrent dans l'équation. Après avoir théorisé la police prédictive algorithmique, il était nécessaire de la concrétiser. Là aussi, les villes des États-Unis ont fait office d'agglomérations tests. C'est au fur et à mesure de l'expérimentation de cette police que plusieurs méthodes sont apparues, tant des méthodes purement algorithmiques que des méthodes criminologiques.

Le premier logiciel prédictif conçu et testé fut *Compstat*, créé par le Chef de la police de Californie William Bratton, au début des années 2010. Appelé à la direction de la police de Los Angeles, c'est cette ville qui sera le premier terrain d''expérimentation de *Compstat*. L'algorithme ne reçoit que des données de terrain et ne s'attache qu'aux infractions simples à la propriété, les plus fréquentes, tels que le cambriolage, le vol de voiture ou le vol à l'arraché. La machine est programmée ici pour faire ressortir les lieux les plus criminogènes ; à la police d'ensuite adapter son action. Ce type de prédiction « 1.0 »[5] des lieux criminogènes devient un succès auprès de la police. Dès lors, pourquoi ne pas l'étendre à d'autres infractions ?

En effet, un fléau sévit dans l'État américain : les infractions par arme à feu et les crimes violents. Certains lieux ont des tendances plus criminogènes, du fait de facteurs spécifiques au voisinage, et les « guerre de gangs » sont très courantes. A Los Angeles, après le succès de *Compstat*, l'idée surgit de tenter de prédire d'autres types d'infractions ; sans pour autant considérer le traitement d'autres données que celles relatives à l'infraction, au lieu et au temps. Les recherches des chefs de police américains, en partenariat avec des scientifiques, les mènent en Suisse, où des chercheurs exploitent

[5] A.G. FERGUSON, « Predicting Predictive Policing », *Washington University L. Rev*., vol. 94, n°5, 2017, p.1130

la sismologie pour élaborer des modèles prédictifs de zones sismiques. Ils s'inspirent de cette programmation qui tend là encore à faire ressortir des « zones à risque », des « *hot spots* », mais de manière bien plus précise et en utilisant parfois des données de voisinage. Ces données ne sont cependant jamais relatives aux individus humains. C'est ainsi qu'est né l'algorithme prédictif *PredPol*, maintenant entreprise, qui s'est développé à plus d'une soixantaine de villes sur le territoire américain. *PredPol* reste à ce jour l'exemple le plus populaire de cette police prédictive « 2.0 », qui traite tant des infractions aux biens que de certaines infractions violentes. Traitement qui repose surtout, il faut le noter, sur ce type de criminalité violente et les affrontements qui sévissent aux États-Unis.

L'expérimentation de la police prédictive qu'illustrent principalement ces deux exemples progresse vers un niveau supérieur, et les futurs utilisateurs d'un modèle 3.0 restent encore prudents face au développement de ce troisième niveau prédictif. Cette police aurait pour but ultime de prédire le comportement criminel lui-même, à l'image du *Minority Report* de Philip K. Dick. Cependant, là où la sismologie est un phénomène calculable, le comportement humain reste imprévisible. Les méthodes de police prédictive du comportement commencent à émerger, toujours en utilisant des facteurs de l'environnement social, économique, culturel … mais pour prédire qui va agir et non plus seulement quelle infraction, quand et où.

Les méthodes de prédiction se multiplient, néanmoins l'une des philosophies de la police prédictive reste d'améliorer le travail policier, d'aider dans la réorganisation de celui-ci sur le terrain, plus que de prédire le crime en soit.

10. Données personnelles - La police prédictive est donc l'un de ces phénomènes qui profite de l'ensemble massif de données. Si elle fait usage de ce flux exponentiel d'informations pour enrichir son travail, une surveillance accrue des données, et donc des personnes, est nécessaire. L'objectif de sécurité et le respect des droits et libertés fondamentaux doivent se conjuguer. La fonction policière ne peut pas avoir accès et traiter n'importe quelle information relative à la personne et doit être cantonnée à la surveillance. En effet grâce aux habitudes et comportements des internautes par exemple, des données de plus en plus précises sont disponibles. La notion de données personnelles est plus que jamais centrale dans la protection du citoyen.

Les données personnelles, requalifiées en « données à caractère personnel » par les institutions européennes, sont une nouvelle composante du droit au respect de la vie

privée. Les États et leurs législateurs ont dû réagir face aux opportunités de collecte des données du Big Data.

Les premiers scandales ont émergé au XXème siècle : des milliers de citoyens ont ressenti une intrusion dans leur vie privée, que ce soit par des acteurs privés ou publics. Et ces méfaits se sont avérés de plus en plus fréquents. En France, c'est notamment l'affaire dite SAFARI qui a soulevé l'indignation des citoyens : le gouvernement avait pour projet, en 1974, de créer un réseau de fichiers interconnectés, automatisés et informatisés, contenant l'ensemble des numéros INSEE des individus sur le territoire. L'annonce a fait un tel tollé que le projet fut abandonné. Finalement, ce scandale servit à éveiller les consciences sur les nouveaux enjeux de l'automatisation ; ainsi est née la commission « informatique et liberté », ayant pour mission d'appréhender ces enjeux, les risques pour les droits des citoyens et va permettre d'accueillir ces nouvelles technologies sans dérives juridiques.

En 1978, le rapport Tricot est rendu, énumérant des recommandations quant à la position à adopter afin que ni le secteur privé, ni le secteur public, ne puissent aller trop loin dans le traitement automatisé des données relatives à la personne. Le rapport Tricot souleva notamment les problématiques publiques de cette automatisation : la multiplication des fichiers de recensement (administratifs ou policiers), la création de profils pouvant émerger de ces fichiers, ou encore le pouvoir considérable que confère la détention de telles informations par des personnes qui sont déjà à la tête de l'État.

Des moyens insuffisamment encadrés permettraient aux entités publiques de détenir des informations sur les citoyens et de s'en servir à des fins pas toujours louables et nous ne serions plus trop loin du monde de Georges Orwell … Les évènements les plus graves pour la nation peuvent entraîner le législateur à franchir certaines limites. Au lendemain des attentats du 11 septembre 2001, le gouvernement de Georges Bush a pris un certain nombre de mesures de lutte antiterroriste, accordant des pouvoirs de surveillance considérables à ses institutions, notamment à la NSA, la CIA ou le FBI.

Des lanceurs d'alerte tels qu'Edward Snowden ou WikiLeaks ont montré que malgré l'objectif de lutte contre le terrorisme existant derrière ces mesures, l'État américain s'était gardé d'informer ses citoyens sur l'exploitation de leurs données et la surveillance généralisée qu'elle entrainait. L'utilisation des algorithmes dans le travail policier, qui tend à améliorer la sécurité des citoyens, doit donc composer avec le respect des droits individuels et ne pas basculer vers le « *Big brother* ». Une étiquette pas toujours facile à respecter pour les pouvoirs publics quand on sait que certaines start-up proposent

des algorithmes surpassant le travail de centaines d'analystes en sécurité intérieure. On en veut pour exemple la société *Palantir*, précurseur dans l'industrie de l'algorithme prédictif, qui, même impliqué dans le scandale Facebook/Cambridge Analytica, est devenu indispensable à la NSA et à notre DGSI française dans le travail de renseignement.

Les autorités ont donc cette lourde tâche d'assurer un équilibre entre la lutte contre l'insécurité, sentiment accru dans notre société, et le respect des droits fondamentaux. C'est cette proportionnalité qui a toujours été la clef de la relation entre les autorités judiciaires et la communauté. Ce rapport d'équilibre pourrait cependant se voir remis en cause par la police prédictive, qui inspire déjà un engouement particulier outre-Atlantique alors même que son utilisation n'est pas réellement encadrée. Ce déséquilibre est d'autant plus probable que la recrudescence de la menace terroriste ne fait qu'exacerber ce sentiment d'insécurité et donne lieu à des politiques sécuritaires. Le caractère transfrontalier de ce type de criminalité rend d'autant plus nécessaire la coopération internationale et donc la circulation et l'échange de données outre-frontières, mais aussi entre le secteur privé, public, et les institutions.

11. Problématique - Tant de facteurs qui mènent à se demander si les avancées technologiques, le développement de l'intelligence artificielle, l'ouverture d'un monde virtuel, justifient nécessairement l'introduction d'une police prédictive dans les outils policiers et plus généralement pénaux. Mais cette ambition de recréer le cerveau humain artificiellement serait-elle justement un outil pour la police ? Servirait-elle ou desservirait-elle, à termes, la lutte contre la criminalité ? Un équilibre évident est à adopter face aux enjeux du Big Data et de l'intelligence artificielle ; car leur utilisation est presque inévitable.

12. Transition vers la prédiction - Sans données, pas de Big Data. Sans Big Data, pas d'intelligence artificielle. Sans intelligence artificielle, pas de police prédictive. Les données disponibles dans notre monde moderne permettent une toute nouvelle approche du travail policier. L'utopie est de prédire grâce à la machine, l'ambition est d'améliorer de plus en plus l'intelligence artificiel et donc les modes d'action des forces de police. La police prédictive avancera nécessairement avec les progrès de l'algorithme et fera muter l'approche policière de la criminalité : petit à petit, cette dernière évolue de la prévention vers la prédiction (I).

13. Prédire pour mieux réagir ? - L'idée, au-delà de prédire le crime, est de restructurer le travail policier et de le réformer grâce à des algorithmes dédiés à cette tâche. L'ambition est grande, face à la hausse de certains types de criminalité comme le terrorisme, la criminalité transfrontière en générale et la cybercriminalité. L'équilibre est délicat à respecter, face à cet outil qu'est la prédiction algorithmique, qui apparaît comme une révolution dans l'approche du phénomène criminel. La science traverse les frontières, et la police prédictive ne saurait tarder à inspirer plus d'un gouvernement ; l'ampleur de la police prédictive pourrait dépasser le simple cadre policier, le simple cadre local, voire le simple cadre national. Mais il est important de garder en tête que ce que la prédiction sert, c'est avant tout la méthode de réaction (II).

Partie I
De la prévention à la prédiction

En 2017, la CNIL a enregistré pas moins de 8 000 plaintes relatives à une atteinte au droit à la protection des données à caractère personnel. Ce droit est désormais fondamental dans notre société que l'on peut qualifier de « connectée ». Les plateformes de données se multiplient : réseaux sociaux, sites marchands, procédures et formulaires en lignes, communications. La multiplicité de ces sources a formé le Big Data et représente une utilité pour tout corps de métier, particulièrement le milieu commercial. Mais elle a aussi su servir aux pouvoirs publics, et pas toujours de manière honnête. Le dernier scandale en date reste celui de l'entreprise *Cambridge Analytica* : cette société aurait récolté plus de 8 millions de données d'utilisateurs de Facebook, et ce à des fins électorales. La collecte de données a ensuite permis à l'entreprise d'établir des profils types, puis de s'en servir pour influencer l'opinion de millions d'américains, et à termes leur vote, en faveur de Donald Trump. Facebook n'est pas non plus sortie indemne de cette affaire ; moins de deux semaines après ces révélations, le président du réseau social, Mark Zuckerberg, se retrouvait face au Congrès américain. Comment *Cambridge Analytica* a pu avoir accès à autant de données d'utilisateurs ? Comment a-t-elle pu les utiliser à de telles fins sans l'autorisation des individus ?

La question a d'ailleurs été posée au PDG de Facebook, à maintes reprises, de savoir si les États-Unis devraient transposer un texte similaire à celui qui va entrer en vigueur dès le 25 mai 2018 en Europe. En effet, à cette date, un nouveau texte de l'Union européenne va s'appliquer, renforçant le respect du droit à la protection des données à caractère personnel. Le fait même que les sénateurs américains se posent simplement la question de la nécessité d'un tel texte dans leur État peut paraître étonnant, mais illustre la différence fondamentale du fonctionnement juridique américain avec celui de l'Europe.

Ce nouveau pan du droit à la vie privée est donc menacé, les législateurs, gouvernements et pouvoirs judiciaires se doivent d'y remédier. D'autant plus que comme tout phénomène humain, la criminalité a su s'adapter et profiter de cette révolution numérique : la communication se simplifie, les mouvements des personnes et objets aussi.

Les autorités répressives doivent désormais faire face à ces menaces et combiner la lutte et la prévention de la criminalité avec les enjeux du développement constant de ces nouvelles technologies et du Big Data, et ce tout en assurant une protection à la hauteur des droits et libertés des personnes.

C'est ainsi qu'est notamment apparue la police prédictive, à des fins d'aide de la police dans leur travail. Une différence existe néanmoins, qui n'est pas des moindres. Cette police prédictive est surtout expérimentée aux États-Unis ; néanmoins la législation sur la protection des données personnelles existe principalement en Europe. En effet la protection des données à caractère personnel est apparue assez tôt en Europe et dans ses États, d'abord dans le milieu marchand mais aussi très vite vis-à-vis des services et autorités publics, et notamment des autorités judiciaires et répressives (Chapitre I). Ces dernières, principalement aux États-Unis donc, ont aussi profité de l'ouverture de cette circulation de données et des progrès informatiques et technologiques. L'introduction des théories de la police prédictive a très vite ouvert la porte à une multiplicité de techniques algorithmiques de prédiction du crime (Chapitre II).

Chapitre I
L'évolution de la collecte des données utiles à la lutte contre la criminalité

Les services de police, dans leur mission d'enquête et de prévention de la criminalité, ont toujours eu besoin de collecter et traiter des données, notamment des données relatives aux personnes. L'idée du fichage des personnes par les autorités judiciaires existait déjà au XIXème siècle en France et a soulevé les premières inquiétudes de la part des individus vers la fin du XX^{ème} siècle, en particulier suite à l'affaire SAFARI. Le développement de la surveillance, corollaire de l'apparition d'une politique pénale se concentrant sur la dangerosité, implique un besoin de plus de données pour lutter contre la criminalité (Section 1). Néanmoins la multiplication de ces sources de données peut avoir un effet inverse et complexifier le travail policier, qui doit faire face aux enjeux qu'impliquent le Big Data dans un tel secteur (Section II).

Section 1 : Les types de données disponibles pour les services de police

Afin de garantir une pleine protection du droit au respect de la vie privée, la collecte, le traitement et la conservation des données à caractère personnel se doivent d'être précisément encadrés certes au niveau du secteur privé, mais aussi dans le secteur public et pénal (§1). On recense en effet de plus en plus de fichiers de police catégorisant soit les personnes soit les types de données ; on pourrait presque parler d'un Big Data propre à la police et au cadre pénal (II).

§1 : L'encadrement du traitement de données dans le contexte pénal

Les États membres de l'Union européenne vont dès le 25 mai 2018 accueillir des nouveaux textes relatifs au renforcement du droit à la protection des données personnelles. La Communauté puis l'Union européenne ont en effet été très attentives à la protection de ce droit, réactives face aux enjeux des nouvelles technologies (A). Cependant la France n'a pas attendu les textes européens pour protéger les données de ses propres citoyens (B).

A. L'encadrement européen

Tant la Convention et la Cour européenne des droits de l'Homme que les institutions de l'Union et la Cour de Justice ont eu vocation à encadrer et préciser les tenants du droit à la protection des données personnelles, tout autant concernant le traitement fait dans un secteur privé que public et pénal. Les institutions européennes ont donc débuté l'encadrement du traitement des données par l'entrée en vigueur de textes (I), précisés et renforcés par une jurisprudence qui s'actualise constamment (II).

I. Les textes européens

14. CESDH - A sa création en 1950, la Convention européenne de sauvegarde des droits de l'Homme (CESDH) n'entendait pas protéger le citoyen européen comme on l'entend aujourd'hui. La notion de protection des données personnelles n'a pas été prévue à l'origine dans la Convention. En 1950, les différents États avaient certes des préoccupations de renseignements, néanmoins peu étaient ceux qui auraient pu prédire la production, la circulation et l'utilisation des données existantes aujourd'hui. La notion même de « données » propres à l'individu était alors sûrement absente des esprits ; aucune technologie, flux immatériel ou machine n'aurait fait émerger de telles problématiques. Historiquement pourtant, c'est au niveau européen que furent adoptés les premiers textes approchant cette notion de protection de l'individu et de ses données : la CESDH en posa les bases en 1953. Dès l'article 8, il est prévu de garantir le droit au respect de la vie privée et familiale, du domicile et de la correspondance. L'article énonce les conditions dans lesquelles des restrictions à ce droit pourraient être admises[6]. Bien que ne disposant pas expressément pour la protection des données, ce sont les juges de la Cour européenne des Droits de l'Homme (CEDH) qui interprèteront l'article 8 en ce sens[7].

15. Convention 108 - Avec la commercialisation des premiers ordinateurs dans les années 1960, accompagnés de processeurs capables d'analyser électroniquement et automatiquement certaines tâches et données, les premiers problèmes n'ont néanmoins pas tardé à apparaître. Ces systèmes automatisés, très vite adoptés par le secteur tant privé

[6] Convention Européenne de Sauvegarde des Droits de l'Homme, 1953, Article 8
[7] Cf *infra*, n°23-24

que public, facilitent la gestion par exemple, mais font émerger des questions quant à l'exploitation et à la conservation de renseignements confidentiels. A ce titre et face à une nouvelle menace potentielle à la vie privée des individus – au caractère privé de leurs données personnelles – la CESDH a très vite tenu à encadrer les nouvelles pratiques technologiques. C'est sous l'impulsion du Conseil de l'Europe qu'a été créé le premier texte universellement reconnu pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, en 1981. Le texte, dit « Convention 108 », est le premier instrument international juridiquement contraignant concernant un tel domaine. Évidemment ouvert à la ratification de tous les États parties à la CESDH, il l'a aussi été à tout États non-partie désirant ratifier un tel texte et l'intégrer dans son arsenal juridique national. Ainsi la France a ratifié la Convention très rapidement[8], réformant certaines de ses dispositions existantes. Le texte s'est vu ratifié par une cinquantaine d'États, certes européens mais aussi non-européens, tel que l'Uruguay en 2013.

La Convention 108 a vocation à « *garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant* »[9]. Il est même pris en compte, dans un chapitre, les possibles transmissions et circulations de données entre États et hors du territoire de l'État dont la personne physique dépend à l'origine.

Sont apparues avec cette Convention les premiers principes pionniers de la protection des données à caractère personnel telles que la loyauté du traitement de ces données, le principe de finalité et la conservation. Avec l'évolution exponentielle des technologies et de l'informatique, l'équilibre entre efficacité et respect des libertés individuelles a été mis à mal, d'où la nécessité d'un premier texte international à caractère contraignant. La Convention 108 a été un tremplin pour les autres institutions et les États européens, et notamment de l'Union Européenne, en matière d'encadrement du traitement des données à caractère personnel.

16. Recommandations ministérielles - Bien qu'en adéquation avec son temps, la Convention 108 a cependant dû faire face à la rapidité de l'évolution technologique dans le domaine qu'elle couvrait. C'est notamment le Comité conventionnel de la

[8] Décret n°85-1203 du 15 novembre 1985 portant publication de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
[9] Convention pour la protection des données à caractère personnel (STE n°108), 28 janvier 1981, dite Convention 108, article 1

Convention 108 qui s'est penché sur la question à plusieurs reprises[10]. Le Comité des ministres a suivi à cette Convention en y ajoutant notamment en 1987 une recommandation, adressée aux États membres, visant à règlementer l'utilisation des données à caractère personnel dans le secteur de la police[11]. En effet, au-delà même de la problématique de l'échange et du traitement des données entre personnes privées, la Convention a su soulever celle du traitement des données par le secteur public et notamment à des fins policières et judiciaires. C'est ce point-là que le Comité a tenu à traiter tout particulièrement, n'étant pas spécifié dans la Convention de 1981. C'est d'ailleurs ce but qui est clairement visé dans le premier article de la Recommandation, qui dispose que bien que les principes de protection des données à caractère personnel aient été mis en œuvre par la Convention 108, et que ceux-ci aient vocation à s'appliquer tant dans le secteur privé que public, il était nécessaire de les adapter précisément dans le cadre de secteurs particuliers. A ces fins, le Comité des Ministres a considéré indispensable de créer des lignes directrices – mais cependant non-contraignantes – spécifiques au traitement des données personnelles dans le secteur de la police.

17. Directive 95/46/CE - Face à la multiplication des sources et de l'intérêt porté par les différentes institutions, le Parlement européen et le Conseil se sont attelés à réfléchir à un renforcement des règles communautaires en matière de données personnelles. Bien que la Convention 108 ait posé les bases des législations à adopter au niveau interne, l'Union s'est très vite rendue compte de la nécessité d'un encadrement renforcé, revoyant ainsi ses exigences à la hausse. L'harmonisation des législations des États membres et la facilitation du libre échange de données entre eux nécessitaient un cadre spécifique et propre.

C'est donc le 24 octobre 1995 que le Parlement européen et le Conseil ont introduit une directive 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[12]. Cette directive avait ainsi pour but premier la prise en compte de « *la marchandisation des données, l'internationalisation des flux et le phénomène de « traçabilité »* »[13]. De ce fait, le texte européen avait surtout vocation à encadrer le traitement des données à

[10] C.CASTETS-RENARD, *Quelle protection des données personnelles en Europe ?*, Ed. Larcier, 2015, p.82
[11] Comité des Ministres, recommandation Rec(87)15, 17 septembre 1987
[12] Directive européenne n°95/46/CE du 24 octobre 1995 du Parlement et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
[13] G.DESGENS-PASANAU, *La protection des données personnelles*, LexisNexis, 2016, p.5

caractère personnel et leurs flux dans un cadre privé, commercial et marchand ; ne portant donc qu'une attention anecdotique au secteur public et notamment au secteur policier et judiciaire.

La directive de 1995 fut néanmoins le premier texte communautaire important à tenter d'harmoniser les législations en matière de protection des données des individus des États membres. Dès lors, la question du caractère fondamental du droit à la protection de ces données s'est posée lors de la rédaction de la Charte des droits fondamentaux de l'Union européenne en 2000. Celle-ci a explicitement consacré le droit à la protection des données et l'existence d'une autorité de contrôle indépendante dans chaque État[14]. La garantie d'un tel droit suit celle du droit au respect de la vie privée. On comprend ici la logique suivie par les rédacteurs du texte : faire entrer dans le sillage du droit au respect de la vie privée celui des données à caractère personnel, qui peut être rattaché dans une certaine mesure à cette notion de vie privée. Il est dès lors nécessaire de les protéger de tout traitement abusif ou attentatoire aux garanties fondamentales.

18. Décision cadre 2008/977/JAI - Bien que le droit à la protection des données personnelles s'encrait et se renforçait en Europe, sa protection dans le cadre de secteurs à vocation non-commerciale présentait des lacunes. Lacunes remarquées et qui ont mené à la rédaction d'une décision-cadre en 2008 spécifique à la protection des données personnelles dans le secteur policier et pénal[15]. Plus précisément, à l'aune des nouvelles exigences de l'Union et de la refonte de son organisation, c'est la coopération pénale et policière qui était au cœur d'une telle décision. En effet celle-ci s'inscrivait dans le cadre de la mise en place de l'espace de liberté, de sécurité et de justice (LSJ), faisant disparaître la notion de pilier et donc sortir la coopération policière et judiciaire du troisième pilier existant jusqu'alors sous la Communauté européenne. Le Conseil précise de ce fait que « *le programme de La Haye visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne, adopté par le Conseil européen le 4 novembre 2004, a souligné la nécessité d'une approche innovante de l'échange transfrontière d'informations en matière répressive, dans le strict respect de certaines conditions fondamentales dans le domaine de la protection des données (...)* »[16]. A l'image des recommandations faites par le Comité des Ministres en 1987, le texte de 2008 tend à concilier respect des droits et

[14] Charte des droits fondamentaux de l'Union européenne 2000/C-362/01 du 7 décembre 2000, article 8
[15] 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
[16] *Ibid,* paragraphe (4) de la décision

libertés fondamentaux des individus avec les exigences liées au maintien de la sécurité publique.

Ainsi tout comme la directive de 1995, la décision-cadre reprend les définitions tenant à ce domaine de protection des données, mais aussi les principes l'accompagnant : licéité, proportionnalité, finalité, droit de rectification et d'effacement. En outre, au-delà des règles à respecter en droit interne, le texte pose surtout les bases de la protection des données personnelles lors d'éventuelles coopérations policières et judiciaires entre États membres.

19. TFUE - Enfin, et afin de concrétiser le souci d'adaptation aux avancées technologiques et à ses biais, il a été inséré des articles spécifiques relatifs à cette protection des données personnelles dans le Traité du Fonctionnement de l'Union européenne (TFUE). L'article 16 du traité confère de ce fait à l'Union la compétence générale de légiférer sur les questions de protection des données et établit à cet égard le principe selon lequel *« toute personnes a droit à la protection des données à caractère personnel la concernant* »[17].

Tant sous le régime de la Communauté européenne que sous celui de l'actuelle Union européenne, les institutions ont su réagir face aux exploits technologiques et informatiques qui, bien que révolutionnant l'efficacité des services et l'échange, menaçaient de plus en plus certains pans de la vie privée des individus ; ce qui a très vite été appelé « données à caractère personnel ». Néanmoins au terme de la première décennie du XXIème siècle, l'avancée scientifique, technologique, la capacité d'échange grâce à Internet n'ont fait qu'augmenter. La rapidité avec laquelle ces évolutions sont apparues a donc interpellé très rapidement le législateur européen, demandant d'ailleurs un travail sur la durée afin de réagir en adéquation avec la célérité de ces domaines et notamment à leur introduction dans de nouvelles sphères, tel que le secteur public.

20. Réformes de 2012 - C'est dès 2012 que le Parlement s'est penché sur la problématique de la modernisation de la directive de 1995, – et donc de la décision-cadre de 2008 – texte qui avait été, lui, rédigé aux débuts d'Internet … Toujours dans un souci de protection des libertés individuelles et du respect de la libre circulation et du libre-

[17] Traité sur le fonctionnement de l'Union européenne, Lisbonne, 2007, article 16

échange entre États, les institutions de l'Union ont travaillé, pendant quatre années, à la refonte des règles de protection des données à caractère personnel. En 2012 la Commission européenne a annoncé plusieurs mesures législatives qui auraient pour vocation de réformer en profondeur la directive de 1995. La Commission ne s'intéresse pas uniquement à la directive principale s'appliquant dans l'Union, mais aussi à la décision-cadre de 2008 portant sur la coopération policière et pénale. Ainsi le projet législatif tend à porter sur la protection des données dans le domaine privé et sur la protection spécifique des données dans le domaine public, mais de manière encore plus précise à porter sur un texte tenant uniquement au domaine judiciaire et policier.

En effet, la multiplication des scandales telles que les révélations faites par WikiLeaks ou Edward Snowden fait réagir sur les comportements adoptés non pas uniquement par des grands groupes privés, mais bien par les États eux-mêmes, leurs gouvernements, services de police et de renseignements. Dès lors, l'Union européenne a tenu à s'assurer d'un cadre légal adapté à son temps, mais aussi applicable à toute forme de traitement des données personnelles. L'ère du Big Data émergeant à cette époque, il est question de s'y retrouver juridiquement dans ces quantités massives d'informations et de données.

21. RGPD - C'est en 2016 que les travaux de la Commission vont se clore, définitivement abroger la directive de 1995, et remplacer le texte de 2008. Le nouveau Règlement général sur la protection des données[18] (RGPD) a pour objectif de mieux encadrer la libre circulation des données personnelles, notamment sur le marché numérique européen, et de renforcer la protection de ces données et les droits individuels l'accompagnant. La date d'application sur le territoire de chaque État-membre fut fixée au 25 mai 2018, leur donnant ainsi le temps de réadapter leurs droits aux nouvelles exigences et dispositions européennes.

22. Directive 2017/680 - Dans le même temps et sous les mêmes conditions de forme, le Parlement et le Conseil ont publié une directive indépendante du règlement, spécifique à la matière pénale[19]. Ainsi, toujours dans la logique du Traité de Lisbonne, la

[18] Règlement (UE) 2016/679 du Parlement et du Conseil du 28 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

[19] 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 des données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

directive « *vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice* »[20]. En ce qui concerne la forme, la directive s'apparente de manière quasi-identique au règlement. Elle comporte donc des définitions des termes utilisés, les droits spécifiques à la personnes concernée, des dispositions quant au responsable du traitement et du sous-traitant etc. Ces dispositions ont en fait vocation à s'appliquer tant aux situations déjà existantes dans les États lors de procédure policières ou pénales, mais reste générale de sorte qu'elle puisse protéger tout individu soumis à une procédure extraordinaire, par exemple dans le cadre de l'enquête. A titre d'illustration, en France, la loi encadre déjà l'étendue des droits de police et de gendarmerie quant à la constitution et l'utilisation de certains fichiers, comme le Fichier de traitement des antécédents judiciaires (TAJ). Ainsi, bien que déjà soumis à des normes de droit interne, le droit français se voit dans l'obligation, avec la directive de 2016, d'adapter ce droit dans le cas où il irait à l'encontre des nouvelles dispositions européennes.

Tant la Convention européenne de sauvegarde des droits de l'Homme que les institutions de l'Union tentent de s'adapter aux nouveaux enjeux du monde numérique. Il apparaît indispensable d'encadrer notamment les pratiques tenant à la collecte, au traitement et à la communication des données des individus. Le droit à la protection de ces dernières est d'ailleurs directement rattaché au droit – bien plus ancien – au respect de la vie privée. Bien qu'inscrit dans les textes, ce droit à la protection des données a été beaucoup mis en jeu, reflétant les enjeux du traitement des données en particulier en ce qui concerne le domaine pénal et policier. C'est d'ailleurs souvent dans le cadre d'enquêtes à des fins de lutte contre la criminalité ou de recherche de la vérité que les États se sont vus confrontés à des poursuites au niveau européen. La jurisprudence des différentes institutions est venue clarifier certaines zones d'ombres, tantôt spécifiques à la conception du droit à la protection des données de chaque État, tantôt à caractère plus général.

II. La jurisprudence européenne

Il est évident que la protection des données à caractère personnel se voit remise en cause dans le cadre d'échanges privés, et de pratiques commerciales. Les premiers textes européens ont d'ailleurs été rédigés à ces fins de protection et de sanction d'éventuelles pratiques frauduleuses ou attentatoires à ce droit récent, ou au droit au respect à la vie

[20] *Ibid,* paragraphe (2)

privée et familiale. C'est en effet à ce droit spécifique que la Cour européenne des droits de l'Homme rattache le droit à la protection des données personnelles – chose qu'elle a faite dans sa jurisprudence, l'article 8 ou toute autre disposition de la CESDH ne le mentionnant pas expressément.

23. Jurisprudence de la CEDH - La jurisprudence de la CEDH est plutôt fournie en ce qui concerne la protection des données à caractère personnel dans le cadre pénal. Celle-ci est vaste, en ce qu'elle va de la géolocalisation, à la conservation des données dans des fichiers pénaux, en passant par les écoutes téléphoniques. Elle traite donc d'un côté de la surveillance et d'un autre de la collecte et de la conservation des données des personnes impliquées dans l'enquêtes ou le processus pénal. C'est le deuxième cas qui sera principalement considéré ici, notamment en ce qui concerne l'interception et la conservation de données obtenues par voie électronique – touchant donc aux enjeux actuels du Big Data. Cependant, cette collecte des données peut très vite s'apparenter à la surveillance elle-même.

24. Droit au respect de la vie privée - La CEDH a donc très vite rattaché le droit à la protection des données à caractère personnel à l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme. Elle assimile ce droit à celui du respect de la vie privée et familiale. C'est notamment ce qu'elle a pu rappeler dans une décision de 2008 : « *la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation des données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (...). La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières* »[21]. La Grande Chambre a dès lors étendu et précisé la portée de ce principe au domaine policier, affirmant l'importance de la proportionnalité entre intérêt public et garanties individuelles. Elle ajoute à ce titre des exigences quant au traitement des données dans un tel cadre : pertinence des données collectées, collecte non-excessive par rapport aux finalités poursuivies – on retrouve ici l'idée de proportionnalité entre l'atteinte au droit à la vie privée et le but poursuivi.

[21] CEDH, Grande Chambre, *S. et Marper c. Royaume-Uni* n°30562/04, 4 décembre 2008, §103

25. Conservation - Enfin, et la Cour attache une importance particulière à ce point-là, la conservation des données collectées doit répondre à des règles strictes, notamment concernant la durée de conservation. Ces fichiers de police ou de renseignements se doivent d'assurer une protection contre tout usage abusif ou extérieur des données qu'ils contiennent. La CEDH reconnaît de ce fait systématiquement comme une atteinte à l'article 8 de la Convention le fait pour un service de police ou de sécurité nationale de collecter et conserver des données personnelles, sans consentement.

26. Non-violation de l'article 8 - En outre, en 2009, des requérants se sont vus déboutés par la Cour de leurs demandes à l'encontre de l'État français. La Cour a en effet, dans sa décision *B.B. contre France*[22], conclu à la non-violation de l'article 8 pour ce qui était de l'inscription de condamnés pour viol au Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS). Les juges européens ont d'abord rappelé l'importance du droit à la protection des données personnelles, en particulier lorsqu'elles sont soumises à un traitement automatisé et qui plus est lorsqu'elles sont utilisées à des fins policières. En outre, la Cour a ici jugé que ce droit ne devait pas aller à l'encontre du but préventif de ce fichier et qu'ainsi, il n'y avait pas de disproportion entre l'objectif poursuivi et l'atteinte à ce droit. De plus, les données étaient non seulement protégées par le droit interne et restreintes à l'utilisation de certaines autorités uniquement, et les requérants possédaient eux-mêmes une possibilité de voie de recours en effacement.

27. Condamnation de la France - A l'inverse, la France a pu être condamnée par la CEDH dans d'autres affaires, en matière de droit d'effacement des données de différents fichiers de police. Ce fut le cas en 2013[23] à propos d'un refus de la police d'effacement du Fichier national d'empreintes digitales (FNAED) ou plus récemment en 2014[24], où l'affaire portée devant la Cour concernait l'effacement de données de l'ancien fichier Système de traitement des infractions constatées (STIC). Dans cette affaire, le requérant se plaignait de son inscription au fichier STIC malgré le classement sans suite de la procédure engagée à son encontre. La Cour a donc condamné la France pour avoir privé le requérant de son droit à l'effacement, d'autant plus que l'inscription de ses informations était une atteinte disproportionnée à ses droits à la vie privée.

[22] CEDH, *B.B. c. France* n°5335/06, 17 décembre 2009
[23] CEDH, *M.K. c. France* n°19522/09, 18 avril 2013
[24] CEDH, *Brunet c. France* n°2101/10, 18 septembre 2014

28. Refus de transmission des informations génétiques - Nombreux sont les autres exemples tant en matière de fichiers nationaux policiers, que de surveillance vocale[25], téléphonique, électronique, de géolocalisation[26] … La Cour a pu aussi très récemment condamner la France pour avoir pénalement poursuivi et condamné un individu ayant refusé de se soumettre à un prélèvement biologique. Ce prélèvement avait pour destination l'enregistrement dans le Fichier national des empreintes génétiques (FNAEG)[27]. Non pas que la Cour oppose le droit de protection des données à l'enquête pénale. Néanmoins ici, au sens des juges européens, le législateur français se devait de proportionner la durée d'effacement et le droit y étant rattaché à la gravité de l'infraction commise. Chose que, la CEDH le rappelle, le Conseil constitutionnel avait lui-même précisé dans une décision de conformité à la Constitution de la loi relative au FNAEG[28]. En outre, « *cette circonstance ne traduisait pas de juste équilibre entre les intérêts publics et privés en jeu* »[29].

La CEDH est donc claire sur son interprétation de l'article 8 : bien que ne mentionnant pas textuellement le droit à la protection des données personnelles, elle le rattache au droit au respect à la vie privée et familiale. Les juges européens portent une attention particulière au traitement de ces données dans le cadre policier, notamment lorsqu'elles sont soumises au traitement automatisé. En effet, bien que la recherche d'efficacité et de prévention soit indéniablement indispensable dans l'enquête et la politique pénale, il n'en reste pas moins qu'au sens de la Cour, les objectifs pénaux recherchés ne doivent pas porter une atteinte disproportionnée à ce droit à la protection des données.

29. Jurisprudence de la CJUE - Au-delà de la CEDH et son interprétation de la Convention, la Cour européenne de Justice (CJUE) a elle-même forgé sa propre jurisprudence applicable aux États-membres de l'UE. Elle a à plusieurs reprises rendu des décisions concernant le cas précis de la protection des données personnelles dans le cadre policier et pénal.

[25] CEDH, *Vetter c/ France* n°59842/00, 31 mai 2005
[26] CEDH, *Ben Faiza c/ France* n°31446/12, 8 février 2018
[27] CEDH, *Aycaguer c/ France* n°8806/12, 22 juin 2017
[28] Conseil constit., Décision n°2010-25 QPC16 septembre 2010
[29] *Op. cit.* note 23

En 2005, c'est la Cour de Justice des Communautés européennes qui a posé le premier cadre jurisprudentiel quant à l'interprétation de ce droit dans le domaine policier et de la sécurité publique[30], droit à l'époque régi par la directive de 1995. Ainsi la Cour a conclu à un principe selon lequel les dispositions de la directive ne s'appliquaient pas en ce qui concernait *« un traitement ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal* »[31]. Ainsi des « *objectifs d'intérêt général pourraient valablement justifier une ingérence dans la vie privée, garantie par l'article 8, paragraphe 2, de la CEDH, dès lors qu'elle est prévue par la loi, qu'elle est nécessaire dans une société démocratique à la poursuite de buts légitime et qu'elle n'est pas disproportionnée eu égard à l'objectif poursuivi* »[32]. Finalement, la Cour de justice semble se rallier à la logique de la CEDH, en ce qu'elle pose une limite au principe d'ingérence dans ce droit de protection des données, à savoir la proportionnalité entre le but pénal poursuivi et l'atteinte.

30. CJUE et conservation des données - Plus récemment, la Cour a pu réaffirmer sa jurisprudence de 2015 à l'aune des travaux sur les nouveaux textes de 2016. En effet elle rappelle que l'article 13 de la directive de 1995 exclut les exigences de loyauté de traitement des données personnelles lorsque l'objectif poursuivi est, là encore, en lien avec le domaine pénal ou la sûreté de l'État[33]. Néanmoins, elle est venue poser des limites dans ce domaine pénal : l'accès aux données, bien qu'exercé par des autorités publiques ou à des fins spécifiques, ne saurait être universel, indiscriminé et inconditionnel[34]. Une des préoccupations de la Cour – au même titre que la CEDH – fut aussi celle de la conservation des données : « *à cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe* [la sécurité nationale, la défense et la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales] » et de préciser qu'en effet « *étant donné que la conservation des données s'est révélée être un outil d'investigation nécessaire et efficace pour les enquêtes menées par les services répressifs dans plusieurs États membres et, en particulier, relativement aux affaires grave telles que celles liées à la criminalité organisée et au terrorisme, il convient de veiller à ce que les données conservées soient*

[30] CJCE, 20 mai 2005, « *Osterreichischer Rundfunk* » Aff. C-405/00 et C-139/01
[31] *Ibid*, §45
[32] *Ibid*, §51
[33] CJUE 8 avril 2015 « *Digital Rights Europe* » Aff. C-293/12 et C-594/12
[34] CJUE 8 avril 2014 « *Digital Rights Ireland* » Aff. C-293/12 et C-594-12, pts. 54 à 60

accessibles aux services répressifs pendant un certain délai, dans les conditions prévues par la présente directive [2006/24] »[35].

31. Exigences différentes - La CJUE a donc posé des principes s'apparentant à ceux énoncés par la CEDH dans sa jurisprudence. Néanmoins il semblerait que la Cour européenne des droits de l'Homme attache une importance plus spécifique au droit à la protection des données à caractère personnel et soit donc plus sévère envers les États et leurs pratiques policières. Cela s'explique cependant en partie au vu de son rôle, comparé à celui de la CJUE, qui elle est saisie en interprétation ou en validité d'une disposition. La Cour de Justice considère donc qu'il faut laisser une plus grande marge d'appréciation aux autorités publiques et plus particulièrement en matière judiciaire et pénale, afin de ne pas nuire aux objectifs de sûreté, de prévention et de détection de la criminalité. Principe que la Cour de Justice ne laisse cependant pas illimité ; là aussi, il faut tout de même respecter un minimum de proportionnalité entre l'objectif pénal poursuivi et l'atteinte qu'il porte au droit à la protection des données.

L'Europe et ses institutions ont donc posé, tant sous l'égide de la Communauté européenne que de l'Union, les trames législatives et conventionnelles à suivre quant à ce « nouveau » droit à la protection des données à caractère personnel. Néanmoins sur ce point, il semblerait que le législateur français avait alors une longueur d'avance sur les textes. Textes qui néanmoins ont vieilli et, à l'image de ce domaine complexe du Big Data et des flux de données, ne se sont pas toujours adaptés aux nouveaux enjeux mondiaux.

B. L'encadrement national

La France a été l'un des premiers pays européens à adopter une législation nationale protectrice du droit à la protection des données, législation qui a été renforcée par les adaptations européennes. Le législateur s'est donc montré réactif quant à la protection des données des citoyens français (I), notamment suite à la méfiance qu'avait inspirée la création d'un fichier de données par l'État. Le Conseil constitutionnel est d'ailleurs attentif à la protection de ce nouveau pan du droit au respect de la vie privée, et notamment concernant les fichiers de police (II).

[35] *Ibid*. §10 et §14

I. Les normes législatives

32. Genèse de la loi de 1978 - Le projet SAFARI laissant planer chez les français un sentiment de « *Big brother* », il a fait s'éveiller les consciences quant à la capacité informatique que les ordinateurs pouvaient avoir et, dès lors, jusqu'où pouvait aller leur utilisation. L'idée même d'une centralisation nationale des numéros de sécurité sociale a fait frémir ; l'État pourrait avoir accès à toutes sortes d'informations et s'en servir à des fins parfois inconnues du grand public. Ainsi les premières peurs de la collecte des données par les pouvoirs publics sont apparues, les citoyens se rendant bien compte du pouvoir de l'informatique et de la technologie.

Au lendemain de cette affaire de 1974, le gouvernement de l'époque a entendu les méfiances et y répondre en créant la Commission Informatique et Liberté. Celle-ci est chargée de réfléchir à une réglementation régissant la protection des données des individus ainsi que la déontologie de la collecte et du traitement de celles-ci. La France a donc été un précurseur en Europe quant à la législation sur la protection des données personnelles. En effet c'est finalement en 1978 que la loi dite « Informatique et Liberté »[36] est publiée, afin de protéger les citoyens français de « *l'auteur présumé de ces abus [*qui*] ne pouvait avoir qu'un nom dans l'imaginaire collectif : l'État* »[37].

33. Loi informatique et liberté - Cette loi, au-delà même du fait de créer un encadrement législatif des pratiques tenant au traitement des données personnelles, vient créer une autorité administrative indépendante ayant pour rôle de policer et contrôler tout abus dans ce domaine. La Commission Nationale de l'Informatique et des Libertés (CNIL) a pour mission d'informer « *toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations* », et de veiller « *à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi* »[38]. A ces fins, la loi prévoit donc des principes directeurs, des conditions de licéité du traitement des données et comporte même des chapitres spécifiques aux traitements de données à des fins médicales ou à des fins journalistiques, littéraires, artistiques. Enfin, le législateur a anticipé là encore les projets européens

[36] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[37] Disponible électroniquement : http://www.cil.cnrs.fr/CIL/spip.php?article1871
[38] *Op. cit.,* note 36, article 11

postérieurs en prévoyant la circulation des données entre États et même avec des États hors Europe[39].

34. Donnée à caractère personnelle - Pour la première fois la loi française fait mention de « *données à caractère personnel* », du « *traitement automatisé* », de « *fichiers* ». Une donnée à caractère personnelle se caractérise selon cette loi comme une information permettant l'identification d'une personne, de la désigner, finalement de la reconnaître. A ce titre l'article 2 de la loi précise qu'il peut s'agir d'un identifiant : on retrouve là les premiers signes de l'immixtion de l'informatique. La directive de 1995 n'aura pas une grande incidence sur cette définition nationale, n'y ajoutant qu'une précision spécifiant des éléments d'identifications comme l'identité « *physique, physiologique, psychique, économique, culturelle ou sociale* »[40]. On voit ainsi l'évolution de la science informatique et technologique, en ce que la directive 2016/680 va ajouter les termes tels que « *données de localisation* »[41], utilisation d'un tel système qui a conduit à de nombreux abus et atteintes aux libertés individuelles, en veut pour preuve la jurisprudence européenne[42].

35. Traitement automatisé - Le « traitement automatisé », au sens de la loi de 1978, se réfère à toute technique ou opération portant sur les données en question, et notamment leur collecte, utilisation, conservation et diffusion. Les textes européens, anciens ou actuels, considèrent le traitement de la même manière que le texte français. Il est donc possible de considérer un tel traitement dans un cadre policier ou pénal, en ce que la collecte d'informations personnelles d'un suspect va par exemple servir à l'enquête ou la prévention d'infractions pénales.

36. Fichier - Enfin, la notion de fichier s'envisage comme un ensemble de ces données « *structuré et stable* », « *accessibles selon des critères déterminés* »[43]. Cela sous-entend donc que la loi fixe les conditions d'accès, de gestion, de conservation et d'accessibilité de tout fichier national ou de traitement de données utilisées par une autorité ou un organe public. Il en est ainsi pour chaque fichier spécifique utilisé par les

[39] A l'époque, les États hors Communauté européenne. Les différentes lois modifiant la loi Informatique et Libertés n'ont pas rectifié les termes « Communauté européenne » lors du passage à l'Union européenne.
[40] Directive n°95/46/CE, *op. cit*. n°12, article 2(a)
[41] Directive 2016/680, *op. cit*. n°19, article 3
[42] Cf *supra* n°23
[43] *Op. cit*, note 36, article 3

forces de police ou l'autorité judiciaire, comme le fichier TAJ, qui est régi par les articles du Code de procédure pénale.

37. Matière pénale - A ce titre, la loi Informatique et Liberté a consacré des articles spécifiques au traitement des données à des fins pénales. En effet c'est en son article 9 que la loi fixe les conditions de traitement de ces données à de telles fins : uniquement certains organes et autorités peuvent y avoir accès et utiliser des données collectées à des fins pénales. Bien que certaines autorités comme les autorités de police et judiciaires aient accès à de telles données et les utilisent à des fins différentes que celles envisagées dans un cadre commercial par exemple, il n'en reste pas moins qu'elles peuvent se voir mises en demeure en cas de violation des principes de la présente loi, voire être sanctionnées.

Néanmoins, il s'avère qu'en 1978, les autorités policières, de gendarmerie et judiciaires ne disposaient pas encore des fichiers existants aujourd'hui et créés dans les années 1990. Bien que l'affaire SAFARI ait permis d'anticiper les éventuelles créations de fichiers nationaux relatifs à tous les citoyens, l'idée de fichiers policiers permettant la prévention et la lutte contre les infractions était fondamentalement différente de son actuelle conception. On peut donc se féliciter de l'anticipation législative de la France quant à la protection des données à caractère personnel, cependant au vu de la célérité qui était à venir dans le domaine informatique et des flux de données, il était évident que ce texte allait nécessiter une constante réformation.

38. Transposition - C'est d'ailleurs bel et bien ce qui s'est passé : la loi de 1978 s'est vue modifiée et modernisée un bon nombre de fois. La création de la CNIL a néanmoins été une aide primordiale dans l'adaptation à la modernisation des techniques de collecte et de traitement des données. Un peu plus d'une quinzaine d'années plus tard, l'Europe avec la directive de 1995 est enfin venue poser un cadre normatif de la protection des données. On aurait pu penser, qu'à juste titre, le législateur français allait s'empresser de transposer la directive afin d'adapter le droit national aux exigences européennes, et surtout afin de le moderniser. Mais étonnamment, il n'en a pas été ainsi : la France n'a ratifié le texte communautaire que dix ans plus tard, ne modifiant la loi Informatique et Liberté qu'en 2004[44]. Renforçant donc la protection des libertés individuelles, la

[44] Loi n°2004-801 du 6 août 2004 modifiant la loi du 6 janvier 1978

transposition de la directive n'avait cependant que pour but un encadrement des pratiques marchandes et commerciales en matière de traitement des données à caractère personnel. Le domaine policier et pénal a donc été un grand oublié de cette réforme, ne modifiant qu'en surface les dispositions de l'article 9 de la loi de 1978.

39. Fichiers policiers - Là encore un paradoxe peut être soulevé car à ce moment-là, les premiers fichiers policiers et d'infractions avaient été créés : le système de traitement des infractions constatées (STIC) et le système judiciaire de documentation et d'exploitation (JUDEX). Il aurait donc été souhaitable de la part du législateur de porter une attention particulière aux recommandations faites par le Comité des Ministres en 1987 afin de renforcer non seulement les droits des individus en matière commerciale, mais aussi en matière publique et policière. Il a donc fallu attendre la décision-cadre de 2008 pour que la France modifie son arsenal juridique dans le domaine de la protection des données personnelles dans le cadre pénal. La décision JAI, transposée en droit français, a permis d'évaluer le degré de protection des données personnelles des textes français régissant notamment le Fichier automatisé des empreintes digitales (FAED) et le FNAEG.

40. Réforme législative - Bien que soumise à de nombreuses réformes, la loi de 1978 a substantiellement été réadaptée surtout grâce à la loi de 2004, mais aussi à la loi pour une République numérique de 2016 qui est venue renforcer les droits des individus et les pouvoirs de contrôle et de sanction de la CNIL[45]. Cette loi a notamment eu vocation à anticiper l'application des nouvelles dispositions européennes applicables dès 2018. Mais alors même que le RGPD est concomitamment accompagné de la directive relative à la protection des données en matière pénale, la loi française de 2016 n'a pas eu vocation à réformer ou envisager un réexamen des dispositions en matière de traitement des données personnelles dans le domaine pénal. Les enjeux du Big Data et de l'utilisation de l'intelligence artificielle avaient cependant largement émergé ; il n'en reste pas moins qu'au 25 mai 2018, la directive 2016/680 a vocation à s'appliquer dans l'arsenal juridique français.

L'Assemblée Nationale a d'ailleurs travaillé en urgence en décembre 2017 à un projet de loi sur la protection des données personnelles, projet de loi adopté le 14 février 2018, qui

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

révisera en profondeur la loi de 1978 et abrogera la décision-cadre de 2008, afin de se préparer à l'entrée en vigueur du paquet européen de protection des données. L'avenir de la protection des données n'est donc désormais soumis qu'à l'observation minutieuse des États membres et de l'Union, à voir si les nouveaux textes européens vont être suffisamment denses et efficaces face à l'ampleur de l'immixtion du Big Data et du traitement par algorithmes dans le domaine de la justice pénale et le domaine policier.

Bien que les plus grosses évolutions et les plus gros risques d'atteintes aux libertés individuelles soient à venir, les institutions juridiques françaises, autres que le législateur lui-même, ont pu poser des principes d'interprétation jurisprudentielle ayant vocation à protéger les individus de toute atteinte disproportionnée lors d'une enquête policière et de procédures de prévention d'infractions. En effet, cette jurisprudence fait état de la présence – depuis bien longtemps encrée dans les pratiques policières – des technologies de surveillance et de collecte des données personnelles.

II. La jurisprudence constitutionnelle

Dans le droit français, le droit à la protection des données personnelles a principalement – si ce n'est exclusivement – une valeur législative ; la Constitution, de la même façon que la CESDH, ne fait pas expressément état d'une telle garantie.

41. Interprétation du Conseil constitutionnel - Une telle absence dans le bloc de constitutionnalité a donc mené le Conseil constitutionnel à développer sa jurisprudence en ce sens afin de préciser l'importance d'un tel droit à la protection des données à caractère personnel. Comme la CEDH peut le faire, le Conseil constitutionnel rattache ce droit au droit à la vie privée : « *Considérant, en second lieu, que la liberté proclamée par l'article 2 de la Déclaration des droits de l'Homme et du citoyen de 1789 implique le droit au respect de la vie privée ; que, par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* »[46]. Cette décision de 2012 a d'ailleurs censuré la majeure partie d'une loi du Parlement relative à la carte d'identité biométrique. Le Conseil s'était ici penché de manière précise sur les conséquences d'une telle carte pour les libertés

[46] Cons. constit. 22 mars 2012, n°2012-652 DC

individuelles dans le cadre policier. « *Le Conseil constitutionnel a en particulier considéré que, eu égard à la nature des données enregistrées, à l'ampleur du traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions permettant d'utiliser le traitement biométrique aux fins de police administrative ou judiciaire portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi* »[47].

Cette loi n'a donc pas eu de suites et a permis au Conseil de poser un principe là encore similaire à celui posé par la Cour européenne des droits de l'Homme : celui de la proportionnalité entre le but poursuivi par les forces de police lors du traitement de données et l'atteinte faite au droit de la protection de ces données. Le Conseil constitutionnel a eu de nombreuses occasions de se prononcer sur de tels sujets en matière de traitement des données personnelles dans un but pénal, et d'affirmer ces principes directeurs qui tracent la frontière entre nécessité de protection de l'ordre public et atteinte disproportionnée aux libertés individuelles.

42. Inconstitutionnalité - Un point lui a notamment été soumis de manière redondante, en ce qui concerne la conservation des données personnelles et le droit d'effacement de fichiers nationaux de la police et de gendarmerie. Ce fut d'ailleurs très récemment le cas dans une de ses dernières décisions en la matière, datant du 27 octobre 2017, à propos du droit d'effacement des données inscrites dans le fichier de traitement des antécédents judiciaires[48], le fichier TAJ.

L'inconstitutionnalité de l'article 230-8 du Code de procédure pénale était alléguée par le requérant. Celui-ci considérait que le texte le privait de son droit à l'effacement de ses données personnelles enregistrées dans le fichier TAJ, alors même qu'il avait été déclaré coupable mais dispensé de peine. En effet, la loi pénale prévoit un effacement de principe et une possibilité d'effacement notamment lors d'un non-lieu ou d'un classement sans suite du fait d'une insuffisance de charges. Dans un tel cas donc, les données seront préservées si personne n'intervient contre la conservation ; le cas échéant, la personne concernée a la possibilité de faire une demande d'effacement, demande traitée par le Procureur de la République. En l'espèce, le requérant ne faisant partie d'aucune des deux catégories de la loi, il a vu sa demande d'effacement refusée, ce qui a motivé sa demande de QPC. Le Conseil a finalement fait droit à sa demande et a

[47] G. DESGENS-PASANAU, *op. cit* note 13, p.168
[48] Cons. constit. 27 octobre 2017, n°2017-670 QPC

abrogé l'alinéa 2 de l'article 230-8 du Code de procédure pénale, considérant qu'il portait une atteinte disproportionnée au droit au respect de la vie privée du requérant et de toute personne de trouvant dans une situation similaire.

43. Droit à l'effacement - Le Conseil aborde là une question particulièrement sensible du droit à l'effacement, qu'il considère souvent trop restreint. Il semble d'ailleurs qu'il se conforme à la jurisprudence de la CEDH qui condamne souvent les États parties pour restreindre trop strictement ce droit. Le Conseil veut donc clairement ouvrir ici le droit à l'effacement des données personnelles du fichier TAJ, à se demander s'il ne sous-entend pas qu'il faudrait appliquer une telle décision à des fichiers similaires comme le FNAEG par exemple. Les juges constitutionnels font preuve d'une volonté de renforcer la protection des libertés individuelles, et même des condamnés, dans le cadre préventif du domaine policier. Car dans le cas de ce fichier, le Conseil considère que la durée maximale de conservation des données des mis en cause n'est pas fixée assez précisément : en fonction de l'âge et du type d'infraction, cette durée de conservation peut varier entre cinq et quarante ans. Les juges ajoutent que cette imprécision joue de plus pour un très grand nombre d'individus, à savoir toute personne mise en cause pour un crime, délit ou contravention de cinquième classe, hors les cas d'acquittement, relaxe, non-lieu et classement sans suite.

44. Article 2 de la DDHC - La jurisprudence du Conseil constitutionnel a en effet durci ses exigences au fil du temps à l'égard du traitement des données personnelles. Déjà sous le régime des anciens fichiers STIC et JUDEX, il avait pu assimiler le droit à la protection des données personnelles au droit au respect de la vie privée – bien que la décision elle-même concernait un autre contexte[49]. Au sens des juges de la constitutionnalité, l'article 2 de la Déclaration des droits de l'homme et du citoyen (DDHC) implique le droit au respect de la vie privée. Droit qui a valeur constitutionnelle et qui peut dès lors être invoqué à l'appui d'une QPC. C'est donc la majeure partie du temps cet article 2 de la DDHC qui sera invoqué par des requérants en cas d'atteinte à leur droit à la protection des données personnelles devant le Conseil. Ce dernier a renforcé ses exigences à l'occasion du contrôle de la loi relative à la carte d'identité biométrique : il explique qu'on est passé d'un contrôle limité à l'absence de disproportion manifeste entre le but poursuivi et l'atteinte au droit, à un contrôle de proportionnalité bien plus

[49] Cons. constit. 23 juillet 1999, n°99-416 DC, loi portant création d'une couverture maladie universelle

poussé[50]. A ce titre, le Conseil contrôle le nombre de personnes concernées par le fichier en question, la sensibilité particulière des informations susceptibles d'être contenues dans ce fichier et ses finalités d'utilisation[51].

Le Conseil constitutionnel attache donc une attention importante au respect du droit à la protection des données à caractère personnel dans le domaine pénal, et ce parfois au détriment du but recherché par la disposition contestée. En effet bien que la collecte des données et leur conservation dans certains fichiers protégés soient utiles ou potentiellement utiles à la prévention d'infractions et à la sécurité intérieure, le Conseil refuse cependant d'être clément du seul fait du domaine concerné. La matière pénale et la sûreté invoquent certes des compromis entre atteintes à certains droits au profit de la recherche de la vérité et de la prévention d'infractions. Néanmoins le Conseil reste méfiant face au surdéveloppement de l'usage de technologies modernes et du Big Data dans le cadre policier et judiciaire, au risque de passer à côté de la violation de certains droits fondamentaux, sans possibilité de marche arrière. L'usage du Big Data et de l'intelligence artificielle fait en effet appel à l'anticipation et à l'attention, et ce pas seulement du côté des enquêteurs et policiers, mais aussi de celui des garants et protecteurs des droits et libertés individuels.

§2 : La création d'un « Big Data policier »

La proportionnalité entre objectif de lutte contre la criminalité et respect des droits et libertés individuels est parfois difficile à apprécier par les services de police et de gendarmerie. D'autant plus que le nombre de données accessibles ne fait que grandir ; la mise en place d'un Big Data propre à la police doit continuer de s'en tenir à certains types de données uniquement (A). Néanmoins les nouvelles perspectives offertes par l'évolution numérique et sociale ouvrent la possibilité de collecte vers d'autres formats de données, qui peuvent se révéler extrêmement utiles aux services d'enquête (B).

[50] Commentaire décision Cons. constit. n°2017-670 du 27 octobre 2017
[51] *Ibid.*

A. Les données à caractère personnel collectées par la police

La loi française, cumulée avec les textes et exigences européennes, s'accordent à définir précisément ce qu'on peut entendre par le traitement des données à caractère personnel de manière générale (I). Ces définitions sont donc applicables dans tout secteur d'activité ; les autorités françaises ont cependant tendance à collecter certains types de données bien précis (II).

I. Les définitions textuelles

45. Enjeux du cadre policier - Le traitement du Big Data et les enjeux juridiques qu'il présente sont d'autant plus difficiles à appréhender et à considérer dans un contexte policier. En effet le principe même de l'enquête étant la recherche de la vérité, la loi va tenter de faire mener au mieux les procédures. L'arsenal juridique et procédural fait donc prévaloir l'efficacité, la rapidité et la précision de l'enquête en mettant à disposition de ses différents acteurs, et notamment des policiers et enquêteurs, des outils facilitant cette tâche. Au-delà même des procédures d'investigation, la prévention est un des rôles et buts principaux des acteurs pénaux, et donc des services de police. A ce titre, les informations mises à leur disposition et qu'ils collectent eux-mêmes vont être traitées afin de pouvoir servir pour le présent, mais vont aussi être conservées afin qu'elles puissent potentiellement se rendre utiles dans le futur.

Ces buts et rôles attribués aux services d'enquête et de police sont évidemment contrebalancés par le nécessaire respect des droits des individus impliqués dans les différents travaux d'investigation, de prévention, de sûreté, de sécurité. Protection d'autant plus importante qu'en ce qui concerne les données personnelles dans le cadre policier, leur transfert et leur flux se doivent d'être favorisés à des fins d'efficacité de l'espace liberté, sécurité et justice au niveau de l'Union européenne. Il apparaît donc primordial en matière de collecte des données de définir plus que précisément les différents termes reliés à ce droit. Il semblerait d'ailleurs que les textes tendant à l'encadrement de la protection des données dans le cadre des procédures pénales se doivent d'être ouverts à la modification et à la réformation. Car dans la thématique du Big Data lui-même, on pourrait presque considérer qu'une branche se crée en matière policière : un Big Data policier. Toutes les nouveautés technologiques, informatiques et de flux, ne sont pas applicables qu'au monde marchand mais viennent aussi conquérir les

services de police. A ce titre, les différents textes encadrant la protection des données doivent rester un minimum modulables, sujets à tout changement au vu du caractère exponentiel que peut prendre la rapidité de l'évolution du transfert des données.

46. Données à caractère personnel - Dès le 25 mai 2018, la loi française en matière de protection des données personnelles dans le cadre de la prévention d'infractions pénales va donc changer au profit de la directive européenne de 2016. Ainsi au sens de la directive, les données à caractère personnel ne peuvent être relatives qu'aux personnes physiques ; seules celles-ci sont donc protégées. Ces données spécifiques sont requalifiées en informations qui permettront dès lors d'identifier la personne en question. Une telle identification peut se faire « *par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »[52]. Il est notable ici qu'une telle définition ne peut qu'être adoptée dans le droit français car, comme mentionné précédemment[53], elle présente bien plus de précision que celle posée par la loi de 1978.

47. Violation des données à caractère personnel - La « violation » de telles données fait référence, selon la directive, non pas à une atteinte à la vie privée comme l'entendent les différentes juridictions européennes et françaises, mais à une violation de sécurité encadrant les données en jeu. Des sanctions sont ainsi à prévoir en cas de telles violations, qui peuvent être intentionnelles ou non-intentionnelles ; peut donc être punie la négligence de sécurité à l'égard de données personnelles. Cette violation doit cependant avoir entraîné « *la destruction, la perte, l'altération, la divulgation non autorisée (…) ou l'accès non autorisé* »[54] des données. Enfin, l'article 3 de la directive mentionne aussi comme pouvant être considérées à caractère personnelles les données génétiques[55], biométriques[56] et concernant la santé[57]. Données qui ne sont pas à négliger en ce que dans le contexte policier, ces informations sont très régulièrement collectées et peuvent servir tant à l'enquête qu'aux procédures postérieures.

[52] Directive 2016/680 (UE), article 3(1)
[53] Cf *supra* n°34
[54] *Ibid*, article 3(11)
[55] *Ibid*, article 3(12)
[56] *Ibid*, article 3(13)
[57] *Ibid*, article 3(14)

48. Traitement - Le deuxième terme central de la protection des données à caractère personnel dans le cadre pénal est celui du traitement : c'est en effet celui-ci qui est encadré afin de s'assurer que la prévention et la recherche d'infractions ne portent pas atteinte aux intérêts ou libertés des individus concernés. La définition donnée par la directive peut s'avérer transposable à celle existante dans la loi Informatique et Liberté. Néanmoins, des différences existent, dont une première qui n'est pas des moindres : le texte européen mentionne que ce traitement peut être fait de manière automatisée. C'est en effet tout l'enjeu de la modernisation du droit à la protection des données personnelles, à savoir l'adapter aux nouveaux moyens de transfert et de traitement « intelligents » - à l'image des algorithmes et intelligences artificielles – qui intègrent les services publics et de police. Hormis cet élément textuel, la liste non exhaustive faite par le législateur européen pour décrire les procédés renvoyant aux traitements de données est pratiquement similaire au texte français. Envisagé dans un contexte pénal et policier, le traitement se réfère donc par exemple à la collecte d'informations auprès de suspects ou de victimes lors d'une enquête ; informations qui peuvent être ensuite enregistrées dans des fichiers spécifiques, conservées voire réutilisées ultérieurement à d'autres fins que celles de l'enquête en cours. L'exemple le plus populaire sera celui du FAED[58].

49. Autorité compétente - Enfin, le cadre de prévention et de détection d'infractions pénales étant spécifique et bénéficiant d'un texte distinct du Règlement général sur la protection des données (RGPD), il convenait naturellement de préciser quelles autorités étaient compétentes. En effet, là où le RGPD s'adresse principalement aux personnes privées, morales et relations commerciales, la directive 2016/680 est censée viser uniquement des autorités et services publics, étant envisagée dans un cadre pénal. Définir ces personnes compétentes permet aussi d'anticiper l'échange et la circulation de données entre États, ou plutôt entre autorités ayant la même compétence. Le texte européen vise donc une autorité publique qui est, au niveau national, compétente pour la prévention, la détection d'infractions, pour l'enquête, les poursuites, sanctions et exécutions pénales, mais aussi toute autorité compétente en matière de sécurité publique. Ainsi une telle autorité peut, en France, être les services de police judiciaire, de gendarmerie, mais aussi les juges d'instruction, les juges d'application des peines ou encore le Procureur de la République… mais exclut les autorités administratives ou un maire par exemple. La seule exception à cette condition sera, selon l'article 3(7) de la directive, celle où l'État membre

[58] Cf *infra* n°52

désigne par la loi un autre organisme ou entité en charge de telles missions et lui accorde des prérogatives pénales d'autorité publique.

II. Les données personnelles collectées par la police française

50. Fichier EDVIGE - « *En 2009, 58 fichiers de police et à usage de police avaient été recensés par la mission d'information* »[59]. Ce dénombrement fait en 2009 par Delphine Batho et Jeacques-Alain Bénisti avait pour objectif d'alerter sur le chiffre grandissant des différents types de fichiers policiers et du Ministère de l'Intérieur, et ainsi de questionner leur réel encadrement. La rédaction d'un tel rapport a notamment trouvé son origine dans la proposition de création du fichier dit EDVIGE en 2008 : un fichier d'exploitation documentaire de valorisation de l'intérêt général. Un titre très esthétique mais cependant trompeur : ce fichier avait pour vocation l'enregistrement de multiples données concernant des personnes à caractère public, que ce soit un individu ou un groupe, mais aussi tout individu présentant un risque pour l'ordre public. Au même titre que le fichier SAFARI en 1974, près de trente ans après, la sonnette d'alarme a été tirée. Ce fichier élargissait non seulement le spectre des données susceptibles d'être collectées, mais avait de plus une finalité de détection de comportements « potentiels ». La création d'un tel fichier répondait en effet à la politique pénale mise en œuvre, qui reposait notamment, dans d'autres pans du domaine pénal, sur la notion de dangerosité[60]. Le projet EDVIGE fut finalement abandonné, laissant cependant au législateur un avertissement quant à la nécessité de renforcer l'encadrement des fichiers de police et de leur création.

Il existe donc un grand nombre de fichiers spécifiques à la police susceptibles de contenir, collecter ou traiter des données personnelles d'individus. Ceux-ci vont des logiciels bureautiques, en passant par les fichiers administratifs jusqu'aux fichiers d'identification et d'antécédents judiciaires. Ce sont ces derniers qui nous intéresseront à titre d'exemple ici, en ce que leur utilisation dans un cadre prédictif serait le plus probable.

52. Fichiers d'identification judiciaire - Hormis le fichier TAJ, qui conserve tout de même une certaine connotation, les forces de police ont aussi à leur disposition des fichiers spécifiques à certaines caractéristiques des individus, permettant lors d'un

[59] D.BATHO et J.A. BENISTI, Rapport d'information n°4113 sur la mise œuvre des conclusions de la mission d'information sur les fichiers de police, Assemblée Nationale
[60] A titre d'exemple, c'est durant la mise en œuvre de cette politique pénale qu'ont été créées certaines mesures et périodes de sûreté.

processus judicaire d'identifier, de rapprocher des informations voire de les faire concorder. C'est le cas du fichier automatisé des empreintes digitales et du fichier national des empreintes génétiques. Selon la CNIL, pas moins de 4 682 387 individus sont actuellement enregistrés dans le FAED et au 1er septembre 2013, 2 547 499 profils génétiques identifiés et 149 097 non-identifiés l'étaient dans le FNAEG.

Le FAED est régi par le Code de procédure pénal aux articles 78-3, 55-1 et 624-7, qui disposent notamment que toute personne susceptible de fournir des renseignements à l'enquête peut voir ses empreintes digitales et palmaires relevées ou se faire photographier. Ces prélèvements sont donc associés à l'identité et sauvegardés dans le fichier, pouvant de ce fait servir à des procédures futures si elles ne sont pas soumises à effacement. Le FNAEG est lui régi par les articles 706-54 et suivants et R53-9 et suivants du Code de procédure pénale. Toute personne étant en lien avec les faits relatifs à une enquête pour un crime et un délit peut avoir à se soumettre à de tels prélèvements génétiques, plus communément entendu comme prélèvement ADN. Au même titre que le FAED, l'empreinte est rattachée à l'identité de l'individu et à l'affaire en cours.

52. Traitement des antécédents judiciaires - En 2013, le nouveau fichier recensant les personnes mises en cause pénalement regroupait déjà 12 200 000 fiches[61]. Un tel chiffre doit en fait être compris à la lumière de la loi dite LOPPSI 2[62] de 2013 qui a supprimé les anciens fichiers STIC et JUDEX, jusqu'alors indépendants l'un de l'autre, pour les regrouper en un seul et même fichier commun aux services de police et de gendarmerie : le fichier TAJ. Celui-ci a été introduit dans le Code de procédure pénale aux articles 230-6 à 230-11 et aux articles R40-23 à R4034. Ce fichier a pour but de stocker et traiter des informations relatives tant à un mis en cause qu'à une victime de crime, délit ou contravention de cinquième classe.

L'article R40-26 liste les différentes données à caractère personnel qui peuvent être collectées, et ce tant pour les personnes physiques que morales. Pour les personnes physiques mises en cause par exemple, les données pouvant être collectées vont de l'identité, la nationalité, l'adresse, en passant par la situation familiale, les numéros de téléphone et adresses électroniques, jusqu'à ce qui est appelé « *état de la personne* » et

[61] M.LENA, « Les attentes liées à l'entrée en vigueur du Traitement des antécédents judiciaires », *AJ Pénal*, n°12, 11 décembre 2013, p.635
[62] Loi n°2011-264 du 14 mars 2011

son « *signalement* ». Il est également précisé qu'une photographie de la personne en question peut être collectée, notamment à des fins de « *reconnaissance faciale* ». Concernant la victime, la liste est pratiquement similaire, en ce que le signalement et la photographie sont exclus.

Le texte dresse donc une liste limitative des données pouvant être collectées aux fins de « *faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs* »[63], l'article R40-24 assurant d'ailleurs le respect du droit à la protection des données personnelles, mentionnant expressément l'article 8 de la loi de 1978 qui encadre elle-même les types de données pouvant être soumises à la collecte. Un terme semble cependant interroger : l'« *état de la personne* ». Le sens précis de ces termes paraît en effet relativement flou et imprécis, en ce qu'ils sont censés désigner d'autres caractéristiques personnelles du mis en cause que celles citées avant cet « *état de la personne* ». Là où le signalement fait appel à des caractéristiques physiques, ou encore à des vêtements que le suspect aurait pu porter, la signification de l'état de la personne ne semble pas si évidente. On pourrait de ce fait se demander si de tels termes n'auraient pas été introduits afin justement d'ouvrir ce fichier à la collecte d'autres données n'entrant pas dans le cadre de celles précédemment citées.

53. Fichier judiciaire automatisé des auteurs d'infractions sexuelles ou violentes - Le FIJAISV, créé en 2004 par la loi Perben II, recense les personnes majeures mais aussi mineures ayant été impliquées – on entend donc condamnées, ayant fait l'objet de sanctions éducatives, d'une composition pénale – dans la commission d'un délit, d'un crime sexuel ou violent. Par infraction violente, on entendra l'assassinat, le meurtre, accompagnés de tortures et actes de barbaries, viol ou violence. Les infractions sexuelles couvrent tous les types de délits et crimes à caractère sexuel. La création de ce fichier a notamment été motivée par la prévention de la récidive, mais aussi à des fins policières, afin de permettre aux services de sécurité et d'enquête d'identifier et localiser rapidement toute personne enregistrée dans le fichier. A ce titre, l'adresse doit être actualisée régulièrement dans ce fichier, et ce à la charge de la personne concernée. Le FIJAISV est régi par les articles 706-53-1 à 706-53-12 du Code de procédure pénale, et contient l'identité de la personne et la nature de la décision rendue à son encontre dans le cadre de poursuites pour une infraction sexuelle ou violente.

[63] Article 230-6 du Code de procédure pénale

54. Potentiel prédictif - Bien que cette liste de fichiers soit non-exhaustive, on voit ici que de manière générale, à travers la collecte des données, la police a accès à des informations à caractère plutôt « objectif » et fixe, tels que l'identité, les coordonnées, les caractéristiques physiques, l'âge … C'est ensuite en fonction de la nature du fichier dans lequel ces données sont enregistrées que la police leur trouvera un intérêt, soit à des fins d'enquête soit à des fins de prévention d'une infraction.

Envisagés dans un cadre non plus préventif mais prédictif, l'utilisation de ces fichiers prendrait une toute autre tournure et un tout autre sens. Les données en effet enregistrées dans ces fichiers pourraient servir par exemple à faire des statistiques au niveau d'un commissariat, d'un secteur, sans pour autant utiliser les informations spécifiques à une personne en particulier : c'est l'intérêt préventif des moyens de police. Néanmoins dans un cadre prédictif, il pourrait en être autrement : on rentre là dans les domaines du *data surveillance* ou de la surveillance tout court, alors même que les données attribuées à un fichier ne poursuivaient pas ce but initialement. Dans le cadre de certaines techniques algorithmiques de police prédictive, ces données pourraient être à termes utilisées par la machine, en évaluation du risque criminel d'un voisinage par exemple[64]. Les principes de finalités et de durée de conservation des données dans les fichiers policiers s'en verraient altérés.

Cependant ces données restent celles tenant au nom, au sexe, à l'âge, aux antécédents judiciaires : ce sont des données juridiquement et administrativement vérifiables, objectivement « vraies » – à moins d'une erreur d'enregistrement ou de collecte. Une autre problématique apparaît en fait dans le contexte pénal et policier, notamment en matière d'utilisation de l'intelligence artificielle : des données différentes de celles à caractère administratif ou judiciaire pourraient être recherchées. Ces informations constituent un nouveau pan des données du Big Data policier, qu'on pourrait appeler « données comportementales ».

[64] Cf *infra* n°75

B. Les nouveaux types de données du Big Data policier

55. Données intrinsèques à l'individu - Ces « données comportementales » pourraient en fait être qualifiées de subjectives, en opposition aux données objectivement obtenues et vérifiables des fichiers traités précédemment. En effet vérifier la véracité d'une adresse, d'un nom ou d'un numéro de téléphone d'une personne s'avère assez évident et facilité par les registres d'état civil, la possession d'une carte d'identité par la personne etc. Dès lors, informer l'individu concerné du traitement de ces données paraît relativement facile pour les services de police. Néanmoins qu'en est-il de données « déduites » du comportement ou de l'antécédent judiciaire de la personne ? C'est en effet le type de données qui pourrait intéresser le travail policier dans l'utilisation d'algorithmes : déduire du taux de récidive d'une personne une dangerosité ou un risque élevé, afin que le logiciel s'attarde plus particulièrement sur la personne.

Toute la question repose sur le fait de savoir si l'efficacité d'un algorithme prédictif justifierait la collecte et le traitement de données comportementales, psychiatriques, intrinsèques à l'individu ; données qui de ce fait ne sont pas nécessairement stables et certaines. Une telle interrogation intégrerait logiquement le travail d'autres professionnels et entités différentes du travail policier – qui jusque-là, peut se contenter de ses propres effectifs, possédant même sa propre police scientifique pour le prélèvement et l'analyse de données génétiques par exemple.

56. Profilage commercial - On connaissait jusqu'à maintenant la naissance et le développement, surtout dans le système de Common Law, du profilage criminel. Ce terme décrit une « *technique criminalistique contribuant à l'établissement de la preuve pénale en facilitant l'identification d'un criminel inconnu* » qui « *consiste à établir le profil psychologique de l'auteur potentiel d'une infraction à partir de l'acte réalisé et des différentes constatations effectuées par les services d'enquête (...)* »[65]. A travers le profilage criminel donc, la ou les personnes (qui ne sont pas nécessairement des professionnels du milieu pénal) tentent d'établir une sorte de portrait-robot social et comportemental ; portrait-robot qui doit ensuite aider les services d'enquête dans leur « traque » de l'auteur d'une infraction.

[65] Lexique des termes juridiques, *Dalloz*, 2014, p.750

Ainsi, au même titre que ce profilage criminel, le Big Data,le développement des flux internet et électroniques ont permis de faire apparaître une pratique de profilage commercial. Une partie du RGPD couvre d'ailleurs cette pratique, qui est l'une des principales raisons de la collecte des données par les entreprises. Sans s'épancher précisément sur le sujet, il s'agit pour les plateformes marchandes, les entreprises et réseaux sociaux de collecter et tracer toutes les informations et utilisations de site internet et les pratiques électroniques des utilisateurs du web pour affiner un certain « profil commercial » de la personne, afin de mieux cibler les potentiels clients et acheteurs. Le nouveau règlement européen définit en effet ce profilage comme un « *suivi du comportement* » de la personne « *afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit* »[66]. Ce suivi est fait la plupart du temps si ce n'est tout le temps, par des algorithmes assignés à cette tâche uniquement : faire un suivi des données et habitudes du consommateurs, les analyser et en déduire des préférences pour que l'entreprise adapte ses techniques de vente.

57. Un nouveau profilage criminel - Ainsi, au même titre que le profilage commercial par le suivi sur internet, le profilage est prévu dans la directive qui va s'appliquer le 25 mai 2018. Il y est même expressément défini comme « *toute forme de traitement automatisé de données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique notamment pour analyser et prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne* »[67]. Ce qui est envisagé ici, c'est bien la collecte de données autre que celle citée par le Code de procédure pénale jusqu'à maintenant : la directive conçoit ici que les services de police ou judiciaires aient accès à des données bien plus larges que la simple identité et les antécédents pénaux.

L'hypothèse est ici que soit les services de police se servent de données collectées par les entreprises via leurs propres algorithmes, soit que les forces de police elles-mêmes aient recours à la constitution d'un profil criminel via le suivi des habitudes sur internet. Là où le profilage criminel sert à établir un profil pour resserrer et préciser les recherches d'un auteur d'infraction, le profilage automatisé sert à prédire et anticiper une infraction qui n'est pas encore commise. Dans un tel cas, les données sont collectées sur une

[66] *Op. cit*. note 18, §24 du RGPD
[67] *Op. cit*. note 19, article 3(4) de la directive

personne en particulier, analysées, et déduites comme constituant un comportement à risque criminogène ou pas. Dans une moindre mesure, une telle pratique s'apparenterait à la vidéosurveillance : suivre une personne désignée, observer ses actes et en déduire une nécessité de « garder un œil » sur elle.

58. Fichiers terroristes - Au-delà de l'enjeu que représente l'utilisation d'internet, on assiste à une multiplication des fichiers à connotation pénale spécifique. L'exemple le plus contemporain est celui des fichiers antiterroristes, qui attachent aux données des personnes enregistrées la connotation terroriste, radicalisée ou au contact de personnes radicalisées. Le Fichier des personnes recherchées (FPR), ou encore le Fichier atteinte à la sûreté de l'État (désormais connu sous le nom de Fichier S), sont des fichiers policiers qui servaient bien avant la recrudescence des actes terroristes, à des fins de surveillance de certaines personnes connues des services pénaux.

Depuis les années 2015, ils se sont vus accompagnés de fichiers de plus en plus spécifiques : le Fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) et le Fichier judiciaire national automatisé des auteurs d'infractions terroristes (FIJAIT). La nécessité de lutte contre cette criminalité violente, qui se caractérise par un renforcement de la prévention et de la surveillance, fait apparaître des fichiers dont la connotation « à risque » est de plus en plus exacerbée. Les nouveaux enjeux criminels actuels sont donc une prérogative de plus pour la police, qui doivent affiner la collecte de données effectuée dans le cadre de leur travail.

Jusqu'à maintenant donc, les données collectées par les services de police servent à alimenter des fichiers et sont relativement fixes. Néanmoins, la collecte et la conservation des données par la police inspirent toujours la méfiance, en ce qu'en conservant les informations à propos d'une personne dans un fichier ou un autre, la personne se voit en quelque sorte catégorisée : « *d'une part ce fichier risque de « préorienter » l'enquête à partir du soupçon qu'il fait peser d'emblée sur les individus fichés, d'autre part il risque de préfigurer une peine perpétuelle* » et instaure de ce fait « *une mémoire sans oubli ni pardon* »[68]. Mémoire qui pourrait être d'autant plus accentuée par la mise en lien de ces fichiers avec les techniques de police prédictive et d'intelligence artificielle. En effet, dès lors qu'un algorithme est calibré pour déterminer un comportement ou événement à risque, et dans l'hypothèse où cette analyse se fait grâce

[68] P.Y. MAROT, « Fonctions et mutations des fichiers de police », *AJ Pénal*, février 2007, p.61

aux fichiers policiers ou au profilage effectué, l'utilisation des données de la personne prend une toute autre dimension. D'autant plus que dans le cadre du *predictive policing*, ce sont plus les données comportementales et sociales qui intéressent le *machine learning* que les données de « simple identification ».

Bien que les données biologiques telles que les empreintes génétiques ou digitales soient indispensables à certaines enquêtes, l'utilisation de l'intelligence artificielle au profit de la prédiction pourrait changer la donne en matière de criminalité et sous-entendrait même de ne plus avoir besoin d'identification génétique *a posteriori* de la commission de l'infraction. L'utilisation d'une multitude de données de types différents permettrait à la police d'anticiper l'infraction. A cet égard, on pourrait presque considérer l'effacement de nombreuses données qui deviendraient obsolètes ; au profit cependant de l'enregistrement de données bien plus délicates et sensibles voire instables …

Section 2 : Les nouveaux enjeux de collecte des données

Il semblerait donc que la police puisse s'en tenir aux fichiers dont elle dispose pour prévenir et lutter contre la commission d'infractions. Néanmoins, avec cette multiplication des sources de données, les limites de la collecte sont parfois difficilement identifiables, compliquant le travail pour les services de police et de gendarmerie (§1). Limites qui sont parfois franchies, auquel cas les atteintes peuvent être de grande ampleur : c'est d'ailleurs un constat à répétition qui a pu être fait aux États-Unis, n'appréhendant pas juridiquement les enjeux du Big Data de la même façon que l'Europe (§2).

§1 : Le Big Data, un enjeu technique pour les services d'enquête

Là encore, l'Union européenne et ses États membres imposent des principes stricts et des marches à suivre à respecter dans le cadre de la collecte et du traitement de données (A) ; principes qui se voient mis en jeu par les perspectives qu'ouvre le Big Data (B).

A. Les obligations encadrant la collecte des données

La protection des données tient à ce principe de respect de la vie privée, en ce que les données en question sont à caractère personnel. C'est afin de garantir ce principe que les différentes normes, et majoritairement la directive 2016/680, imposent des obligations et lignes de conduite dans la collecte et le traitement de ces données (I). Un écart dans cette marche à suivre ou une violation fait évidemment encourir une sanction, et ce sans exception faite au statut des services de police ou de renseignements. La protection des données des individus est encore plus renforcée par les droits qui leurs sont accordés dans le traitement de celles-ci (II).

I. Les obligations tenant à la collecte et au traitement

Il est possible de regrouper les différents principes tenant au traitement des données personnelles en trois grandes obligations : la licéité, la loyauté et la finalité. En effet ces principes sont présents pour toute forme de collecte et de traitement des données, que ce soit pour les entreprises et personnes morales que pour les personne publiques, l'État, les forces de police ou de renseignements. Néanmoins la spécificité du caractère pénal du traitement n'en est pas moins atténuée, notamment en ce que la finalité est fondamentalement différente de celles qui pourraient être poursuivies par des entreprises ou personnes privées : « *lorsque des données à caractère personnel sont traitées à de telles autres fins, le règlement (UE) 2016/679 s'applique, à moins que le traitement ne soit effectué dans le cadre d'une activité ne relevant pas du champ d'application du droit de l'Union* »[69].

59. Licéité - La protection des données personnelles apparaissant de plus en plus comme un droit rattachable au droit au respect de la vie privée, il paraît évident que le législateur prévoie des normes encadrant toute collecte et analyse de ces données. Tout fichier ayant pour vocation le contenu de données spécifiques pour des fins déterminées devra avoir une base légale. Celle-ci doit effectivement fixer les conditions dans lesquelles les services d'enquête pourront par exemple prélever l'ADN d'une personne ; on ne pourrait imaginer un officier de police judiciaire interpeller une personne quelconque à des fins de prélèvements ou de recueil de son identité sans motif légitime

[69] *Op. cit*. note 19, article 9(1) de la directive

ou sans informer la personne des raisons. Tout fichier ou nouveau recensement d'informations collectées se doit donc d'être prévu et autorisé par la loi – un commissariat ne pourrait pas arbitrairement créer un fichier conservant des informations sur des personnes uniquement impliquées dans certaines infractions spécifiques, sans utiliser les systèmes déjà existants. Nombreux ont été les exemples – certains vus précédemment[70] – de fichiers qui n'ont finalement pas vu le jour, jugés trop attentatoires à certaines libertés et droits. De telles ébauches n'ont pas eu de suites, les projets ou propositions de loi ayant été rejetés.

60. Loyauté - Le principe de loyauté est, avec la licéité, l'un des premiers à être imposé par la directive 2016/680 en son article 4. Une telle notion prend une dimension un peu plus délicate ici, au vu du contexte pénal auquel elle prend part. Le législateur européen décrit le principe de loyauté comme « *une notion distincte du droit à accéder à un tribunal impartial (…). Les personnes physiques devraient être informées des risques, règles, garanties et droits en ce qui concerne le traitement de données à caractère personnel les concernant et les modalités d'exercice de leurs droits par rapport au traitement* »[71]. Autrement dit, le principe du traitement loyal veut que ce dernier ne puisse pas en soi porter préjudice à la personne concernée et qu'elle puisse donc être informée de toute voie de recours étant à sa disposition, ou des droits encadrant le traitement de ses données.

En outre, en matière pénale, et notamment dans le cadre de la sécurité ou de la prévention d'infractions, les pratiques policières ou d'enquête nécessitent parfois une part « d'ignorance » de la personne. En matière de vidéosurveillance par exemple, de réutilisation de données déjà enregistrées, ou encore de comparaison de nouvelles données avec ces dernières etc. La directive rappelle en ce sens que la loyauté et la transparence de l'utilisation des données à caractère personnel « *n'interdit pas en soi aux autorités répressives de mener des activités telles que des enquêtes discrètes ou de la vidéosurveillance (…) pour autant qu'elles soient déterminées par la loi et qu'elles constituent une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des intérêts légitimes de la personne physiques concernée* »[72].

[70] Cf *supra* n°50
[71] *Op. cit.* note 19, §26 de la directive
[72] *Ibid*

Le but de la surveillance policière du Big Data n'est en effet pas de suivre à la trace tout un chacun, mais bien de prioriser la surveillance de ce qui peut présenter un risque pour la communauté. A ces fins, c'est le terme de proportionnalité tout autant que celui de loyauté qui doit être pris en compte, tout en retenant les finalités poursuivies par ces autorités qui collectent les données.

61. Finalités - Le principe de finalité s'avère être sûrement l'un des plus délicats à appréhender dans le cadre pénal du traitement des données. La directive et le RGPD le répètent dans chacun des textes : dès lors qu'une collecte de données sort du cadre des finalités originellement poursuivies, l'autre texte doit s'appliquer. Il faut entendre par là que dès lors qu'une personne morale va exploiter des données à des fins pénales, le RGPD ne sera plus approprié ou du moins prévoira des sanctions, inversement si les services de police utilisent les données contenues dans leurs fichiers à d'autres fins que des fins pénales ou anticriminelles, le RGPD devra s'appliquer.

Néanmoins en pratique la subtilité semble aller plus loin, en ce qu'il est parfois difficile de concilier sûreté de l'État, lutte contre la criminalité, prévention des infractions, avec le respect de certains droits fondamentaux. En effet le dernier exemple en date illustrant si bien la nécessité de proportionnalité entre l'atteinte et l'objectif poursuivi, reste celui de la double abrogation successive par le Conseil constitutionnel du délit de consultation habituelle de sites internet terroristes[73]. Bien que l'objectif soit la prévention et l'anticipation, voire la lutte contre l'endoctrinement terroriste, l'atteinte à certains droits et libertés n'était pas justifiée par la surveillance accrue d'une simple consultation.

Bien que la question de la protection des données personnelles n'ait pas été réellement abordée par le Conseil constitutionnel dans cette décision, la problématique du *Big Data surveillance* pourrait ressortir ici. Pris dans un contexte de protection des données, l'interprétation du Conseil constitutionnel traduit en effet une disproportion entre la finalité pénale – telle que décrite dans le texte européen – et l'atteinte portée aux libertés de l'individu – la protection de ses données et flux de données. Le titre même de la directive détermine cette seule finalité qui doit être poursuivie de « *prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales* ». Aux autorités compétentes et traitantes des données d'évaluer la proportion d'activités de traitement pour atteindre cette finalité.

[73] Cons. constit. décision n°2016-611 QPC du 10 février 2017 et n°2017-682 QPC du 15 décembre 2017

II. Les droits de la personne

Les droits de la personne concernée par le traitement des données dans le cadre du travail policier fait là aussi face à un équilibre délicat entre l'obligation de participation de l'individu à la recherche de la vérité et de coopération à la prévention d'infractions avec la protection de ses données à caractère personnel. Le rôle dans l'exercice du droit à la protection des données par cette personne s'illustre entre la transmission des informations aux services d'enquête et de police et le droit à la modification et à l'effacement de ces données des fichiers. Fichiers qui ont en effet une connotation, catégorisant parfois les personnes.

62. Obligation de coopération - Les victimes, suspects et témoins, lors d'une enquête, sont tenus de participer à celle-ci en apportant les informations demandées par les officiers de police judiciaire par exemple. Le principe pour les personnes touchant de près ou de loin à cette enquête est qu'elles doivent participer à la recherche de la vérité, du moins elles ne doivent pas y faire obstacle. Car en effet, le Code pénal punit principalement le fait d'omettre intentionnellement la communication de certaines informations ; notamment lorsque celles-ci peuvent permettre de démontrer l'innocence d'une personne. Au même titre, est réprimé le fait de refuser de donner des informations à propos de l'auteur potentiel si on en a connaissance, tout autant que le fait de donner un témoignage mensonger.

Dès lors, dans le cadre de la protection des données personnelles, se pose la question de l'obligation de communication de toutes données aux services de police. Il est évident que de manière générale, des informations telles que l'identité ou l'adresse, tant que celles-ci sont utilisées aux fins communiquées à l'individu, ne peuvent être refusées. Néanmoins, la jurisprudence a récemment revu ces obligations au regard des dernières exigences et condamnations européennes. En effet, dans un arrêt de décembre 2017, le Tribunal correctionnel de Grenoble a relaxé une prévenue du chef de refus de prélèvement génétique, prélèvement qui devait être à termes conservé dans le FNAEG[74]. C'est en outre au vu d'une condamnation de la France par la CEDH que le juge pénal a rendu un tel arrêt, concernant justement la durée de conservation et le droit d'effacement[75].

[74] TGI Grenoble, 3 octobre 2017, n°2204/17CJ
[75] CEDH, *Aycaguer c. France*, 22 juin 2017, n°8806/12

63. Droit à l'effacement - Le droit à l'effacement représente et conditionne en quelque sorte le droit de regard des individus sur le traitement de leurs données personnelles par les services de police ou de renseignements. Au-delà même du droit à la sécurité des données assuré par le service traitant, la personne peut elle-même exercer une action sur leur conservation. Droit très souvent appelé « droit à l'oubli » dans le cadre marchand et commercial, le droit à l'effacement peut s'exercer à l'égard des fichiers de police. L'article 16 de la directive 2016/680 en dispose : tout État se doit de prévoir dans la loi la possibilité aux individus concernés de demander un effacement de leurs données des fichiers de police, des fichiers à finalité ou caractère pénal. Elles peuvent de même contester l'exactitude des données et demander leur rectification.

Ainsi pour chaque fichier précédemment cité, la loi prévoit un droit de demande d'effacement pour la personne dont les données sont concernées. C'est notamment sur ce point que la France s'est vue rappelée à l'ordre à plusieurs reprises par les juges européens, ces derniers jugeant que la durée de conservation des données dans certains fichiers était trop importante ou encore que le droit à l'effacement était injustement fermé à certaines catégories d'individus. C'est à ce titre que le Conseil constitutionnel a rendu sa décision de censure à propos du FNAEG[76].

Aussi, dans l'hypothèse d'un algorithme prédictif, si celui-ci était lié en permanence avec les autres fichiers, utilisant donc leurs données à des fins de détection et d'anticipation de la criminalité, cela signifierait que ces données pourraient être utilisées constamment, en permanence. Le droit d'effacement se devrait d'être d'autant plus renforcé que les finalités d'utilisation des données dans le cadre pénal pourraient être élargies et de plus en plus floues, voire incertaines. La pression mondiale faite sur les réseaux sociaux et entreprises pour accroitre la protection des données personnelles pourrait, dans l'hypothèse de l'insertion de l'intelligence artificielle dans le cadre policier, influencer les normes de protection des données en ce sens et exiger de plus en plus d'encadrements.

64. Données sensibles - Enfin, la nature du droit à l'effacement a encore plus de sens dans le cadre de la collecte de données dites sensibles. Ces données bénéficient d'une protection plus accrue, du fait que leur traitement présenterait un risque plus élevé pour

[76] Cf *supra* n°43

les droits et libertés des personnes les concernant. Le risque principal dans l'utilisation de ces données spécifiques est notamment la discrimination. Ces données se rapportent par exemple à l'appartenance religieuse, l'origine ethnique, les opinions individuelles …

La directive relative à la matière pénale mentionne d'ailleurs les données qui « *révèlent l'origine raciale, ethnique* »[77] comme étant des données particulièrement sensibles en ce que leur traitement policier peut engendrer des conséquences préjudiciables aux droits et libertés de la personne. Le principe serait même, selon le législateur européen, que de telles données soient exclues du traitement, à l'exception du consentement expresse à leur utilisation, ou à moins que le traitement « *ne s'accompagne de garanties appropriées pour les droits et libertés de la personne concernée fixées par la loi et ne soit autorisé dans des cas autorisés par la loi* » ou « *qu'il ne soit nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne* » ou « *qu'il ne porte sur des données manifestement rendues publiques par la personne concernée* »[78]. En d'autres termes, à moins que la communication de ces informations ne soit délibérée ou qu'elles ne permettent la manifestation de la vérité, notamment à des fins de protection de l'ordre public, ce type de données ne peut être soumis au traitement.

Les textes prévoient non seulement des obligations dans le traitement des données personnelles, mais renforcent aussi la protection des garanties de la personne en lui attribuant des droits de regard sur la collecte de ses données par la police. Or, bien que ces protections soient les bienvenues, elles sont de plus en plus menacées par les nouveaux enjeux du Big Data.

B. La mise en jeu des principes de protection par le Big Data

Là où l'utilisation du Big Data par les personnes morales privées sert à faire ressortir les préférences et centres d'intérêts des clients potentiels, le travail policier tend dans une certaine mesure à faire de même : collecter des indices, afin d'orienter l'enquête de plus en plus précisément vers des éléments suspects chez une personne. « *Les outils du Big Data sont des outils de surveillance, et le maintien de l'ordre public compte sur cette*

[77] *Op. cit*. note 18, §(37) du RGPD
[78] *Ibid.*

surveillance pour résoudre et prévenir le crime »[79], ce qui implique que le Big Data ne s'élargit non pas seulement de manière générale, mais s'élargit entre les différentes sphères de traitement. Le Big Data formé par les pratiques consommatrices et commerciales pourraient-il se confondre avec le Big Data servant au maintien de l'ordre ? Il est en effet difficile de concevoir une coopération entre ceux qui créent le Big Data – le secteur privé – et les services de police et de renseignements. Coopération qui s'avère cependant de plus en plus nécessaire.

65. Nouvelles technologies - Le Big Data est directement relié à son corollaire de l'utilisation des nouvelles technologies. C'est par le truchement des appareils connectés que ces masses de données deviennent le Big Data et que les informations sont collectées. C'est par la multiplication des plateformes de communication et d'échanges que les individus voient leurs données collectées et utilisées.

Les pratiques policières fonctionnent sur la base de la collecte d'informations auprès des personnes concernées par l'enquête, et ce originellement à l'initiative des officiers ou enquêteurs : la recherche de la vérité se fait par l'investigation, l'amassement des indices et la déduction. Néanmoins, les nouveaux enjeux que présente le Big Data font que les personnes livrent elles-mêmes des données qui peuvent être collectées postérieurement ; se pose dès lors la question de l'utilisation des informations collectées dans le secteur privé par les autorités publiques. Andrew Guthrie Ferguson relève à juste titre que les informations contenues dans le Big Data influencent indirectement qui l'on va surveiller et prendre comme cible. Le processus d'enquête ou de prévention dans le contexte pénal se voit de ce fait inversé : on passerait de la déduction basée sur des faits existants, à la supposition et l'induction via les seules pratiques et informations données « inconsciemment », captées et collectées par ces nouveaux appareils.

66. Géolocalisation - L'exemple type semble être celui de la géolocalisation sur les smartphones, qui se fait désormais plus automatiquement que par choix de l'utilisateur. Le smartphone, même en veille, fonctionne en permanence pour la plupart des individus en possédant ; dès lors qu'une borne ou un réseau Internet est à proximité, l'appareil va automatiquement s'y connecter et déclencher un signal captable. Lorsqu'il qu'il est émis, la géolocalisation s'avère particulièrement aisée – celle-ci étant souvent

[79] « *The tools of big data are the tools of surveillance, and law enforcement relies on surveillance to solve and prevent crime* » in A. GUTHRIE FERGUSON, « The Rise of Big Data Policing », *New York University Press*, 2017

activée inconsciemment par les utilisateurs lors du téléchargement d'applications ou de l'utilisation d'un GPS par exemple. Une telle rapidité de géolocalisation représente un atout majeur pour les services d'enquête – il n'est désormais plus nécessaire de placer une balise sur un véhicule par exemple. Évidemment, toute géolocalisation à des fins pénales ne peut se faire de manière « automatique », l'accord du juge doit être délivré au même titre que pour les écoutes et le bornage des appels téléphoniques par exemple. L'ancienne Garde des Sceaux Christiane Taubira, dans le cadre du débat sur la loi relative à la géolocalisation, faisait d'ailleurs le constat des chiffres suivants : « *Pour ce qui est de la géolocalisation par terminal téléphonique, nous sommes passés de 1 000 à 3 000 réquisitions en 2009 à 20 000 réquisitions en 2013* »[80]. L'évolution des techniques de surveillance et de police s'avère de ce fait proportionnelle au développement technologique des interfaces virtuelles et électroniques. La CEDH a d'ailleurs réitéré sa jurisprudence en matière de géolocalisation policière, qu'elle considère être une atteinte au respect à la vie privée au sens de l'article 8[81].

67. « Vie virtuelle » - Cette multiplication des sources de données relatives aux individus s'illustre non seulement dans le développement des nouvelles technologies mais aussi dans l'utilisation des réseaux sociaux, le développement d'une « vie virtuelle ». Les plateformes telles que Twitter ou Facebook sont fondées sur l'idée même du partage d'informations – dont on a pu néanmoins voir les limites très récemment avec l'affaire *Cambridge Analytica*. Non seulement l'utilisation régulière de ces interfaces virtuelles donne des informations sur les modes de vie, opinions, centre d'intérêts et interactions des individus, mais elle peut aussi se matérialiser dans la localisation et les lieux fréquentés. Leonard Scott, ancien chef de la police de la ville de Corpus Christi, au Texas, considère que les données extraites des médias et réseaux sociaux vont fondamentalement altérer les méthodes de patrouille aux États-Unis, en ce qu'au lieu de se rendre sur le lieu d'un fait avéré et constaté, les policiers pourraient anticiper des évènements grâce aux informations tirées de ces réseaux, et établir un périmètre plus ou moins large de patrouille mais néanmoins ciblant une certaine probabilité[82].

[80] Compte rendu de la deuxième séance du 11 février 2014, J.O. Débats Assemblée Nationale
[81] CEDH, *Ben Faiza c. France*, 8 février 2018,
[82] B. HEATON, « Behavioral Data and the Future of Predictive Policing », Government Technology, disponible électroniquement : http://www.govtech.com/Behavioral-Data-and-the-Future-of-Predictive-Policing.html

Les informations ressortant de cette vie virtuelle pourraient en outre aider substantiellement les services d'enquête à établir des portraits robots ou, comme mentionné précédemment, des profils types afin d'évaluer les tendances comportementales des individus. Bien que certaines formations policières intègrent ces réseaux sociaux et traquent elles-mêmes via ces plateformes certaines personnes « suspectes », un tel travail ne peut se généraliser – pour des raisons tant d'effectif, qu'économiques ou d'efficacité. Le partage qui s'effectue sur ces plateformes va se voir d'autant plus réduit – dans une moindre mesure cependant – que les scandales relatifs à la collecte de données et les législations de protection se multiplient. Ce qui, à termes, va effectivement fermer certaines portes d'accès à ces données, au profit du respect des droits et libertés des individus mais parfois au détriment du travail policier.

La solution serait probablement d'encadrer la saisie de comptes informatiques, tels que les comptes Facebook, au même titre que se fait actuellement la saisine du matériel informatique et téléphonique dans le cadre d'enquêtes. Néanmoins ces réseaux sociaux contiennent une telle quantité de données diverses qu'à moins de contrôler le type d'information à collecter, l'atteinte ne pourrait qu'être trop grande aux droits de la personne et à son intimité. Bien que de manière générale, l'exigence de finalité soit respectée dans le cadre pénal – souvent l'enquête ou la prévention – elle ne peut qu'être renforcée en ce que les sources et accès aux données grandissent de manière exponentielle.

68. Secteur privé et autorités judiciaires - Le fait que le Big Data enfle de plus en plus rapidement implique aussi la question du partage des données entre institutions et autorités. En effet les contours du droit d'accès à tel ou tel fichier catégorisant pénalement les individus peuvent paraître de plus en plus flous en ce que la politique pénale évolue elle aussi avec les moyens techniques mis à disposition. Mais la plus grande question de la circulation des données dans le cadre national reste celle de la relation entre les autorités pénales et le secteur privé.

En effet en 2016, suite à une fusillade à San Bernardino revendiquée par Daech, le FBI souhaitait accéder au contenu de l'iPhone, téléphone de la marque Apple, de l'auteur de la tuerie. Les dirigeants de la marque de téléphone ont cependant opposé aux autorités américaines l'inexistence d'une telle « *porte dérobée* », qui si elle venait à exister menacerait grandement la protection des données des utilisateurs. Débats qui ont donc soulevé la question de savoir dans quelle mesure les entreprises privées pouvaient refuser,

ou autoriser, l'accès aux données personnelles de leurs clients aux autorités pénales poursuivant un objectif d'enquête ou de prévention de la criminalité. En France, le refus de transmettre des éléments à une réquisition judiciaire constitue une infraction pénale, sous la forme d'une contravention de deuxième classe.

Les évolutions dans ce secteur sont en fait à venir et à étudier, afin d'arriver à une bonne coopération entre le secteur privé et les autorités de police ou de gendarmerie. L'Institut national des hautes études de la sécurité et de la Justice a émis dans un rapport de 2016 des hypothèses et propositions de coopérations dans ce cadre-là. L'idée centrale serait en fait que cette entraide reflète un « *caractère gagnant-gagnant* »[83] entre les deux parties. Le rapport donne l'exemple de l'entreprise Renault qui a pu en 2012 établir un accord avec la gendarmerie nationale dans le cadre de la lutte contre les vols de voiture : la gendarmerie a accès à certaines bases de données de l'entreprise, et celle-ci « *construit une base de connaissance actualisée des techniques de vols de véhicule telles qu'observées par la police* »[84]. Une autre proposition porte sur l'élargissement à d'autres domaines de l'entente qui existe déjà entre la police et les opérateurs téléphoniques : lorsqu'une réquisition leur est présentée dans le cadre de l'enquête, chaque partie possède ses propres interlocuteurs spécialisés dans cette communication des données.

Des efforts d'encadrement sont encore à prévoir afin de faire face à plusieurs enjeux qu'impose le Big Data, qui grandit lui-même de plus en plus. En Europe, la protection des données personnelles, et même dans le cadre pénal, est cependant accrue et l'une des plus solides dans le monde. Protection qui cependant, n'est pas encore totalement assurée aux États-Unis par exemple, ce qui en fait le théâtre de scandales à répétition. L'État américain est en effet un exemple pertinent des biais que peuvent engendrer une mauvaise protection des données et une négligence vis-à-vis des enjeux du Big Data.

§2 : Les États-Unis, théâtre des scandales du Big Data

La différence de régime juridique et de système judiciaire est fondamentale entre les États-Unis et la France, voire l'ensemble des États membres de l'Union. L'État

[83] Institut National des hautes études de la sécurité et de la Justice, « Vers une police 3.0 : enjeux et perspectives à l'horizon 2025 », 27ème session nationale « Sécurité et Justice », Groupe de diagnostic stratégique (GDS) n°3, 2015-2016, p.21
[84] *Ibid.*

américain possède bien des principes fondamentaux protégeant les droits primaires de l'individus, dont le droit à la vie privée n'est pas aussi évident qu'en France par exemple (A). La protection des données personnelles des citoyens américains est donc partiellement acquise, d'autant plus que les différents États et le niveau fédéral ne sont parfois pas en phase sur cette protection (B).

A. Les principes fondamentaux américains de protection des données

69. *Bill of Rights* - L'entrée en vigueur du RGPD en Europe en cette année 2018 met les États de l'UE au cœur des débats portant sur le Big Data dans le monde. Les États-Unis portent d'ailleurs une attention particulière à ce texte, et ce d'autant plus depuis le scandale engendré par l'affaire *Cambridge Analytica/Facebook*. Faisant partie du système du Common Law, leur droit est principalement fondé sur le système du *precedent*, selon lequel les décisions de justice sont la base des règles juridiques du pays. Les textes suivent éventuellement ensuite, ayant en général une valeur inférieure à la jurisprudence – bien qu'un concept tel que la hiérarchie des normes ne soit pas aussi strictement appliqué dans les États de Common Law qu'en France. La jurisprudence est donc dans ces pays-là une réelle source de droit. Les États-Unis possèdent cependant des textes à valeur équivalente à celle de notre Constitution de 1958, comme notamment le *Bill of Rights* de 1789, qui ne sont autres que les dix premiers amendements de la Constitution américaine. Cette dernière est ainsi introduite par dix articles énonçant des droits et libertés propres aux individus, auxquels il ne peut être dérogé.

Dès lors, la question se pose de savoir si le droit à la vie privée est contenu dans ce *Bill of Rights* ou du moins comment un tel droit est protégé. Car effectivement, ce droit au respect à la vie privée est le droit individuel qui fonde le mieux le droit à la protection des données personnelles. Au même titre qu'en droit français, le droit à la protection des données n'est en effet pas constitutionnellement prévu – pour des raisons évidentes d'époques durant lesquelles ces textes ont été rédigés. Ainsi plusieurs articles du *Bill of Rights* sont régulièrement reliés à la protection de la vie privée et donc à la protection des données.

70. Quatrième amendement - Le Quatrième Amendement de la Constitution américaine dispose pour la protection des individus contre les recherches, fouilles, saisies

abusives ou injustifiées par la police, à moins d'une « cause probable »[85]. Ces derniers termes sont un des principes directeurs du processus pénal et du travail policier aux États-Unis. Ce quatrième amendement peut se traduire ainsi : « *ne pourra être violé le droit des citoyens à la sécurité personnelle, de leur logement, de leurs papiers et documents, contre les perquisitions et saisies abusives ; aucun mandat de perquisition ne pourra être délivré s'il n'est pas fondé sur une cause probable, sur des affirmations sous serment, et si le lieu, la personne et les biens objets de la perquisition ne sont pas décrits précisément* »[86].

Cet amendement est donc relatif au droit au respect de la vie privée de la personne et la protège de toute atteinte disproportionnée ou abusive à ses biens et effets de la part d'une autorité publique ou étatique, et surtout de la part de l'autorité pénale. La constitution mentionne ici toute perquisition ou saisie déraisonnable ; dans un contexte contemporain, une telle perquisition se fait dans la majorité des cas par une autorité judiciaire ou de police. On peut donc y voir une garantie de la protection de la vie privée, néanmoins l'interprétation de cet article reste controversée, car il est surtout question d'une atteinte à la propriété plus que d'une atteinte à l'intimité dans son sens large.

71. Interprétation du Quatrième Amendement - Néanmoins d'autres articles du *Bill of Rights* ont été mis en perspective avec le Quatrième Amendement, permettant son interprétation large. C'est notamment l'article 9, qui dispose que la Constitution doit, justement, pouvoir être interprétée largement dans certains cas, afin qu'aucun droit ne puisse être restreint ou nié aux personnes. Ainsi, si le caractère protecteur du respect de la vie privée du Quatrième Amendement n'est pas tout à fait clair, il convient de l'interpréter comme tel à la lumière de l'article 9 afin de ne pas priver les citoyens de ce droit. Dans la même logique, le Quatorzième Amendement dispose qu'aucun État ne doit priver ses citoyens de la vie, de la liberté ou de la propriété sans un procès équitable[87]. Cet alinéa de l'article 14 est communément appelé « clause liberté »[88], clause qui a été interprétée largement par la *Supreme Court* à plusieurs reprises comme garantissant un droit à la vie privée[89].

[85] *Probable cause*
[86] Traduction du *Fouth Amendment to the United States Constitution* : « *The right to the people to be secure in their persons, houses, papers and effect, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized* ».
[87] « *Due process of law* » peut se traduire par procès équitable ou procédure légale régulière
[88] *Liberty clause*
[89] *Meyer v. Nebraska*, 262 U.S. 390 (1923)

Le droit au respect de la vie privée n'est donc à l'origine pas expressément garanti par la Constitution américaine, néanmoins l'article 4 du *Bill of Rights* protège les personnes contre toute perquisition, recherche ou saisie abusive de leurs biens. Article qui peut être interprété comme protégeant aussi la personne contre toute intrusion injustifiée et déraisonnable dans sa vie privée, et ce au regard de l'article 9 par exemple. Dès lors, la question se pose de savoir si cette interprétation a été ou pourrait être élargie à la protection des données à caractère personnel, comme il a été fait en Europe.

72. *Patriot Act* - Au lendemain du 11 septembre 2001, les États-Unis ont renforcé leurs politiques de lutte contre le terrorisme, au prix de certaines libertés individuelles. Nombreuses ont été les révélations quant à la collecte et la surveillance des données personnelles des citoyens par la NSA, la CIA et d'autres agences de renseignements de l'État américain. A l'aire du Big Data, la problématique de la protection des données des citoyens américains est d'autant plus exacerbée qu'il n'existe pas de réelle base constitutionnelle ou textuelle pour la protection de ces données. La seule protection potentielle émanant de l'article 4 de la Constitution américaine s'est vue rapidement chassée lors du vote du *Patriot Act* à peine plus d'un mois après les attentats de New-York. Ce texte a autorisé un grand nombre de possibilités d'immixtion des autorités dans la vie privée des citoyens, leur domicile, l'écoute de conversations téléphoniques, le suivi d'emails … et contient notamment une section 215 relative aux pouvoirs accordés à la NSA et au FBI. Cette section permettait ce qui était appelé la « *bulk collection* », la « collecte en gros », de données diverses relatives aux personnes, et ce sans leur autorisation ni même qu'elles soient au courant. En outre, le texte n'exigeait même pas la preuve d'un doute ou d'un soupçon suffisant quant à la participation de la personne à une activité illégale. En d'autres termes, une telle section du *Patriot Act* permettait la surveillance et la collecte des données de n'importe qui.

Bien que modifié et partiellement renouvelé, le *Patriot Act* a subsisté en grande partie jusqu'en 2015, date à laquelle il a expiré. Certaines de ses dispositions ont été renouvelées, néanmoins la section 215 a été supprimée : désormais, la NSA, pour obtenir un suivi téléphonique ou une saisie de données électroniques, doit s'adresser aux compagnies de communications afférentes, et ce avec l'autorisation préalable d'un juge fédéral, qui lui octroiera un mandat. On voit là encore la différence du système américain de Common Law, plutôt basé sur la réaction *a posteriori*, avec le système français et plus largement européen, qui agit légalement en amont. Ce propos s'illustre notamment par le

récent scandale *Cambridge-Analytica* : les problèmes posés par cette affaire sont presque dans leur ensemble déjà traités par le RGPD, finalisé en 2016. Les autorités américaines, elles, n'ont plus qu'à agir afin que de telles atteintes ne se reproduisent plus. Il serait néanmoins nécessaire de rattacher les données du Big Data, données « modernes », à la vie privée dans son ensemble, de manière constitutionnelle. Par contraste avec le système européen, la protection de la vie privée a une valeur de protection de la dignité, là où elle a plus une valeur de liberté au sens de la philosophie juridique américaine[90].

Le fossé juridique existant entre l'Europe et les États-Unis en matière de protection des données se creuse d'autant plus que le système fédéral de l'État américain implique des encadrements disparates au sein même du territoire, entre États et institutions fédérales.

B. Des protections fédérales et étatiques disparates

L'encadrement légal au niveau fédéral est donc relativement léger quant à la protection des données personnelles aux États-Unis. Lacune textuelle qui est cependant paradoxale quand on voit qu'à l'inverse, l'État américain peut en très peu de temps publier un texte qui met à mal toute vie privée – à l'image du *Patriot Act*. Certains efforts ont été faits par le gouvernement américain, cependant ce sont majoritairement les États eux-mêmes, de manière indépendante, qui essaient de protéger les données de leurs citoyens. Un texte général serait néanmoins nécessaire au niveau national, notamment pour encadrer les pratiques policières. En effet, à la différence du système français par exemple, la police aux États-Unis est seule directrice de l'enquête, le système judiciaire américain ne disposant pas de l'équivalent d'un juge d'instruction ou d'un Procureur général dans de telles circonstances. On peut donc imaginer que l'encadrement du Big Data policier et de son traitement à des fins de police prédictive pourraient causer des atteintes aux intérêts individuels.

L'encadrement de la protection de la vie privée aux États-Unis se construit donc comme un « *puzzle* »[91], à travers différents textes et jurisprudences relatifs à différents secteurs :

[90] G. ZANFIR, « EU and US Data Protection Reforms. A comparative View », The 7th Edition of the International Conference, *European Integration Realities and Perspectives*, 2012
[91] *Ibid.*

télécommunications, secteur bancaire, vidéosurveillance, domaine de la santé … Ainsi, concomitamment à l'audition du PDG de Facebook Mark Zuckerberg devant le Congrès américain, des sénateurs ont proposé un texte législatif d'encadrement du traitement des données personnelles par les personnes et entités privées. Se pose cependant toujours la question de la protection de ces données dans un cadre pénal et policier aux États-Unis. Le gouvernement américain et sa police de manière générale fait largement primer la protection de l'ordre public sur ce droit à la protection des données à caractère personnel sur le territoire.

73. Traitement automatisé. Après les attentats du 11 septembre, le *National Criminal Intelligence Sharing Plan*[92] fut mis en place par différents acteurs du secteur policier américain, notamment en réponse au *Patriot Act*. Une recommandation a été faite de prendre en compte le respect de la vie privée des individus dans le développement de logiciels et systèmes d'intelligence artificielle, et ce au titre du Code fédéral des régulations[93]. En outre, dès 2005, le département de Justice avait publié des recommandations quant au traitement automatisé des données dans un cadre policier[94]. Ces recommandations concernaient par exemple la nécessité d'avoir une raison pénale et justifiée de collecter les données, d'avoir des soupçons raisonnables[95], de s'assurer de la validité des données, de renouveler et modifier, voire effacer ces données tous les cinq ans, de l'encadrement des personnes ayant accès à ces systèmes, et surtout la nécessité que ces traitements ne portent pas atteinte à la vie privée des personnes.

Mais le principe du *precedent* reste encré dans le système de Common Law, la jurisprudence a une valeur supérieure. Concernant le concept de soupçons raisonnables, en 2000, la Cour Suprême américaine avait permis d'élargir ce concept indispensable aux actions policières, ce faisceau d'indices, lorsque les investigations portent sur des zones géographiques qualifiées comme à taux criminogène élevé[96]. Depuis, la jurisprudence reste la même, et la loi sur la protection de la vie privée n'évolue pas vraiment.

[92] U.S. Department of Justice, « The National Criminal Intelligence Sharing Plan », Washington, D.C., October 2003
[93] Titre 28, part 23 du « Code of Federal Regulations »
[94] M.PETERSON, « Intelligence-Led Policing Report », Department of Justice, 2005
[95] « *Reasonable suspicion* » est un principe directeur du droit pénal, censé diriger toute procédure policière ou d'enquête
[96] *Illinois v. Wardlow*, 528 U.S. 119, 124 (2000), Supreme Court

74. Diversité des encadrements - Nombreuses ont pourtant été les tentatives. La protection des données personnelles trouvant généralement son origine dans l'encadrement du secteur privé et commercial, c'est ce dernier qui devrait au moins commencer par faire l'objet d'une loi ; viendrait ensuite celle sur la protection des données dans le cadre pénal. Les textes disparates évoquent de manières indépendantes une protection des données, ou un droit d'être informé d'une fuite … sans s'entendre sur une mise en commun. Le gouvernement de Barack Obama a tenté une telle approche avec la proposition de création du *Consumer Privacy Bill of Rights*, un *Bill of Rights* posant les droits fondamentaux de protection des données des consommateurs. Mais ce texte n'a pas vu le jour. Plus récemment, le sénateur Patrick Leahy, accompagné de six confrères, a introduit au Congrès le *Consumer Privacy Protection Act*, en novembre 2017. Reste à voir si les derniers scandales et fuites de données vont accélérer le processus d'adoption.

Un rapport de la RAND Corporation sur la police prédictive énumère en outre des principes considérés comme acquis dans l'arsenal juridique américain, notamment à travers la mise en œuvre de textes relatifs à la santé, au domaine économique mais aussi à la circulation des données[97]. Des principes comme ceux de la finalité, de la qualité du data, de la transparence sont donc entendus comme s'appliquant de manière générale dans les différents États nord-américains. Les États ont ensuite, seuls, développé l'application de ces principes dans leurs propres lois afin de protéger leurs citoyens respectifs. L'État de Californie a notamment un grand nombre de textes relatifs à la protection des données, qui étendent et interprètent largement certains textes fédéraux. Mais là encore, l'encadrement de la collecte des données dans un cadre policier pèche.

La protection des données à caractère personnel dans un cadre policier manque donc cruellement d'encadrement aux États-Unis. Les autorités de police doivent certes s'adresser à un juge fédéral afin d'obtenir des informations détenues par une personne morale privée, néanmoins au vu de l'expérimentation croissante qui se fait de la police prédictive dans ce pays, il serait nécessaire de se pencher sur l'éventualité d'un texte national. En effet, la preuve a bien été apportée que les données personnelles peuvent être déviées du but pour lequel elles ont été originairement transmises ; personne n'est donc à l'abri d'une mauvaise utilisation de ces informations dans le cadre policier. Un exemple

[97] W.L. PERRY et al., « Predictive Policing: the Role of Crime Forecasting in Law enforcement Operations », RAND Corporation, 2017, p.87 : principes établis par le *U.S. Department of Health, Education and Welfare* en 1973, *Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy*, *Transborder Flows of Personal Data* de 1980

extrêmement liberticide et discriminatoire a déjà eu lieu dans l'une des villes expérimentant une IA prédictive, démontrant à juste titre que certaines données n'ont pas lieu d'être détenues et traitées par les autorités pénales et judiciaires[98].

[98] Cf *infra* n°106

Chapitre II
La police prédictive : le nouveau traitement du Big Data dans la lutte contre la criminalité

Les différents États, européens mais aussi américains, ont bien conscience de l'expansion de cette masse de données et des enjeux qu'elle présente tant pour les citoyens que pour les autorités répressives. Il faut rappeler que le Big Data est un corollaire de l'utilisation de l'intelligence artificielle : l'un est l'essence de l'autre, ils ne peuvent réellement exister séparément. Le secteur privé a su tirer profit de cette évolution technique et des capacités de l'intelligence artificielle. Est donc très vite apparue l'interrogation suivante : pourquoi ne pas l'utiliser à des fins de sécurité publique ? Comment l'intelligence artificielle pourrait améliorer le travail policier ? C'est là qu'intervient la police prédictive (Section 1). Les algorithmes font, voire ont fait, leur place dans les commissariats, afin de servir les acteurs de l'enquête et de la prévention. Il ne faut cependant pas que les autorités répressives se laissent aveugler par l'engouement qui existe autour de cette idée faussement lisse de l'intelligence artificielle policière (Section II).

Section 1 : L'intelligence artificielle au service du travail policier

Les villes américaines, et notamment Los Angeles et New York, ont testé les premières ces techniques de logiciel prédictif. Développés en partenariats avec des scientifiques, ces algorithmes peuvent prendre plusieurs formes, se basant sur des données et des programmations différentes. Les premières techniques prédictives apparues ont eu vocation à se concentrer sur les facteurs de lieu et de temps du crime (§1), impulsant un deuxième temps dans la prédiction : les techniques de prédiction du comportement criminel à proprement parler (§2).

§1 : Les techniques de prédiction spatiotemporelles

La plupart des techniques de prédiction du lieu du crime se concentrent seulement sur les données de lieu, de temps et de type d'infraction. Un grand nombre de procédés

techniques existent, néanmoins trois ressortent comme les plus courants : la cartographie du crime (A), l'analyse spatiotemporelle (B) et les méthodes de répétition (C).

A. « *Hot spot* » et cartographie du crime

75. *Hot spot* - L'utilisation de l'intelligence artificielle à des fins de prédiction de la criminalité s'illustre majoritairement dans l'étude du phénomène criminel dans l'espace. Sont apparues notamment les techniques de « cartographie du crime » et de *« hot spot »*, autrement dit l'évaluation du risque de perpétration d'actes criminels dans un lieu géographique déterminé. Ces techniques s'illustrent sous forme de cartes légendées, souvent par des couleurs ou des formes variant en fonction du caractère élevé ou bas du risque criminel que présente une certaine région (voir schéma ci-dessous). Par région, il faut entendre quartier, du moins voisinages dans les villes utilisant ce type de procédé.

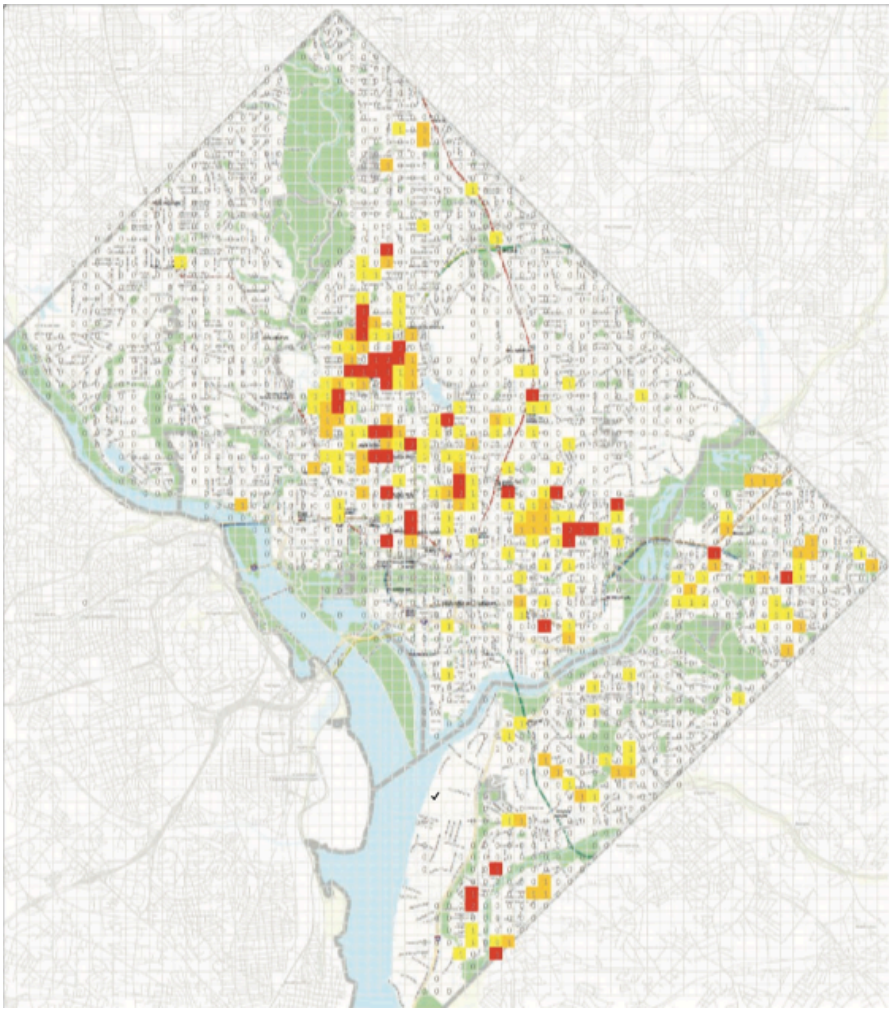

Schéma issu du rapport de la RAND Corporation de 2017 sur la police prédictive (p.21), illustrant les cambriolages dans la ville de Washington D.C. La couleur jaune représente une zone à faible risque, l'orange un risque moyen et le rouge un risque élevé.

76. Données utilisées - La spécificité de ce procédé est qu'il se base sur des données passées, des statistiques criminelles, qui peuvent remonter parfois à plusieurs décennies : ce sont toutes les données de l'histoire du crime d'une zone géographique qui servent de support à l'analyse algorithmique. « *Le passé est prologue* »[99] du phénomène criminel à venir pour ces techniques de cartographie du crime ; les développeurs et les services de police utilisant cet outil mettent en effet à profit le fait que le phénomène criminel ne soit pas, géographiquement parlant, uniformément éparpillé[100]. Les individus ont eux-mêmes conscience de ce caractère non-uniforme, dans la vie de tous les jours, en évitant certaines rues, de passer dans certains voisinages à certaines heures de la journée, et ce de manière légitime ou non ; « *les individus peuvent se tromper à propos du risque que représentent certains lieux, mais ils ne se trompent pas sur le fait que le risque d'être victime d'un crime n'est pas géographiquement constant* »[101].

Cette méthode de prédiction a donné naissance à de nombreux types d'algorithmes, tous ayant des similarités en matière d'objectifs et de données sources, mais aux programmations originelles différentes. En effet, les techniques peuvent aller de la cartographie de la criminalité en générale, à la détermination de la probabilité de commission d'infractions déterminées à certains endroits, ou encore la prédiction de phénomènes criminels sur le long terme. Au-delà même de la pure police prédictive, ces techniques peuvent permettre l'identification de caractéristiques criminelles, sociologiques et comportementales.

En fonction de la technique de programmation utilisée, la cartographie peut se faire par la multiplication de lieux qualifiés à risque (*hot spot*) ou par le groupement de ces risques en un seul point à risque. Dans toutes les hypothèses, l'algorithme va se fonder sur une multiplicité d'éléments indépendants, individuels les uns des autres afin de créer une sorte de « moyenne » géographique. Cela peut permettre aux services de police, par exemple, de déduire des similarités entre certaines infractions et de relier des crimes entre eux, ce qui peut tendre à la recherche d'un seul et même suspect.

77. Étendue de la zone étudiée - L'analyse diffère cependant en fonction de la zone géographique étudiée, en fonction de son étendue. L'analyse et la marche à suivre

[99] « *The past is prologue* », RAND report, *op. cit,* note n°97
[100] *Ibid*.
[101] "*People might be mistaken about the risks of some places, but they are not mistaken that their risk of being a victim of crime is not geographically constant*", J.E. Eck and al., « Mapping Crime: Understanding Hot Spots », U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 2005

faites par l'intelligence artificielle ne seront pas les mêmes pour une seule rue que si la zone étudiée est un quartier entier. Un exemple illustrant parfaitement ce propos serait la différence entre les deux questions suivantes : « *où la drogue est-elle vendue ? Qu'est-ce que le marché de la drogue ?* »[102] (en d'autres termes, qu'est-ce qui a fait qu'un tel marché s'est développé dans telle ville). Ces deux questions, bien que liées, sont effectivement fondamentalement différentes l'une de l'autre. On comprendra dès lors que les données fondant la recherche algorithmique seront bien plus vastes dans le cadre de la deuxième question que dans la première qui implique uniquement la prise en compte de localisations. Bien qu'ayant majoritairement pour but de prédire la criminalité, la qualification de *hot spot* peut aussi être donnée à une zone géographique à fort taux ou fort risque de victimation.

78. PredPol - Le développement de l'utilisation de ces techniques de *crime mapping* par les services de police s'est surtout illustré aux États-Unis, avec le logiciel PredPol. Cet algorithme, inspiré des logiciels de sismologie, tend en effet à identifier les lieux géographiques des villes auxquelles il s'applique qui représentent le plus fort taux de criminalité, et donc les lieux les plus susceptibles d'être frappés par un phénomène criminel dans le futur. La détection algorithmique de *hot spots* faite par l'utilisation de PredPol a dépassé son simple but prédictif, ou du moins l'a complété, en ce qu'elle a fait ressortir des tendances délinquantes qui ne sont à l'origine pas nécessairement propres à l'individu auteur de l'infraction. S'appliquant en grande partie aux cambriolages résidentiels, le logiciel a par exemple fait ressortir qu'un cambriolage commis dans un certain quartier de la ville pouvait en influencer voire en déclencher un ou plusieurs autres dans la même zone, dans un laps de temps proche. Le *crime mapping* a fait ressortir – ou plutôt a renforcé – une théorie criminologique de la « contagion » du crime.

L'algorithme de PredPol n'ayant pour vocation que la prédiction spatiotemporelle, les éléments du Big Data utilisés seront dès lors relatifs à la géolocalisation, les types d'infractions, les heures de commission de celles-ci … L'algorithme reste minimaliste dans l'exploration du Big Data et son exploitation. Néanmoins ses utilisateurs se félicitant des résultats obtenus, l'ambition de ce logiciel pourrait être revue à la hausse et de ce fait demander un plus grand nombre de données.

[102] *Ibid*, "*Where are drugs being sold? What is the market for drugs?*"

B. Les analyses spatiotemporelles et de terrain

Le « *risk terrain modeling* »[103] et l'analyse spatiotemporelle du crime sont deux méthodes algorithmiques de police prédictive distinctes l'une de l'autre ; elles ont cependant des similarités en ce qu'elles s'inspirent de l'environnement géographique ou spatiotemporel des phénomènes criminels. Ces programmations tendent en effet à étudier les influences extérieures et environnementales sur le crime ; influences autres que sociologiques ou propres au délinquant. Fonctionnant dans la même optique que le *crime mapping*, l'analyse faite par l'IA se fait essentiellement sur des infractions telles que les cambriolages, les vols domestiques ou de voiture … dont les auteurs ne sont que rarement connus. Les données utilisées sont donc à l'origine, dans le cadre de ces procédés, des données de localisation, de temps et de caractéristiques tenant à l'infraction.

79. L'analyse spatiotemporelle – Ce sont ces derniers types de données qui sont particulièrement utilisés dans le cadre de l'analyse spatiotemporelle du crime. Les caractéristiques de l'infraction en jeu dans l'analyse vont permettre à l'IA d'établir des liens entre le crime et son environnement spatiotemporel. Pour ce qui est du facteur temps, l'analyse ne se fera pas uniquement sur l'heure ou le moment précis de la journée de commission de l'acte, mais tend aussi à porter sur une période bien plus vaste. Ainsi l'analyse va aussi porter sur des périodes de l'année voire même sur la saisonnalité du crime. Sur ce dernier élément, les logiciels d'analyse spatiotemporelle ont pu notamment faire ressortir le fait qu'en été, les enfants et adolescents n'étant plus à l'école, il peut y avoir une augmentation du taux d'infractions de faible gravité ou de cambriolages[104].

Néanmoins, une telle déduction ne pourrait-elle pas être faite par l'Homme lui-même ? Il n'est en effet pas nouveau que certaines périodes de l'année sont plus « propices » au crime, ou comme l'avait assez tôt constaté Durkheim, que le taux de suicides a tendance à augmenter en été plutôt qu'en hiver. Cependant l'analyse spatiotemporelle du crime par logiciel va bien plus loin qu'un constat qui pourrait émerger d'une étude sociologique faite par l'Homme. La tâche est en effet confiée à l'IA qui, à termes dans les bureaux de police ayant vocation à s'en servir, serait soumise à l'apprentissage autonome. A ce titre, l'analyse spatiotemporelle et de la saisonnalité du crime pourrait être décuplée, en ce

[103] *Modélisation géographique du risque*
[104] RAND report, *op. cit,* note 97, p.49

qu'elle se fait en temps réelle et par analyse permanente des phénomènes criminels de la ville en question.

80. *Risk terrain modeling* ou analyse géographique du risque criminel - La méthode du *risk terrain analysis* ou *risk terrain modeling* diffère de l'analyse spatiotemporelle en ce qu'elle prend en compte des caractéristiques bien plus spécifiques de la géographie des lieux analysés. Le RAND Report sur la police prédictive[105] prend les exemples des bars présents dans le voisinage, des commerces vendant de l'alcool, des routes particulièrement fréquentées. Le but est qu'ensuite l'algorithme fasse des liens entre le lieu étudié et ces éléments clés pour en déduire un risque plus ou moins élevé de criminalité. Les résultats donnés par le logiciel vont prendre une forme relativement similaire à celle de la cartographie du crime, sous forme de variations de couleurs ou de formes en fonction du risque que représente telle ou telle zone. Néanmoins on voit bien que la démarche à l'origine du résultat obtenu est bien différente de celle des *hot spots*. Dans ce dernier cas, le logiciel est basé sur des données passées uniquement géographiques, dans le cas du *risk terrain modeling*, on a plutôt affaire à un « portrait » de la zone en fonction de différentes caractéristiques propres au voisinage. Ce procédé est en fait une superposition des principes de la technique des *hot spots*, de principes de criminologie de l'environnement socio-économique et de principes d'analyses policières[106].

81. Illustration - La question qui sous-tend l'utilisation des méthodes d'analyse géographique du crime est celle de savoir qu'est-ce qui rend une zone vulnérable au crime, qu'est-ce qui fait que cette zone représente un risque plus certain qu'une autre zone[107]. Le but est en effet non seulement la prédiction mais serait aussi que l'IA détermine à termes les facteurs qui influencent la criminalité dans un secteur. A titre d'exemple, la ville de Colorado a expérimenté cette technique en intégrant notamment dans les facteurs environnementaux de la zone étudiée la présence de blocs de logements collectifs. L'étude portait notamment sur les vols de voiture. En présence d'un tel facteur, les vols s'expliquent par le fait que les logements collectifs ne permettent pas aux familles de garer leur voiture dans une zone visible depuis l'appartement – laissé sans surveillance,

[105] *Ibid*, p.51
[106] J.M. CAPLAN and L. KENNEDY, « Risk Terrain Modeling Compendium for Crime Analysis », Rutgers Center on Public Security, Newark, 2011
[107] A.G. FERGUSON, *op. cit.* note 79, p.67

le véhicule a donc plus de chances d'être volé[108]. Ainsi cet élément caractéristique géographique pourra être retenu comme tel par l'IA, qui enregistrera cette donnée comme « à risque ».

82. Évaluation statistique - Le procédé de *risk terrain analysis* peut aussi se faire de manière statistique. Dans un tel cas de figure, c'est la distance entre l'infraction commise et les facteurs environnementaux pris en compte qui va être calculée (et non pas uniquement l'analyse d'une multiplicité de facteurs). Dans un deuxième temps, l'algorithme va évaluer les similarités géographiques entre les différents points d'infraction et les différents points représentant les facteurs d'influence. En d'autres termes, les points ayant des distances similaires avec des facteurs qui ont été considérés comme influençant des crimes déjà commis, seront considérés comme des lieux à risque.

Un exemple de logiciel expérimentant cette technique algorithmique est celui de *DigitalGlobe's Signature Analyst*, à Washington D.C., qui avait vocation à évaluer les zones géographiques présentant des risques de vols à l'arraché. Une première carte de la ville présentait sous forme de points noirs les lieux où était communément commis ce type d'infraction. Après analyse logicielle, en fonction des facteurs environnementaux entourant ces points noirs, la carte s'est vue colorée du jaune au rouge autour de ces zones – le jaune exprimant un risque faible de vol à l'arraché, le rouge un risque élevé.

C. Les méthodes de « répétition proche » du crime

Là encore, cette méthode n'a pu être expérimentée que dans des commissariats américains et porte donc le nom anglais de « *near-repeat methods* », qui peut se traduire par les méthodes de « répétition proche », ou même méthodes de concomitance des crimes.

83. *Near repeat methods* - Cette démarche part du principe que les crimes à venir sont très proches dans le temps des crimes commis à l'instant T, de crimes actuellement constatés. Elle nécessite donc une statistique relativement actuelle, si ce n'est immédiate ou au jour le jour du taux de criminalité d'une zone ciblée. Cette technique algorithmique

[108] *Ibid*, p.68

est en fait fondée elle aussi – comme les méthodes de cartographie du crime – sur une technique de prédiction sismologique, qui tend à déterminer les points futurs de tremblements de terre en fonction de ceux immédiatement passés.

Les *near repeat methods* se sont avérées efficaces surtout pour les cambriolages domestiques, les autres infractions ne semblant pas présenter de données assez précises dans le temps et dans l'espace pour faire une prédiction si précise de leur immédiateté. Une étude menée aux États-Unis suite aux résultats de l'utilisation de cette technique algorithmique, a montré que 76% de cambrioleurs interrogés avaient tendance à revenir sur les mêmes lieux sur lesquels ils ont commis des infractions de cambriolage jusqu'à ce qu'ils se fassent arrêter[109]. Un constat qui confirme la logique utilisée par cette technique prédictive.

Ainsi par le truchement de la prédiction du crime dans le temps, cette technique permet à termes de faire aussi des prédictions dans l'espace. En analysant la concomitance d'une infraction avec une autre, un tel outil permettrait de déterminer les zones à risques du moins sur le court terme, dans un futur proche de l'ordre du jour ou de la semaine. Ce procédé s'est aussi avéré intéressant en matière de violences par arme à feu entre gangs et groupuscules. Là encore, c'est la nature même de ces infractions qui justifie une potentielle efficacité du procédé ; des tirs initiés par les membres d'un gang vont en général – si ce n'est toujours – engendrer des tirs adverses, et ainsi de suite.

Dès lors, les *near-repeat methods* ne peuvent être efficaces que si les données sont extrêmement précises ; ce qui sous-entend une technique de constatation des évènements en temps réel particulièrement développée. La mise en œuvre à grande échelle de ces techniques de police prédictive sous-entendrait donc une surveillance accrue de certaines zones, une communication parfaite entre les unités de police et une grande réactivité.

La plupart des ambitions prédictives se sont en majeure partie concrétisées jusqu'ici par des logiciels d'analyse de l'espace et du temps. Les données que demandent de telles techniques sont plus facilement récoltables et surtout traitables, ne mettant pas trop en jeu les droit et libertés des citoyens. Néanmoins, la police prédictive a vocation à s'étendre à l'analyse d'autres données, et ce pas uniquement pour la prédiction de la récidive.

[109] S.D. JOHNSON et al., « Space-Time Patterns of Risk: A Cross National Assessment of Residential Burglary Victimization », *J Quant Criminol*, 2007

§2 : Les techniques de prédiction du comportement criminel

Là où les techniques de cartographie du crime font ressortir des zones criminogènes sans se préoccuper des individus, certains souhaiteraient gravir un échelon dans la prédiction et utiliser les données littéralement « personnelles ». Le datamining sert notamment à ça, en ce qu'il explore les données relatives à la personne (A). Là encore, les techniques algorithmiques s'accumulent, certaines inspirées de théories criminologiques comme celle de la dissuasion (B), d'autres suivant le courant de pensée de la police prédictive, comme l'évaluation du risque (C).

A. Le « datamining »

84. Datamining - Au même titre que l'expression de « Big Data », le *datamining* est devenu un terme communément utilisé en matière de traitement algorithmique et de données. Cette exploration ou extraction de données renvoie, en matière d'intelligence artificielle, à l'exploitation du Big Data à certaines fins. Cédric Villani, dans son rapport sur l'intelligence artificielle, parle même de « *fouille de données* »[110].

Ainsi dans un contexte pénal ou policier, le datamining est le premier échelon, du moins le plus général et représentatif, des méthodes de police prédictive. Le datamining représente en fait le traitement des données collectées, sous-entendant donc que l'exploration se fait dans une masse conséquente d'informations. Les procédés de datamining permettent de brasser des données, les sélectionner pour ensuite les utiliser. Tout ceci dans l'optique évidemment que la charge repose sur un mécanisme automatisé, un algorithme : du fait de la masse de données traitée, l'Homme ne pourrait – ici l'agent de police – efficacement extraire autant d'informations.

En effet, nombre de structures algorithmiques de police prédictive sont en fait fondées sur les principes du datamining. Le datamining renvoie à toute méthode qui consiste à « *construire un modèle mathématique pour faire des prédictions en se basant sur des données* [préalablement] *saisies* »[111] - autrement dit, la majorité des méthodes adoptées par les algorithmes prédictifs. Néanmoins dans une optique de prédiction du crime, pour

[110] C. VILLANI, « Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne », Mission parlementaire du 8 septembre 2017 au 8 mars 2018, 2018
[111] « *Building a mathematical model to make predictions based on input data* », RAND report, *op. cit*. note 97, p.34

le travail policier, il semblerait plus logique que les méthodes les plus rapides soient utilisées. Effectivement, certaines méthodes de datamining ne sont non pas moins efficaces mais vont tendre à un traitement plus important et détaillé d'un plus grand nombre de données. Or, l'intégration et la mise en perspective d'encore plus de données peut s'avérer – bien qu'effectuée par une IA – beaucoup plus chronophage, n'étant de ce fait pas nécessairement utile aux services d'enquête et de police. Il est cependant évident que plus de données il y aura à traiter, meilleur le traitement sera et le résultat n'en sera à termes que plus précis. Néanmoins, ces méthodes de datamining demandant un plus grand nombre de données ne sont pas totalement exclues en ce qu'elles peuvent servir aux infractions les plus régulièrement commises. En effet, si l'accent veut être mis sur l'anticipation de cambriolages, ou de vols de rue, il est possible que l'IA centre ses résultats sur une zone géographique au fort taux de cambriolages. En réalité, deux techniques principales de datamining ressortent majoritairement en matière de police prédictive.

85. Le « *clustering* » ou groupement de données - La première technique algorithmique de datamining qui ait pu être imaginée en matière d'IA et de détection du crime est celle du « *clustering* », qui peut se traduire par le groupement ou l'agrégation de données. Cette méthode consiste pour l'algorithme en l'analyse et le regroupement de données, considérées comme similaires, en plusieurs groupes. L'IA, par le biais de la fouille des données, va identifier des similarités entre celles-ci et les regrouper entre elles, faisant donc ressortir une caractéristique commune. Si l'on prend un exemple simple, en matière de cambriolage, le *clustering* s'illustrerait par l'identification d'heures et de zones frappées régulièrement par cette infraction, et permettrait donc de faire ressortir un groupe « cambriolage fréquent dans telle zone à telle période de la journée ». De manière plus poussée, cette méthode de datamining pourrait faire ressortir des caractéristiques comportementales ou des *modus operandi* présents pour une même infraction, permettant ainsi aux autorités de conclure à un seul et même auteur, voire d'anticiper la commission de l'acte.

A titre d'illustration, au Royaume-Uni, un agent de police et un universitaire se sont associés afin de modéliser un algorithme de *clustering* afin de faire ressortir des groupes de spécificités au sein d'infractions sexuelles violentes. Grâce à la mise en place de cet algorithme, les deux hommes ont pu faire ressortir des caractéristiques relatives aux auteurs mêmes de ces infractions, les communiquant aux services de police, qui pouvaient

donc utiliser de telles informations à des fins de prévention et d'enquête, afin de rendre leur travail plus efficace. Cette méthode semble pouvoir permettre de faire ressortir des informations non pas uniquement sur les lieux ou heures d'infractions mais réellement sur les caractéristiques types de la personne délinquante ou de son mode opératoire. Une fois de tels groupes référencés par la police, cette dernière pourrait améliorer l'efficacité de son travail, la rendant plus proactive.

86. La technique de « *classification* » - La deuxième méthode la plus commune dans le datamining est celle de *classification*. Bien que le mot anglais semble plus facilement transposable en français, il faut plutôt comprendre ici la méthode comme une typologie, une nomenclature – termes qui renvoient toujours à l'idée de classification. Cette technique se différencie de la première tout d'abord en ce qu'elle est basée sur l'apprentissage autonome : au vu de données préexistantes, l'algorithme a ici pour but d'apprendre des tendances passées qui vont déterminer des observations et lui permettre de prédire un chiffre, ou un scénario plausible voire possible dans le futur. A l'image de la police prédictive, la méthode de *classification* va donc analyser des données criminelles et pénales passées pour par exemple faire ressortir un taux plus ou moins élevé de risque de cambriolage dans la zone géographique étudiée. En outre, là encore, le datamining fait par l'intelligence artificielle aurait vocation aussi à prédire l'action même d'une personne en particulier. Le rapport RAND donne notamment l'exemple des gangs ou groupes criminels, dont certains membres sortent de prison à des dates rapprochées. La technique de *classification* permettrait d'identifier quel membre serait le plus susceptible de récidiver, d'avoir un comportement violent à la sortie, et ce en fonction des données collectées sur les comportements des précédents membres relâchés[112].

D'un point de vue purement technique cependant, les algorithmes de *classification* se fondent sur une construction et une programmation relativement simple de prise de décision – telle que la méthode de l'arbre. Cette méthode de l'arbre pose un constat – une variable – qui, s'il n'est pas validé, est orienté vers une autre issue possible. Ainsi si l'on reprend l'exemple du cambriolage, les issues proposées pourraient être « haut risque », « risque moyen » ou « risque faible » ; si la variable étudiée ne peut avoir pour résultat « haut risque », alors elle sera réorientée sur « risque moyen », en ainsi de suite[113].

[112] RAND report, *op. cit*. note 97, p.39
[113] *Ibid.*

Nombreuses sont les autres méthodes de datamining, qui pourraient être utilisées à des fins policières. Les méthodes de *clustering* et de *classification* restent néanmoins les plus simples et, pour l'instant, les plus fréquemment mises en œuvre en matière de prédiction du comportement. On remarque que ces méthodes peuvent en effet permettre de prédire ou d'anticiper, du moins identifier, des caractéristiques ou un profil comportemental ; en tout cas d'intégrer le facteur du délinquant en lui-même dans la technique prédictive.

B. Les théories de dissuasion ou « *focused deterrence* »

87. Théorie de la dissuasion ou « *deterrence* » - Plus populaires dans la culture criminologique anglo-saxonne, les théories de « *deterrence* », dites de dissuasion, sont en fait fondées sur l'idée que les délinquants peuvent se voir dissuadés de commettre des infractions du fait du caractère de la punition, du risque punitif et pénal. Les origines de ces théories rejoignent celles de Garry Becker, de l'école criminologique de Chicago du milieu du XIX^{ème} siècle, qui avait une approche économique du crime. Garry Becker, à la suite d'un dilemme personnel, a fait ressortir l'idée selon laquelle les délinquants commettraient des actes délictueux par calcul économique coût-bénéfice. L'individu commettrait donc un acte répréhensible si le coût punitif de celui-ci – en d'autres termes la sanction pénale à la clef – était inférieur au bénéfice pouvant être tiré de la commission de cet acte[114]. Dès lors, la théorie de « *deterrence* » fonde principalement ses idées sur une telle approche, en ce que la menace pénale pèse sur le délinquant. En effet, les premières applications de ces théories ont vu le jour dans les années 1990, en matière de violence par arme par des mineurs.

Ainsi, la théorie de la dissuasion sous-entend que les individus seraient dissuadés de commettre des crimes s'ils avaient la certitude qu'ils vont être punis sévèrement et rapidement pour cet acte[115]. L'idée principale repose sur le fait que plus ces caractères de célérité et de sévérité sont exacerbés, plus la dissuasion sera forte. A contrario, si la sanction prévue pour l'infraction en question est faible et n'a pas de réelle systématicité, l'auteur sera bien moins dissuadé de passer à l'acte. Dès lors un premier constat ressort de cette théorie : on parle bien de sanction et donc de la fin de la chaîne pénale. En effet la sanction peut être prise soit dans son contexte légal, en ce qu'elle est prévue par la loi

[114] G. BECKER, « Crime and Punishment: An Economic Approach », University of Chicago and National Bureau of Economic Research, 1974
[115] M.S. SCOTT, « Focus Deterrence of High-Risk Individuals », Center for Problem-Oriented Policing, 2017, p.4

et le législateur, et ce dans la majorité des systèmes juridiques contemporains ; soit dans son sens de punition, à ce titre c'est là encore dans la majorité des systèmes judiciaires le juge qui est chargé de la décision quant à l'issue du procès. En aucun cas la sanction ne fait partie des attributions et des pouvoirs des services de police ; celle-ci débute en quelque sorte la chaîne pénale et doit justement agir afin que le reste des acteurs de cette chaîne puisse – ou non – à termes juger et punir le suspect.

88. « *Focused deterrence* » - C'est ici qu'entre en jeu la technique de « *focused deterrence* », délicate à traduire en français car peu utilisée ; ce terme peut néanmoins s'entendre comme une technique de dissuasion ciblée. Le but premier est en effet de concentrer l'objectif de dissuasion sur un individu en particulier, du moins de rendre cette technique effective au niveau de la personne et de faire dépasser le simple stade de la théorie. L'objectif est d'envoyer un message dissuasif précis et ciblé à une partie réduite d'une population connue par les services judiciaires et de police comme prenant part à des actes violents[116]. Ce message tend en fait à faire savoir à cette population spécifique que les services répressifs et policiers sont informés des agissements violents, message qui sous-entend donc qu'un contrôle ou une arrestation est prestement encouru.

89. Application à la police prédictive - La question se pose alors de savoir comment une telle technique peut avoir un rapport avec les techniques de police prédictive, du moins comment elle peut avoir un rapport avec l'exploitation du Big Data aux fins d'anticipation de la criminalité. Tout d'abord comme le précise Andrew Guthrie Ferguson, cette technique de *focused deterrence* est principalement utilisée à des fins de réduction de la violence ou des crimes, et peut donc être particulièrement utilisée pour cibler des gangs ou groupes violents. L'utilisation de l'intelligence artificielle se lie donc avec la technique de dissuasion dès lors que le travail policier veut s'orienter vers la baisse d'un phénomène violent : au lieu d'attendre tout comportement suspect en patrouillant dans plusieurs zones différentes, la technique de *focused deterrence* appliquée à un algorithme va permettre de cibler des personnes et des lieux en particulier.

Classiquement, le processus consisterait en l'identification par le logiciel des personnes à cibler, la notification à ces personnes de la connaissance policière de leurs actes et enfin, en cas de passage à l'acte, la punition potentiellement plus sévère de ceux

[116] « *Focused deterrence involves a targeted and explicit message to a narrow slice of the population that police, prosecutors, and the community know who is engaged in violence and that the killings must end* », A.G. FERGUSON, *op. cit.* note 79, p. 35

qui ont effectivement été prévenus. On retrouve ici l'utilisation du Big Data et des données mises à la disposition de la police. Dans un premier temps en effet, au vu des données pénales existantes, des groupes vont être identifiés, ayant un potentiel violent ; les identités des différents membres de ces groupes vont ensuite être comparées avec celles contenues dans les fichiers de police existants, pour finalement croiser les passés pénaux de certains d'entre eux avec d'autres personnes mises en cause, ayant eu des contacts avec les suspects[117].

90. Défauts de la technique - Par le truchement de l'intelligence artificielle, les suspects sont prévenus de la connaissance et du suivi par les services de police et de « l'épée de Damoclès » pendant au-dessus de leur tête : s'ils passent finalement à l'acte, la sanction sera immédiate et sévère. Une telle stratégie de police prédictive tend en fait à anticiper toute violence voire à l'éviter, mais reste néanmoins très incertaine, que ce soit en matière policière ou en matière de protection individuelle. Technique expérimentée aux États-Unis, il en ressort que la méthode de *focused deterrence* implique très souvent un traitement encore plus sévère par la justice en cas de passage à l'acte.

Dans un système tel que le système français, les exigences strictes de légalité criminelle en droit pénal ne sembleraient pas pouvoir permettre de telles stratégies policières. Beaucoup de conditions seraient à remplir : prévoir le domaine d'application d'une telle détection (à quelles infractions s'appliquerait-elle ?) par exemple. Mais la question se poserait surtout du suivi de la personne dès lors qu'elle a été prévenue de la connaissance des services de police ; dans quelle mesure sa surveillance pourrait-elle être autorisée ? La technique de dissuasion, accompagnée du travail de l'intelligence artificielle a pour vocation l'arrêt complet d'actes violents – il n'en reste pas moins que les personnes visées n'ont commis, à l'instant T du message transmis, aucun acte répréhensible. C'est ici plus une détection d'un risque de la personne qu'une anticipation de son geste. On retrouve l'idée très controversée de la dangerosité, à l'exception que l'individu est ici en liberté et n'a pas encore agi.

[117] A.A. BRAGA, « SMART Approaches to Reducing Gun Violence », Bureau of Justice Assistance, U.S. Department of Justice, 2014

C. L'évaluation et la prédiction du risque

Ces techniques sont les plus délicates et risquées à mettre en œuvre, en ce qu'elles s'attèlent à « prédire » le comportement même d'un individu déterminé. Délicates en ce que le comportement humain est variable et changeant, et dangereuses pour les libertés et droits de l'individu lui-même[118]. Deux techniques sont au cœur de la police prédictive : l'une qui se fonde sur des calculs de scores déterminant le risque représenté par un individu, méthode qui se fonde donc sur les données passées, l'autre qui a pour vocation de ne pas uniquement utiliser les informations passées mais d'anticiper le comportement d'une personne alors même qu'elle ne serait pas déjà connue des services de police. A ce titre, et c'est là qu'est aussi la délicatesse du procédé, la frontière est parfois mince entre évaluation purement scientifique et étude sociologique du comportement criminel.

91. *Risk assessment* - Les premières méthodes dites de « *risk assessment* », d'évaluation du risque, reposent sur des calculs de scores faits en fonction d'un certain nombre de facteurs déterminés. Se fondant sur des facteurs connus et donc passés, la plupart de ces méthodes ont vocation à prédire la récidive plus que le crime de manière générale. Ces méthodes sont les plus connues en matière de police prédictive du comportement. En outre, la plupart de ces méthodes d'évaluation du risque sont croisées avec d'autres, comme celle de dissuasion.

92. Le procédé de « *heat list* » - L'une de ces techniques d'établissement du taux de risque présenté par un individu est fondée sur une liste de facteurs qui, plus ils sont cumulés, plus ils présentent un score élevé pour la personne validant ces critères. Plus simplement, le cumul de ces facteurs fait augmenter le score ; plus il est élevé, plus il confirme le caractère « à risque » de la personne. Il faut entendre par risque celui que représente une personne de commettre une infraction, mais il peut aussi s'agir du risque d'être victime. Ainsi l'utilisation de cette méthode de liste peut être faite à des fins de prédiction de la criminalité mais aussi de la victimation.

93. Illustration à Chicago - Le procédé a notamment été testé à Chicago et a présenté des résultats étonnamment satisfaisants. Un nombre de critères ont été listés puis mis en perspective avec une liste établie par la police de personnes pouvant être potentiellement

[118] Cf *infra* n°107

mises en cause dans des violences, plus précisément par balle. Le score pouvant aller de 1 à 500, plus celui-ci était élevé, plus la personne était considérée comme ayant des chances d'être victime ou à l'inverse d'être tireur[119].

La subtilité de la mise en œuvre d'un tel procédé d'évaluation prédictive repose sur le fait que la ville de Chicago est le théâtre de nombreuses violences entre gangs et groupuscules – la majorité des violences commises étant faites par armes à feu et ayant pour cause un conflit entre ces gangs-là ou leurs membres. Ainsi des facteurs tels que les arrestations passées et l'appartenance à un de ces groupes ou le contact avec certaines personnes en faisant partie étaient des éléments de ces listes qui pouvaient influencer le score. Son efficacité a pu être prouvée à quelques reprises comme en 2016 lors du week-end de la fête des mères, durant lequel l'algorithme avait justement identifié 80% de la totalité des victimes de tirs ayant eu lieu à la fin de ces deux jours[120]. Néanmoins, bien que présentant des résultats positifs de manière isolée, cette programmation algorithmique n'a pas substantiellement fait baisser ce type de criminalité à Chicago[121].

94. Technique LSI-R - Une technique similaire est communément utilisée aux États-Unis (technique qui s'apparente à celle du PCL-R en matière d'évaluation de la dangerosité psychopathique). Ce procédé est là encore utilisé directement par les services de police et se présente sous la forme d'un algorithme qui évalue le risque présenté par les individus en probation ou liberté conditionnelle. Ce programme utilise cependant des données plus dynamiques et certains éléments obtenus en temps réel comme la temporalité et la géographie des activités criminelles dans certaines régions. D'autres facteurs sont évidemment utilisés comme le passé pénal et criminel des individus en question, mais aussi des éléments bien plus spécifiques comme les conditions familiales et maritales, les problèmes personnels ou de drogues, l'emploi, les relations interpersonnelles et l'entourage … Ce procédé LSI-R (*Level of Service Inventory-Revised*)[122], a pour fondement l'établissement d'un score qui représentera là encore le niveau de risque de commettre une infraction.

[119] Tout dépend de l'étude qui était faite : victimation ou risque criminogène
[120] Editorial Board, « Editorial: Who will kill or be killed in violence-plagued Chicago? The algorithm knows. », Chicago Tribune, 10th May 2016, disponible électroniquement : http://www.chicagotribune.com/news/opinion/editorials/ct-gangs-police-loury-algorithm-edit-md-20160510-story.html
[121] A.G. FERGUSON, *op. cit.* note 79, p.39
[122] RAND Report, *op. cit*. note 97, p. 91. « *Level of Service Inventory-Revised* » peut se traduire par un inventaire révisé de niveau de service, traduction qui n'illustre pas vraiment le procédé … Ce dernier n'a en effet qu'été utilisé aux États-Unis pour l'instant.

95. Prédire le premier passage à l'acte - Enfin, l'utilisation de l'IA à des fins de police prédictive a vocation à bien plus que le calcul de scores de risques que présentent les individus, notamment en matière de récidive. Le but serait à termes de pouvoir utiliser des données telles que les relations interpersonnelles, les habitudes journalières, les lieux de fréquentation des individus par exemple, pour prédire si une personne qui n'a pas encore commis d'acte criminel serait susceptible d'en commettre. Le chef de la police d'Overland Park où a été testée la technique LSI-R, John Douglas, estime que, dans un futur proche, la police prédictive pourrait bénéficier d'informations novatrices qui viendront des études sociologiques du comportement[123]. Le but serait à termes de « virtualiser » ou « coder » des facteurs et data tels que les habitudes comportementales et sociologiques des individus pour prédire la potentialité de certaines actions et de la criminalité. L'enjeu serait ici d'autant plus important que de tels algorithmes prédiraient le passage à l'acte d'individus alors même qu'ils n'ont jamais été impliqués dans un comportement délinquant.

Ces procédés prédictifs ne sont certainement pas une liste exhaustive de tous ceux existant aujourd'hui. Ils sont cependant les plus connus et généralisés dans l'utilisation de la police prédictive ; bien que la prédiction du comportement ne soit pas encore tout à fait concrétisée. La variété de ces techniques offre certes des nouvelles possibilités de travail à la police, mais il n'est pas certain qu'elles se fondent si facilement dans le travail policier.

<u>Section 2</u> : L'algorithme : nouvel outil policier ou menace pour les libertés ?

L'utilisation de l'intelligence artificielle à des fins prédictives soulève des interrogations légitimes à propos de son impact sur le travail policier. Les premiers commissariats américains ayant expérimenté la police prédictive et notamment PredPol, se sont targués d'obtenir des résultats plus que satisfaisants ; la communauté ayant placé beaucoup d'espoir dans ces algorithmes (A). Néanmoins l'envers du décor n'a pas tardé à se révéler au grand jour : les logiciels prédictifs peuvent être facilement biaisés (B).

[123] B. HEATON, *op. cit.* note 82

§1 : L'intelligence artificielle au service du travail policier

La police prédictive repose principalement sur la logique selon laquelle en améliorant l'efficacité de la police, le taux de criminalité baissera. Résultat qui a été constaté dans certaines villes américaines expérimentant la police prédictive (A). Mais l'un des plus grands espoirs placés dans ces logiciels est celui de l'objectivisation du travail policier (B).

A. L'amélioration des chiffres du crime

96. PredPol - Les différentes méthodes algorithmiques de police prédictive, dont la liste est constamment approvisionnée, sont apparues une par une suite à l'engouement qui a émergé autour de cette nouvelle méthode de traitement des infractions. Ainsi l'apparition d'un procédé ou d'un autre se fait généralement par le développement d'un nouveau logiciel directement dans un commissariat – PredPol étant loin d'être le seul existant. En effet de nombreuses villes – encore une fois, majoritairement américaines – ont à leur tour expérimenté l'une de ces méthodes à l'échelle locale. Dans la plupart des cas, la mise en place d'un tel logiciel se fait à titre d'expérimentation, afin d'évaluer si elle serait réaliste sur le long terme. Évaluation qui s'est avérée positive aux yeux de nombreux commissariats américains avec PredProl, désormais l'algorithme prédictif le plus populaire aux États-Unis, dont les exploits sont vantés par un grand nombre de chefs des services de police sur le territoire américain. Nombreux sont donc les chiffres ressortant comme positifs quant à la réduction de certaines infractions dans les villes ayant testé l'utilisation d'un algorithme prédictif.

97. Débuts à Los Angeles - La première ville américaine ayant initié l'utilisation de PredPol dans ses commissariats est la ville de Los Angeles, dès 2011. Pendant près d'un an entre 2013 et 2014, le taux de certaines infractions a baissé : l'un des départements policiers, la *Foothill Division*, a vu une baisse de 20% des crimes prédits sur l'année[124]. Le site internet PredPol se vante même d'une journée « sans crime » dans ce département, le 13 février 2014. Les premiers essais se sont faits par la technique suivante : des cartes étaient données aux officiers de police des différentes divisions utilisant PredPol, indiquant les points de patrouille où se rendre, points de ce fait *a priori* à risque. A l'image

[124] Chiffres issus du site web PredPol : http://www.predpol.com/results/

de toute expérimentation, certaines cartes avaient été établies par un procédé prédictif, par l'algorithme PredPol, d'autres avaient été établies par des analystes travaillant à l'intérieur de la division en question et étant donc familier avec les chiffres et tendances criminogènes de la zone. En outre, seulement certaines infractions étaient visées : les cambriolages, vols de véhicules et vandalisme sur les voitures. Ces infractions représentent en effet la majorité des délits commis dans la ville de Los Angeles.

Les officiers ont donc été amenés à travailler ainsi pendant un an lorsqu'ils avaient à traiter de ces délits, étant équipés d'ordinateurs ou processeurs de localisation et de signalisation d'infractions dans leurs voitures de patrouille – technologies déjà utilisées indépendamment de l'expérimentation de PredPol. En moyenne, l'utilisation des techniques prédictives « de base » a eu pour conséquence une baisse de 7,4% de la commission des infractions étudiées, et une baisse de 3,5% lorsque les données issues des outils de prédictions les plus développés étaient utilisées. En outre, dans l'ensemble, il s'est avéré que l'utilisation d'un algorithme de police prédictive a fait réduire le nombre de cambriolages, de vols de voiture et de vandalisme[125]. Le fait pour les officiers en patrouille d'être informés *a priori* des lieux et heures de potentielles infractions a eu un effet de dissuasion, principale cause de la baisse de ces chiffres. Il reste cependant fort probable que les délinquants s'adaptent ; là où le logiciel prédictif était utilisé, le chiffre baissait, mais il devait par conséquent augmenter dans une zone non-couverte par le traitement algorithmique …

Dans d'autres zones de Los Angeles, sur la même période, les analystes ont pu prédire 2,1% des délits, là où l'algorithme en prédisait 4,7%[126] ; dans la ville de Kent, 6,8% des infractions étaient prédites par l'homme, 9,8% l'étaient par le logiciel[127]. Or, la majorité de ces chiffres si satisfaisants s'avère être issue des statistiques que les fondateurs de PredPol ont eux-mêmes établis. Ainsi une part de méfiance et d'objectivité est à garder, en ce que ces chiffres pourraient être gonflés et extrêmement subjectifs. Il n'en reste pas moins que dans beaucoup de villes ayant expérimenté PredPol, les taux d'infractions ont

[125] P.J. BRANTINGHAM, M. VALASIK, G.O. MOHLER, « Does Predictive Policing Lead to Biased Arrests? Results from a Randomized Controlled Trial », *Statistics and Public Policy Journal*, vol. 5, n°1, 2018
[126] G.O. MOHLER et al., « Randomized Controlled Field Trials of Predictive Policing », *Journal of American Statistics Association*, 1399, 2015
[127] *Ibid.*

substantiellement baissé sur certaines périodes. La ville d'Alhambra a même vu son taux de cambriolages diminuer de 32% en 2013[128], selon le site internet PredPol.

98. Autres logiciels - PredPol n'a pas été le seul algorithme à faire ses preuves, ainsi des chiffres similaires ont pu être obtenus grâce à d'autres logiciels indépendants, dans d'autres villes des États-Unis. La ville de Memphis dans le Tennessee a mis en place un programme informatique appelé *Blue CRUSH*[129] basé sur les techniques du *data mining*, se servant de données géographiques et spatiotemporelles passées. Suite à l'utilisation de ce programme, la police de Memphis a même rapporté que les données d'infractions constatées étaient très rapidement enregistrées et traitées par le logiciel prédictif, permettant ainsi au commissariat de répondre aux menaces de criminalité imminentes avant même qu'un acte soit commis. Initialement mis en place en 2005, période à laquelle Memphis était une des villes qualifiées des plus dangereuse aux États-Unis, les résultats cinq ans après ont été impressionnants. En 2010, les infractions de car-jacking avaient diminué de 75% par rapport à 2006, les cambriolages de commerces à main armée de 67%[130].

L'initiative est venue de l'important accroissement du nombre d'infractions violentes et de l'insécurité conséquente dans cette ville du Tennessee. En 2008, l'algorithme Blue CRUSH a aidé l'un des commissariats à démanteler un réseau de trafic de drogues et de prostitution implanté dans des hôtels de la ville. Au courant de la présence du réseau dans la ville, c'est le logiciel qui a, par analyse des données de constatation de la consommation, vente et production de drogues, ciblé petit à petit certaines zones de différents voisinages, à chaque fois curieusement proches d'un hôtel. Ceci a donc mené la police à investiguer ces bâtiments, recherches qui ont effectivement révélé des réseaux de trafic, de ventes et de consommation de drogues, de prostitution, de prostitution de mineurs, de vols et même un homicide[131].

99. IBM - Là encore, le système Blue CRUSH a été développé par une entreprise privée d'autant plus connue qu'elle est une des initiatrices des premiers ordinateurs :

[128] *Op. cit.* note 124, http://www.predpol.com/results/
[129] Le terme « Blue » renvoie à la couleur bleue des uniformes de la police américaine, le terme CRUSH est un acronyme de « *Crime Reduction Utilizing Statistical History* », soit « réduction du crime par l'histoire statistique ».
[130] RAND report, *op. cit.* note 97, p.69
[131] « Four Area Hotels Closed for Business Following 'Operation Heartbreak Hotel' », Shelby County District Attorney General, 2008

IBM. L'entreprise a très vite su tirer avantage de l'apparition des techniques informatiques de police prédictive et ainsi proposer aux villes les plus menacées par la criminalité des algorithmes prédictifs. Là encore, les développeurs se targuent sur le site internet d'IBM des scores obtenus par l'utilisation de leurs algorithmes : Richmond, en Virginie, est passée de 5ème ville la plus dangereuse des États-Unis à 99ème – chiffres néanmoins peu détaillés[132].

100. Chiffres inconstants - Bien que la majorité des villes américaines ayant expérimenté des algorithmes de police prédictive aient vu leurs chiffres de criminalité diminuer dès les débuts de l'utilisation de ces logiciels, elles ont aussi vu dans leur majorité que ces chiffres n'étaient pas constants et durables. En effet, les résultats obtenus sur le long terme par la ville de Memphis par exemple, ne sont pas majoritaires. L'exemple de PredPol l'a souvent montré : des baisses de chiffres sont obtenues rapidement durant la première année d'utilisation du procédé, néanmoins les taux d'infractions réaugmentent souvent les années suivantes. Les chiffres obtenus ont tendance à ne pas être constants. A Los Angeles, bien que les chiffres aient été acceptables entre 2013 et 2014, le taux d'infractions concernées par le traitement s'est vu rehaussé entre 2015 et 2016[133].

De telles constatations n'influencent cependant que rarement l'opinion des chefs de police utilisant PredPol ou d'autres logiciels : la plupart du temps, même en présence d'augmentation de la criminalité, l'intelligence artificielle continue de s'implanter dans les bureaux de police. En effet la philosophie non-commerciale existant derrière l'utilisation de logiciels prédictifs pousse souvent les administrations judiciaires américaines à la développer.

B. L'objectivisation du travail policier

Le développement de l'IA au service de la police, en particulier en matière de prédiction de la délinquance et de la criminalité, se trouve être souvent remis en cause et

[132] Chiffres issus du site web IBM : http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/crimefighting/transform/ . En effet, il n'est pas vraiment précisé en combien de temps ces chiffres ont été obtenus, seul le classement de la ville de Richmond est donné à titre d'exemple …

[133] B. POSTON, « Crime in Los Angeles Rose in All Categories in 2015, LAPD Says », L.A. Times, 2015, disponible électroniquement : http://www.latimes.com/local/crime/la-me-crime-stats-20151230-story.html

critiqué. Néanmoins, à l'origine même de la mise en œuvre des premiers algorithmes se trouvent des causes favorables au renforcement de la protection des individus, de leurs droits, mais aussi du travail policier en général et de ses agents et officiers. PredPol a fait certes ses débuts à Los Angeles, et s'est diffusé sur le territoire et notamment dans les villes faisant face à des conflits entre groupes violents mais aussi entre policiers et groupes ethniques et culturels. Les lourds faits divers et scandales tenant à la mort de certains individus de la communauté afro-américaine du fait de tirs policiers ont largement influencé l'utilisation de l'intelligence artificielle dans le contrôle et la prévention aux États-Unis.

101. Neutralité de l'intelligence artificielle - La stigmatisation de certaines communautés ethniques, religieuses ou culturelles a prouvé que le travail policier en était parfois effectivement impacté ; orientant faussement les soupçons de certaines patrouilles ou agents vers une personne noire aux États-Unis par exemple, plus que vers une personne blanche. Or trop souvent, l'issue d'une intervention fondée sur des éléments biaisés s'est avérée tragique – ces dérives policières ont mené à la création du mouvement *Black Lives Matter*. Stigmatisations et violences au détriment des individus, mais aussi de manière plus générale du travail policier qui s'en trouve dévié de ses objectifs. En effet, les violences policières sont beaucoup trop fréquentes aux États-Unis, à l'image des évènements de Ferguson par exemple, en 2014. Le problème étant en outre que les victimes de tirs policiers ne sont pas toujours armées, tentant simplement de s'enfuir. Les protestations naissent de plus en plus dans les villes concernées, en faisant une cause populaire nationale.

Ce sont donc ces pratiques discriminatoires au sein de certains bureaux de police américains qui ont appuyé la nécessité d'un changement de fonctionnement dans ceux-ci, de l'intégration de nouvelles techniques qui pourraient faire barrière à toute stigmatisation et racisme. C'est à ce titre que le développement des politiques pénales et policières basées sur le Big Data et l'utilisation de machines et algorithmes informatiques ont été accueillis – du moins au départ – d'un bon œil. Les événements de violences policières sont la preuve du manque de neutralité dans le processus d'action de certains agents. Ainsi, quoi de mieux qu'une entité non-humaine, scientifique et robotique, pour atteindre cette neutralité dans le processus de décision ?

L'intégration de l'IA et des techniques de police prédictive ont donc été vues par la population et notamment certaines communautés victimes d'injustices policières, comme une porte s'ouvrant sur l'objectivisation du travail et de l'action policière. Ce sont du moins les attentes que beaucoup ont eu à l'égard de l'introduction de PredPol par exemple. Et effectivement la présentation de ce dernier a confirmé certaines de ces attentes. Le logiciel PredPol étant programmé sur le modèle d'un algorithme de sismologie, il n'est censé se baser que sur les données suivantes de l'infraction : quoi, quand et où. Ainsi, présenté comme tel, PredPol n'a pas vocation à utiliser des données relatives aux personnes mais exclusivement indépendantes de toutes données ou caractéristiques personnelles. C'est d'ailleurs ce que le site internet du logiciel rappelle : les seuls éléments relatifs à la personne impliqués dans le processus algorithmique sont en fait les signalisations faites par les victimes.

102. Résultats théoriques - Des points positifs ont aussi été rapidement trouvés aux méthodes de police prédictive utilisant des données à caractère personnel ou tenant à l'individu. En effet, à travers le brassage informatique, bien plus rapide et efficace pour faire ressortir des chiffres, des statistiques sont ressorties concernant les caractéristiques du crime au niveau local. Du point de vue de la recherche, de tels résultats ont aussi pu servir au travail théorique en ce que justement, des théories sont apparues de cette utilisation de l'IA.

Une telle théorisation s'illustre par exemple avec la méthode de *focused deterrence*, de la dissuasion : déjà reconnue dans le milieu criminologique et pénal, ses fondements se sont vus renforcés en ce qu'elle a permis le développement de la police prédictive. En effet, le fait de renforcer la présence de patrouilles de police informées en direct par le logiciel des zones à risques, les délinquants s'en voient dissuadés – ce qui montre effectivement des tendances sociologiques et humaines intéressant les chercheurs ou universitaires.

L'analyse algorithmique permet en outre une ouverture du champ de vision sur le phénomène criminel dans une zone déterminée – souvent une ville. Certains facteurs peuvent échapper à l'attention de la police, bien qu'étant composée de professionnels – tout agent reste humain et face à un trop plein d'informations, des détails et liens peuvent échapper à n'importe qui. Ainsi la programmation informatique et le datamining semblent être des solutions effectives à ces oublis en ce qu'ils peuvent faire apparaître aux professionnels une caractéristique, un facteur, qui aurait été oublié ou qui aurait été délicat

à appréhender par un officier. Dans les cas de l'analyse spatiotemporelle par exemple, un facteur criminogène aurait très bien pu ne pas être soupçonné.

103. Efficacité - Au-delà de l'objectivité et de l'impartialité de la machine, l'utilisation de l'IA à des fins de police prédictive sert aussi à l'amélioration de l'efficacité de la police dans son travail. Le fait de délester les agents de certaines obligations parfois chronophages et contre-productives, leur permet de rendre ce gain de temps utile à d'autres fins : concentrer les patrouilles sur certaines zones, sur certaines infractions etc. L'efficacité ne peut qu'augmenter si l'utilisation des moyens de police prédictive et du datamining s'ajoutent aux moyens existants.

104. Coût - La question se pose cependant du coût de l'intégration de telles innovations, qui impliquent forcément la modernisation de certaines installations et une programmation informatique faite par d'autres professionnels que ceux du cadre pénal. Les adeptes de PredPol ont cependant la réponse à de tels doutes qui pourraient émerger : il faut certes adapter les installations existantes, néanmoins l'efficacité des algorithmes prédictifs compense la nécessité d'effectifs policiers. Effectivement, si l'on suit une telle logique, – qui sous-entendrait que tout logiciel prédictif est sans faille et extrêmement précis – PredPol permettrait de mieux répartir les patrouilles et les tâches policières au sein des effectifs existants, supprimerait certaines dépenses relatives à de nouveaux effectifs de patrouilles, et améliorerait les conditions de travail des employés existants.

105. Précision - Enfin, au vu de la multiplicité grandissante des sources nourrissant le Big Data et de la capacité des intelligences artificielles, les techniques prédictives se devraient d'être de plus en plus précises, d'autant plus si le facteur de l'apprentissage autonome est ajouté à l'équation de la police prédictive. Plus l'algorithme et la machine ont d'informations à leur disposition, plus les liens peuvent se créer ou être écartés. Plus les résultats seront validés ou non par l'Homme, plus l'IA montrera de précision dans le processus de prise de décision.

Les avantages accordés aux algorithmes prédictifs sont donc nombreux, et les espoirs d'efficacité de l'IA grandissent. Néanmoins, ces arguments « pro-PredPol » sont relativement théoriques, et étaient du moins ceux donnés en amont de la concrétisation des méthodes de police prédictive. Il s'avère qu'en tout état de cause, bien que les résultats statistiques soient parfois satisfaisants, les enjeux derrière la pure efficacité

peuvent être graves. Car en effet, derrière la machine, il n'en reste pas moins que c'est toujours le cerveau humain qu'on retrouve.

§2 : Des algorithmes surtout liberticides

Les réjouissances n'ont été que de courte durée dans les villes utilisant la police prédictive ; ses défauts ne se sont pas faits attendre. Des défauts d'autant plus graves qu'ils prennent la plupart du temps la forme d'atteintes aux libertés et droits des individus (A). Le caractère liberticide de la police prédictive pourrait cependant être évité, à condition de prendre en compte ces possibilités en amont de son utilisation (B).

A. Les atteintes avérées aux libertés individuelles

La mise en œuvre pratique de la police prédictive aux États-Unis s'est avérée souvent satisfaisante en matière de chiffres et de réduction de la délinquance. Certaines techniques ont eu un effet de dissuasion, permettant d'anticiper l'acte criminel – l'un des buts premiers de la police prédictive et du *data surveillance*. Néanmoins le désir de développer immédiatement l'utilisation de l'intelligence artificielle au service de la lutte contre la criminalité relève aussi beaucoup de l'utopie. À se concentrer uniquement sur une politique de chiffre, certes le datamining et le *predictive policing* peuvent être efficaces. Or il se trouve que la prédiction du crime se fait parfois au détriment des libertés et droits individuels, et présente une menace non-négligeable à l'encontre de principes constitutionnels, juridiques et pénaux. Et ce tant en Europe que sur le continent nord-américain.

106. « *Les biais de la machine* » - En effet les premiers résultats obtenus à Los Angeles, Chicago ou Memphis ont vite ravi les départements de police, et semblaient répondre aux attentes de tout un chacun. Le ravissement n'a été que de courte durée. Le 23 mai 2016, l'organisation à but non lucratif spécialisée dans le journalisme d'investigation *Pro Publica* publie sur son site internet un article alarmant sur les résultats obtenus par un algorithme prédictif en 2014[134]. L'article titre « *Les biais de la*

[134] J. ANGWIN, J. LARSON, S. MATTU, L. KIRCHNER, « Machine Bias », *Propublica*, 2016, disponible électroniquement : https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

machine »[135], « *un logiciel est utilisé sur le territoire pour prédire les futurs criminels. Et ce logiciel a des préjugés contre les noirs* »[136]. *Pro Publica* va alors soulever le premier problème de l'intelligence artificielle, qui devait pourtant être évité grâce à la police prédictive : la machine pourrait être raciste.

Une jeune femme se voit arrêtée et punie d'une amende pour avoir tenté de voler un vélo attaché dans la rue – acte tenté, la jeune femme s'étant faite prendre sur le fait par un voisin. Ce dernier ayant prévenu la police à temps, la jeune femme, en fuite, est arrêtée. Dans cette même ville de Fort Lauderdale, et tout à fait indépendamment des faits précédents, un homme est arrêté pour vol dans un magasin. Chacun des individus cités ici s'est vu puni d'une amende à hauteur de 80$, les infractions commises étant de la même catégorie[137].

Il faut préciser qu'à ce moment-là, le département de police de Fort Lauderdale utilise un algorithme prédictif dans lequel les agents intègrent toute arrestation, les données relatives à chacune de celles-ci et donc des personnes arrêtées. L'homme était, lui, connu de la machine : braquage à main armé, vol à l'étalage … il avait en effet été l'auteur de nombreuses autres infractions bien plus graves, qui lui avaient d'ailleurs valu de faire de la prison pendant 5 ans. La jeune femme, elle, n'avait qu'un antécédent enregistré pour une infraction minime – à hauteur d'une contravention – qui de plus avait été commise lorsqu'elle était mineure.

Au moment de l'arrestation, l'intelligence artificielle programmée sur la base de la méthode du *risk assessment* fait ressortir un score de « risque criminogène » pour chacun des individus. Les chiffres ressortant de l'analyse sont étonnants : la jeune femme présente un score plus élevé que l'homme au passé délinquant. Un détail différenciant les deux individus qui ne devrait pas être pertinent dans le processus algorithmique apparaît cependant : la jeune femme est noire. Deux ans plus tard, le constat confirme le biais informatique : la jeune femme n'a pas recommis d'acte délinquant, alors même que l'homme s'est vu condamné à plusieurs reprises pour cambriolage. Or, ces scores générés par la machine sont utilisés dans les tribunaux, parfois pour évaluer la sortie de prison de détenus.

---

[135] « *Machine bias* »
[136] « *There's software used across the country to predict future criminals. And it's biased against blacks* »
[137] « *Petty theft* », qui peut se traduire communément par « larcin », et être qualifié juridiquement de vol simple.

107. Inquiétudes confirmées - L'information est relayée, alors même qu'en 2014 l'*Attorney General* Eric Holder avait tenté d'attirer l'attention sur les risques de biais de la machine dans les pratiques de police prédictive : « *bien que ces mesures soient réalisées avec les meilleures intentions, je suis inquiet sur le fait qu'elles pourraient malencontreusement ébranler nos efforts investis dans l'assurance d'une justice individualisée et équitable* »[138]. Son inquiétude était bien de voir l'effet inverse désiré dans la mise en œuvre de ces algorithmes, à savoir l'exacerbation des disparités et injustices déjà existantes dans certains pans du système judiciaire américain. Préoccupations qui se sont donc malheureusement confirmées : Pro Publica soulève dans ce même article que de manière générale, ces algorithmes étiquettent – à tort – bien plus facilement les personnes noires que les personnes blanches ; inversement, les logiciels évaluent parfois faussement les personnes blanches comme présentant un risque bas de délinquance.

L'investigation faite par l'organisation Pro Publica a très largement secoué toutes les espérances et les attentes de ceux qui ont vendu la police prédictive et l'intelligence artificielle prédictive comme la solution à tous les problèmes. Il n'en reste pas moins que ces algorithmes sont, quoi qu'il arrive, originairement programmés par l'Homme. C'est bien le cerveau et la pratique humaine qui sont derrière la création de telles techniques censées être neutres ; les données soumises à l'analyse et l'algorithme de départ sont nécessairement le fruit d'une réflexion humaine. Et ce quand bien même l'intelligence artificielle fonctionne sur une base d'apprentissage autonome – les biais en sont d'ailleurs d'autant plus accentués dans un tel cas. Justement, le processus d'apprentissage va se faire sur la base d'informations à l'origine teintées et biaisées ; on ne peut donc que s'attendre à ce qu'elle intègre dans son analyse une méthode discriminatoire.

108. Données sensibles et discrimination algorithmique - Le caractère « raciste » et discriminatoire ressortant de cet algorithme prédictif a donc remis en cause beaucoup de présupposés sur l'utilisation de l'IA dans les commissariats et à des fins pénales. Ce problème, constaté pour l'instant uniquement aux États-Unis, pourrait en principe être évité en Europe. C'est du moins ce que les textes de l'Union pourraient prévenir à travers la protection accrue des données dites sensibles. La protection

[138] « *Although these measures were crafted with the best of intentions, I am concerned that they inadvertently undermine our efforts to ensure individualized and equal justice* »

spécifique accordée à ce type de données montre bien qu'elle est nécessaire : l'appartenance ou l'origine ethnique, culturelle, religieuse a faussement teinté les analyses informatiques américaines. Or, à la clef de ces calculs logiciels, c'est très souvent la prison qui se trouve pour les personnes concernées. Le danger est donc d'autant plus important qu'on parle de restrictions des libertés individuelles au bout de la chaine.

Cela soulève en outre la question de l'erreur judiciaire – à se demander cependant si l'on parle toujours d'erreur judiciaire lorsque la décision est fondée sur un résultat algorithmique … L'issue peut être encore plus grave en ce que certains États américains appliquent encore la peine de mort. Bien des personnes ont été faussement condamnées à cette peine dans l'histoire judiciaire américaine ; à ce titre, si la police prédictive est un facteur supplémentaire de risque d'erreur judiciaire, les conséquences pourraient être dramatiques.

109. Surveillance totale - Les préoccupations américaines sont aussi tournées vers la problématique de la surveillance accrue des citoyens, avec notamment les révélations faites par *Wiki Leaks* ou Edward Snowden, quant aux pratiques de la NSA ou de la CIA. Les atteintes à la vie privée sont donc une inquiétude grandissante chez les américains – la police prédictive ne peut qu'accroitre ces appréhensions, et ce à juste titre au vu du système juridique américain[139]. Au-delà du suivi par vidéo surveillance, c'est le *data surveillance* qui inquiète et qui pourrait en effet être impliqué dans la prédiction de la criminalité. Le risque d'atteinte aux droits individuels est là encore présent, en ce qu'un algorithme, pour être précis et ne pas induire en erreur, a besoin d'une large quantité de données.

La « sur-surveillance » peut s'avérer d'autant plus dangereuse qu'elle engendrerait une inquiétude des individus vis-à-vis des autorités et du système judiciaire. L'incidence directe serait l'autocensure voire même le changement, la modification du comportement des individus. Cette dernière conséquence irait alors à l'encontre même des objectifs de la police et de la lutte contre la criminalité. Le sentiment d'être constamment observé et surveillé atteindrait rapidement tout un chacun, les délinquants ou criminels les premiers, qui s'adapteraient à de telles pratiques et rendraient dès lors plus difficile la tâche aux logiciels.

[139] Cf *supra* n°72

Les conclusions trop rapidement faites, le faux étiquetage d'individus basé sur des caractéristiques discriminatoires, pourraient rendre dangereuse l'utilisation de l'intelligence artificielle à des fins qui, à l'origine, sont destinées à la protection des citoyens contre la criminalité. Et ces failles de la police prédictive ne sont pas les seules ; la liste n'est pas exhaustive, en ce que l'importation de ces techniques en Europe engendrerait des atteintes aux principes des États de l'Union, et de la France, qui sont indispensables à l'efficacité et à la bonne administration de la justice[140]. Des solutions pourraient être envisagées, face à l'expérience américaine, pour palier à tout risque de violation des droits et libertés ou tout effet contre-productif.

B. Anticiper les biais de la police prédictive

Bien que le nombre de risques que présente la police prédictive ne soit pas proportionnel aux avantages qu'elle pourrait apporter, l'expérience américaine peut permettre à l'avenir de se préparer à ces biais. Des solutions théoriques existent en effet, pour faire de l'IA prédictive plus un outil qu'une menace – à voir si dans le futur, cette théorie est applicable en pratique.

110. Transparence - L'une des nouvelles problématiques au centre des enjeux du Big Data et de l'intelligence artificielle est celle de la transparence des entités, privées ou publiques, utilisant ces procédés. Dans le cas de la police prédictive, il faudrait en effet mettre un point d'honneur à ce que cette transparence soit respectée, pour éviter toute situation d'incompréhension quant au fonctionnement, aux résultats et à l'utilisation de l'IA prédictive. Un rapport de recherche financé par un programme européen en 2013 voit deux moyens principaux de mise en œuvre de la transparence : une transparence du système lui-même et une transparence quant à l'utilisation faite de ce système[141]. En d'autres termes, il serait nécessaire de pouvoir faire comprendre à tout citoyen, du moins ceux impliqués dans la chaîne pénale, comment un tel logiciel fonctionne. Non pas qu'il faudrait que toute personne puisse comprendre la programmation algorithmique, mais du moins faudrait-il que toutes les données utilisées soient citées, ainsi que ce à quoi elles sont dédiées dans cet algorithme. La deuxième étape est ensuite la transparence quant à

[140] Cf *infra* n°119
[141], E. SCHLEAHN, P.AICHROTH, S.MANN, R.SCHREINER, I.SHEPHERD, B.L.W. WONG, « Benefits and Pitfalls of Predictive Policing », Conference Paper, 2015

l'utilisation qui en est faite par les autorités : les résultats sont-ils interprétés ? Analysés ? Utilisés directement sans remise en cause ? Questions qui, si les autorités y apportent des réponses, permettraient d'assurer l'intégrité totale du processus pénal guidé par des techniques de police prédictive.

111. Information - La transparence, au-delà de rassurer l'individu et les citoyens, leur permettrait un droit de regard sur ces techniques. L'apport d'un regard critique sur la police prédictive pourrait en effet exclure l'utilisation de certaines méthodes, à la faveur d'autres ; dans des sociétés démocratiques, l'avis du citoyen sur l'utilisation de ses données ne peut qu'être la meilleure barrière à toute atteinte à ses intérêts. Une transparence sur la collecte et l'analyse des données permettrait d'éviter de transformer le Big Data en « *black data* »[142], afin d'en faire à terme un « *bright data* »[143]. Andrew Guthrie Ferguson suggère à ce titre une approche inversée de la police prédictive[144], qui permettrait tout autant l'anticipation du crime ; au lieu d'une surveillance accrue des individus susceptibles d'être impliqués dans des vols de voiture ou car-jackings, la solution alternative serait de prévenir et informer les propriétaires de modèles de voiture étant les plus enclins au vol. Par l'éveil de la conscience collective, le sentiment de surveillance constante diminue, l'atteinte potentielle aux intérêts de la personne elle aussi.

112. Protection des données - Au-delà même de la transparence sur l'utilisation de l'IA à des fins prédictives, la prévention peut se faire encore plus en amont, quant à la protection des données des individus. Une meilleure information et l'ouverture de plus de possibilités de contrôle de ses propres données permettraient à tout citoyen d'anticiper un usage non voulu de celles-ci. Un tel contrôle se fait notamment avec les PET[145], systèmes permettant d'harmoniser les obligations tenant à la vie privée et les données personnelles avec les analyses qui peuvent en être faites. L'anonymisation, la pseudonymisation, la gestion des options de publications des données, sont autant de mesures disponibles pour les personnes pour qu'elles puissent de plus en plus accroitre la protection de leurs données à caractère personnel.

[142] A.G. FERGUSON, *op. cit.* note 79. Littéralement « data noir », peut se traduire dans le contexte voulu par l'auteur par « data flou », sous-entendu le voile qui peut couvrir l'utilisation du Big Data lorsque les résultats sont discriminatoires et attentatoires aux libertés.
[143] *Ibid.* Littéralement, « data clair », traduit ici l'idée même d'une utilisation transparente du Big Data.
[144] *Ibid*, p. 169
[145] *Privacy-Enhancing Technologies*

113. Encadrement légal - Mais de manière générale, la mise en œuvre de telles mesures ne peut se faire que par un encadrement législatif en amont. Dans l'hypothèse d'une politique pénale intégrant l'usage de la police prédictive, la loi pénale devrait en effet encadrer strictement toute exception à la protection des données, régir les différentes méthodes pouvant être utilisées. On pourrait par exemple envisager un texte ne prévoyant que l'utilisation d'algorithmes prédictifs spatiotemporels ou géographiques, et excluant toute analyse basée sur la personne. Du moment que la police prédictive est utilisée à des fins de prise de décision, qui peut engendrer des conséquences pénales et judiciaires, l'expérimentation de tels logiciels ne peut faire l'objet d'un suivi que de la part de ses utilisateurs et créateurs – à savoir les autorités de police et les analystes.

En outre, l'hypothèse d'intégration de la police prédictive dans le processus pénal ne peut remplacer complètement toutes les autres pratiques policières et de lutte contre la criminalité. L'expérience, la pratique, et ce qu'on pourrait appeler l'instinct policier, absolument nécessaires dans l'enquête, ne pourront jamais être remplacés par la machine.

Conclusion Partie I

La multiplication des sources de données, du fait de la mutation de l'environnement numérique et virtuel, a créé cet ensemble de méga donnés, le Big Data. En parallèle, l'initiation et les progrès liés à l'intelligence artificielle ouvrent des possibilités de traitement simplifié de ce Big Data. Ainsi, l'un fonctionne avec l'autre, ils sont des corollaires. L'intelligence artificielle permet un meilleur traitement du Big Data ; l'intelligence artificielle n'a, elle, pas lieu d'être sans ces données. Les problématiques de la police prédictive nécessitent donc de se préoccuper de la question des données personnelles. Ces dernières se voient traquées et utilisées tant dans le secteur privé que le secteur public. Ce qui ouvre des perspectives et possibilité pour les autorités répressives, à des fins d'amélioration du travail judiciaire et policier.

L'Union européenne a su anticiper la protection de ces données à caractère personnel, consciente de ces enjeux qui peuvent menacer les libertés individuelles. Enjeux auxquels les États-Unis, eux, n'ont pas toujours su faire face. Et ce, alors même qu'ils sont la première nation à concrètement expérimenter la police prédictive. Ce manque législatif peut ne pas être si grave pour les individus dans le cas des méthodes spatiotemporelles et de localisation du crime, les données personnelles étant exclues de cette analyse prédictive. Néanmoins, ce manque serait réellement dangereux pour les libertés individuelles dans le cas du développement des techniques prédictives du comportement criminel, ces dernières annonçant la nouvelle ère de la police prédictive, alors même que les premières sont encore au stade de l'expérimentation.

Une fois les bases de la police prédictive posées, il est nécessaire de regarder plus loin que sa simple expérimentation. Car les méthodes prédictives poursuivent toutes un but commun : l'amélioration de la réaction.

Partie II
De la prédiction à la réaction

114. Former - « *Beaucoup de futurs jeunes officiers sont des adeptes de la technologie et espèrent que ces technologies qu'il utilisent à la maison le seront … dans leur travail* »[146]. L'intégration de l'intelligence artificielle parle en effet plus aux dernières générations, ayant grandi avec les nouvelles technologies, c'est pourquoi on pourrait imaginer que ces jeunes officiers s'adapteraient beaucoup plus facilement à la police prédictive. Il est vrai que ces générations de policiers seraient plus enclines et ouvertes à accueillir des algorithmes prédictifs, et on pourrait donc penser qu'il leur faudrait peu de temps pour s'y adapter et savoir s'en servir. Cependant les méthodes prédictives ne sont pas assimilables aux technologies « classiques » utilisées dans la vie de tous les jours. La précipitation pourrait en effet être l'ennemie de l'efficacité de la police prédictive ; former ses utilisateurs et les informer sur les risques et limites à ne pas atteindre, est indispensable.

Car une mauvaise utilisation de l'intelligence artificielle prédictive peut avoir des conséquences particulièrement graves : les officiers de police sont certes les premiers impactés par son utilisation, mais certainement pas les derniers. La fascination existant autour de la création d'un cerveau artificiel doit s'accompagner d'une réflexion profonde sur l'éthique de cette intelligence robotique. Dans le cas du contexte pénal, le travail policier est effectué en amont de la chaîne pénale et est indispensable à la participation aux différentes procédures qui vont, à termes, conduire à une décision de condamnation ou non. L'introduction d'une technique aussi novatrice que la police prédictive aurait donc nécessairement une influence sur le procès pénal et impacterait le travail de tous ses acteurs (Chapitre 1). La rapidité à laquelle va l'innovation technologique est tellement importante qu'elle dépasse les frontières ; tout comme les nouvelles formes de criminalité, qui savent elles aussi s'adapter aux mutations de la globalisation.

[146] "*A lot of the younger officers that are coming up are very adept with technology and have an expectation that the technology they use at home will be used … on the job*", B.HEATON, "Predictive Policing a Success in Santa Cruz, Calif.", Governmental Technology, October 8 2012, disponible électroniquement : http://www.govtech.com/public-safety/predictive-policing-a-success-in-santa-cruz-calif.html

Les exemples d'expérimentation et d'adoption de la police prédictive sont les plus pertinents aux États-Unis. En outre, au vu des politiques que certains dirigeants américains ont pu mener, il ne serait pas étonnant que les autorités fédérales soient elles-mêmes attirées par l'expérimentation de ces techniques au niveau national, à des fins de renseignements, de lutte contre la criminalité touchant tout le territoire. L'État américain est loin d'être le seul à s'ouvrir aux logiciels prédictifs ; les pays européens commencent eux aussi à s'y intéresser. Or, qui dit Europe, implique nécessairement un encadrement de la part de l'Union européenne. Et au vu des problématiques criminelles touchant le territoire européen, en particulier le terrorisme, les coopérations émergent et se renforcent, notamment en matière d'échanges de données. L'intelligence artificielle dépasse les frontières, la criminalité organisée s'internationalise : les États des différents continents adaptent leur politique, et les enjeux de la police prédictive et du Big Data commencent à atteindre ces politiques (Chapitre 2).

Chapitre I
L'influence de l'intelligence artificielle sur le fonctionnement interne de la chaîne pénale

Les théories derrière la police prédictive ont vocation à faire muter le travail policier, sans le transformer fondamentalement ; les officiers doivent pouvoir s'adapter, sans trop changer leurs habitudes de travail. L'introduction des techniques de police prédictives ont cependant un impact, qu'on le veuille ou non, sur toute la chaîne du travail policier (Section 1). Or, si le travail policier est impacté, le reste de la chaîne pénale l'est nécessairement ; bien que les effets des algorithmes prédictifs n'aient pas encore été pleinement constatés sur la phase post policière, les conséquences sur le travail des autres acteurs judiciaires peuvent se concevoir (Section II).

Section 1 : L'adaptation de l'organisation policière

Le travail policier consiste en plusieurs tâches, toutes tendant de manière générale vers deux buts précis : la lutte contre la délinquance et la prévention de celle-ci. A ces fins, la police travaille principalement à l'investigation et à l'action sur le terrain, en temps réel. Ce sont donc les phases d'enquêtes qui pourraient être influencées par l'utilisation d'un algorithme prédictif (§1), aussi bien que l'organisation des effectifs sur le terrain (§2).

§1 : Le bouleversement des techniques d'enquête

Avant même d'agir directement dans les rues et quartiers des agglomérations où ils travaillent, les policiers se doivent, dans le cadre de la recherche de la vérité, d'investiguer les faits qu'ils constatent. La preuve en est avec PredPol, qui a bouleversé certains travaux d'enquêtes (A). En outre, si la police américaine permet une immixtion de l'algorithme prédictif dans l'enquête, il faudrait imaginer les conséquences d'un tel cas de figure en Europe (B).

A. La nécessaire adaptation américaine à PredPol

115. Proactivité - « Proactive ». Ce terme raisonne comme le but ultime de la police prédictive dans la bouche de ses développeurs. L'essence des techniques de prédiction du crime réside dans le travail policier. Et pour être efficace et moderne, la police se doit d'être plus proactive. C'est ce que va permettre l'introduction de la police prédictive dans les commissariats et plus généralement dans la chaîne pénale. Bien qu'encore considérées comme au stade de l'expérimentation, ces nouvelles méthodes – tant scientifiques que juridiques – commencent à s'enraciner dans certaines villes. Cela implique que leur système policier évolue et va nécessairement changer. Car afin d'atteindre ces objectifs de proactivités, il semble qu'en pratique, ce soit bel et bien la police qui s'adapte à l'intelligence artificielle prédictive et non le logiciel qui se fond dans le système policier.

Les résultats concrets observés précédemment[147] sur le territoire américain montrent bien que les équipes de police, lors de l'expérimentation de PredPol par exemple, ont dû changer leurs manières de travailler. Il est vrai que c'est à l'origine le but de l'introduction de la police prédictive – du moins aux États-Unis. La nécessité d'objectivisation du travail policier au niveau local implique forcément une mutation des habitudes de travail des agents. PredPol a non seulement permis d'introduire les méthodes d'anticipation des infractions mais aussi et surtout un changement dans les pratiques des bureaux de police.

116. Système judiciaire américain - Aux États-Unis, le fonctionnement des enquêtes de police est bien différent du modèle français ; ne serait-ce que par la forme que prend l'organisation de chaque État. L'État américain comprend en effet un système fédéral d'enquête pénale et des systèmes distincts d'enquêtes spécifiques à chaque État. Quoi qu'il en soit, ces deux systèmes ont pour point commun le fait que les autorités de poursuites et d'enquête, que ce soit le procureur ou la police, relèvent du pouvoir exécutif et non du pouvoir judiciaire. Ceci illustre le caractère inquisitoire des poursuites pénales du système de Common Law. Ainsi l'enquête est menée par la police de manière indépendante et uniquement à charge – les éléments seront ensuite transmis à l'entité chargée des poursuites.

Au niveau fédéral, ce sont des agences qui mènent les investigations, employant des enquêteurs spécialisés. Dans l'hypothèse où la police prédictive se démocratiserait et

[147] Cf *supra* n°96

attendrait le niveau fédéral, les craintes des citoyens vis-à-vis du FBI, de la NSA ou de la CIA ne pourraient qu'accroître.

Ces éléments propres au système d'investigation, associés à l'utilisation de logiciels prédictifs, donneraient à la police et aux organes de poursuites – tant étatiques que fédéraux – un pouvoir encore plus fort dans le procès. L'enquête faite à Fort Lauderdale[148], au-delà du caractère discriminatoire de l'algorithme, montre que l'attribution d'un score de dangerosité ou de risque criminogène à une personne influence le travail, les soupçons de la police et donc le futur pénal de cette personne. Dans l'exemple de cette jeune femme noire, son passé pénal se résumait à une infraction de faible gravité commise lorsqu'elle était mineure, avant qu'elle soit arrêtée pour la tentative de vol d'un vélo – c'est ce pourquoi son nom s'est vu inscrit dans le logiciel prédictif. Dans l'hypothèses où cette femme se ferait arrêter une seconde fois pour une autre infraction, le score donné *a priori* par l'algorithme ne ferait que conforter l'avis d'un jury, du moins appuierai les éléments de poursuite de la police et du procureur.

Et ce qui conforte les poursuites menées à charge réduit forcément les chances de défense du suspect. Celle-ci peut de son côté engager des enquêteurs privés, les investigations menées par la police américaine ne servant qu'à la partie poursuivante … Or, comment contredire, même au moyen d'une contre-enquête, des résultats chiffrés par un algorithme policier ? Si PredPol reçoit une certaine certification de fiabilité en ce qu'il est utilisé par des autorités officielles, quelle chance donner au suspect pour se défendre face à une machine censée être neutre et impartiale ? Bien qu'une investigation telle que celle de *Pro Publica* puisse remettre en cause la légitimité de ces algorithmes, de tels éléments n'ont en principe aucune valeur juridique au prétoire.

Au mieux, la police prédictive peut servir l'enquête dans un cas tel que celui de Memphis avec le logiciel *Blue CRUSH* ayant permis de démanteler un réseau de drogues et de prostitution. Ce logiciel n'ayant visé que des quartiers, ne se focalisant pas sur les individus en soit, il a éveillé l'attention professionnelle de la police sur certaines zones de la ville. L'algorithme n'a ici fait que guider les enquêteurs, leur donner une piste potentielle ; l'instinct policier et le professionnalisme a fait le reste, et ce sans jouer avec les limites des droits et libertés des personnes suspectes.

[148] Cf *supra* n°106

117. *Reasonable doubt* - L'intelligence artificielle prédictive pourrait donc être efficace dans l'enquête surtout lorsqu'elle prend la forme de techniques algorithmiques géographiques ou spatiotemporelles. Au niveau local, ces techniques pourraient être bénéfiques pour les polices d'État situées dans les villes, afin de détecter des chaînes d'activité criminelle, ou tenter de réduire le taux de commission de certaines infractions dans des zones déterminées. L'enquête sous-entend aux États-Unis une recherche d'éléments incriminant le suspect. La multiplication des éléments à charge a pour but de mener à son arrestation, qui sera dès lors fondée sur un « doute raisonnable »[149]. En d'autres termes, l'arrestation n'est pas censée être totalement arbitraire et basée sur un simple doute, mais bien sur une intime conviction étayée par les preuves pénales collectées.

Se pose alors la question de la valeur d'un élément à caractère prédictif : pourrait-il fonder l'intime conviction ? Peut-il être qualifié de preuve en tant que telle ? La valeur probante d'un indice ou d'un élément utilisé à l'audience par le procureur (*prosecutor*) prend toute sa dimension du fait du travail policier effectué en amont, durant l'enquête. L'apport d'un résultat algorithmique prédictif lors de l'audience pourrait être à double tranchant aux États-Unis. Soit l'algorithme inspire encore la méfiance au jury et aux différents acteurs du procès, dès lors les biais possibles pourraient être évités, mais on accorde alors le bénéfice du doute aux policiers eux-mêmes. Dans une hypothèse alternative, les chiffres apportés par le logiciel et appuyant les preuves de la police contre l'accusé pourraient au contraire être pris comme nécessairement vrais et impartiaux et le condamner avant même que sa défense ne soit présentée …

Finalement, le plus gros impact que pourrait avoir la police prédictive dans la phase d'enquête américaine, serait sur les droits du suspect et sur le renforcement des pouvoirs conférés à la police et au procureur en matière de poursuites. Néanmoins en matière de travail policier pur, les agents pourraient avoir à adapter leur travail voire même leurs attributions et savoirs professionnels à l'introduction d'algorithmes prédictifs. Bien que travaillant avec des analystes du crime, il est évident qu'il faut un minimum de savoirs scientifique et informatique pour pouvoir se familiariser pleinement avec ces logiciels. Or, si certains modèles prédictifs pourraient permettre des économies quant aux effectifs policiers, les dépenses pourraient toucher tout ce qui entoure

[149] *Reasonable doubt*

l'introduction de ces méthodes : nouveau matériel, éducation, formations, nouveaux types d'emplois et de spécialisations.

Dans plus d'une cinquantaine de villes des États-Unis, la police a dû s'adapter et intégrer le logiciel PredPol à ses habitudes de travail. Bien que ce dernier a largement fait sa place dans les commissariats qui l'utilisent, les conséquences post travail policier ne se font pas encore totalement ressentir sur le procès. Mais les enjeux sont grands et il semblerait indispensable de les anticiper. Bien que la police prédictive n'ait pas encore fait sa place en Europe comme elle a pu la faire aux États-Unis, certaines États ont cependant commencé à l'accueillir. Il conviendrait donc d'anticiper là aussi les conséquences d'une transposition de ces techniques.

B. Les conséquences d'une éventuelle transposition européenne

Les enjeux d'une importation de la police prédictive en Europe – bien que certains États la testent déjà – sont tant d'ordre juridique, que politique et sociétal. Effectivement, certains pays européens tentent déjà une expérimentation de logiciels prédictifs sur leur sol, et la France en fait partie. Cette implantation n'en est encore une fois qu'au stade d'expérimentation et ne doit pas avoir d'impact sur la manière de travailler de la police, il ne s'agit donc pour l'instant que d'analyse.

La privatisation de la sécurité et des moyens de police est une des inquiétudes de l'Europe vis-à-vis de la police prédictive. Aux États-Unis, le système policier est bien différent de celui en Europe ; bien que chaque État européen ait sa propre organisation pénale et policière, on ne trouve pas de réelle similitude au système fédéral américain dans l'Union européenne. Ainsi, bien que la sécurité soit aussi d'ordre public pour l'État américain, chaque État voire chaque ville a sa propre police, avec sa propre organisation et ses propres moyens. A ce titre, une ville américaine est libre de choisir de privatiser certaines de ses techniques. En France, une telle configuration est difficile à concevoir ; le commissariat d'une ville ne pourrait décider arbitrairement d'utiliser un nouvel outil géré par une société privée.

118. Logiciels privés - Il ne faut cependant pas s'y méprendre : la plupart des logiciels développés à des fins policières sont en majeure partie créés par des entreprises privées. *Anacrim*, programme ayant récemment permis de relancer l'affaire dite

« Grégory », a par exemple été créé par une société spécialisée dans la recherche et le développement d'outils informatiques et d'analyse militaire, de renseignements et de sécurité. Une fois présenté et adopté par le Gouvernement français, le logiciel est manipulé par certains commissariats déterminés, l'utilisation encadrée. L'algorithme n'a en effet servi que pour peu d'affaires, comme l'affaire Grégory ou l'inculpation de Francis Heaulme. Il n'est pas automatiquement utilisé.

Si l'on pousse l'idée jusqu'au bout, l'introduction de méthodes prédictives par des personnes morales de droit privé pourrait petit à petit se généraliser au territoire européen, ces personnes morales ayant intérêt à vendre leurs savoirs et techniques brevetées dans chaque État. Non pas qu'une telle hypothèse est à proscrire fermement, mais il faudrait ainsi imaginer cette généralisation comme celle de l'industrie pharmaceutique par exemple. Dans une moindre mesure, si la privatisation de la sécurité venait à se développer – d'abord avec la police prédictive – elle pourrait presque devenir une industrie et un lobby.

D'un côté, la recherche en matière d'anticipation du crime et de renforcement des techniques de sécurité pourrait être bénéfique pour les États. Mais à quel prix pour les libertés et droits individuels, les principes juridiques et judiciaires de chaque État ? Un tel développement et une telle hypothèse ne seraient pas totalement inimaginables aux États-Unis, mais le système européen aurait tendance à anticiper beaucoup plus un tel cas de figure, voire même à l'empêcher. Une certaine privatisation des techniques informatiques est à prévoir dans le cas où la police prédictive ferait sa place dans les commissariats, mais on ne pourrait pas aller jusqu'à une privatisation de la police en elle-même. D'autant plus qu'en France, ces techniques pourraient être disponibles tant pour la police que pour la gendarmerie, cette dernière dépendant de l'armée. On parlerait alors d'une introduction de la police prédictive à un niveau un peu plus élevé, qui est cependant une autre problématique[150].

119. Police prédictive européenne - En Europe, les villes expérimentant des logiciels de police prédictive ne se basent d'ailleurs pas sur des données personnelles. Aucune ne se risque pour l'instant à tester les méthodes prédictives de profilage ou de scores. Dans la majorité des cas, si ce n'est dans tous les cas, ce sont les méthodes d'analyse de terrain et de temps qui sont à l'œuvre dans certains commissariats. En

[150] Cf *infra* n°126

Allemagne par exemple, un système algorithmique a été mis au point, nommé *Precobs*[151] – clin d'œil aux *Precogs* de Philip K. Dick – dans plusieurs villes. Cependant l'État met un point d'honneur à ce que ces logiciels n'aient pas d'impact substantiel sur le travail policier habituel – il ne faut pas que la prédiction prenne pour l'instant le dessus sur l'enquête, le travail de terrain et la chaîne pénale, au risque d'atteintes ou de faire dévier les pratiques policières. L'Europe n'oppose pas un non définitif à la police prédictive, mais reste toujours méfiante. On en veut pour preuve l'anticipation d'atteintes éventuelles à certains droits avec le RGPD et la directive l'accompagnant – un cadre législatif serait nécessaire dans l'UE avant même d'envisager d'implanter réellement des algorithmes prédictifs dans les États.

Si l'on prend l'exemple de la France, l'utilisation d'un algorithme prédictif dans les commissariats pourrait dénaturer l'enquête. Celle-ci repose principalement sur une dualité : l'enquête préliminaire et l'enquête de flagrance. La police prédictive pourrait éventuellement servir dans une enquête préliminaire, notamment si on utilise une méthode spatiotemporelle. Les analyses et résultats donnés par le logiciel pourraient permettre de cibler certains lieux et ainsi permettre par exemple aux officiers de police judiciaire d'interroger les personnes du voisinage. Néanmoins, l'utilisation de la police prédictive pourrait être problématique voire dangereuse en ce qui concerne l'ouverture d'une enquête de flagrance.

Un arrêt de 1953[152] a permis de dessiner les contours de cette enquête de flagrance en retenant la notion « *d'indices apparents d'un comportement délictueux* ». Mais là où la jurisprudence a précisé les limites de la notion de flagrance, l'utilisation d'algorithmes prédictifs pourrait l'élargir. En effet, si le système prédictif s'avère particulièrement précis et efficace, comment ne pas lui faire confiance ? La flagrance pourrait dès lors être élargie dans la pratique, à des indices de comportements délictueux donnés par l'intelligence artificielle. On perdrait alors le terme « apparent » de la jurisprudence de 1953, qui prenait tout son sens.

Face à tous ces biais possibles et avérés, la police prédictive attise autant de méfiance qu'elle n'inspire la confiance. Néanmoins une bonne utilisation de ces techniques ne peut se faire qu'en comprenant la philosophie existant en réalité derrière l'initiative prédictive.

[151] *Pre Crime Observation Systems*
[152] Cass. Crim., Arrêt Isnard, 22 janvier 1953

En effet, les théories derrière la police prédictive ont avant tout vocation à servir le travail policier.

§2 : L'intelligence artificielle au service de l'organisation policière

La vocation de proactivité des logiciels prédictifs est certes mise en avant par leurs programmateurs, mais ne font pas toujours leurs preuves, la volonté de prédiction prenant le dessus. Certains développeurs se sont donc attelés à une mission particulière : créer un algorithme certes prédictif, mais qui est avant tout programmé pour analyser le travail d'intervention de la police (A). Au vu de l'engouement que peut inspirer ces techniques prédictives, les gouvernements et services de renseignements ne sauraient tarder à être attirés par une éventuelle utilisation au niveau national (B).

A. Un modèle « responsable »[153] de police prédictive

Les développeurs de techniques de police prédictive tentent jusqu'ici de se rapprocher le plus possible d'un idéal de lutte contre la criminalité : la prévision de celle-ci. Néanmoins l'évaluation faite de ces techniques par le groupe RAND a souligné certains pièges dans lesquels il ne faudrait pas tomber en tentant par-dessus tout de prédire le crime. Parmi ces pièges, celui dans lequel la majorité des analystes et commissariats sont en train de tomber : se concentrer plus sur la précision de la prédiction que sur l'utilité stratégique qu'elle représente. Car il faut le rappeler, la police prédictive n'a pas pour vocation première de dire quel sera le prochain crime et où il aura lieu, mais bien d'analyser des données afin d'améliorer le travail d'anticipation de la police.

120. Chiffre *versus* efficacité - Le RAND Report donne l'exemple d'un outil prédictif utilisé en Irak qui avait pu prédire la probabilité d'un attentat à Mossoul dans les prochaines 48 heures[154]. L'information était en effet extrêmement précise en termes d'analyse, mais n'avait néanmoins aucune « valeur stratégique »[155] au sens des autorités compétentes. L'autre exemple donné est celui de l'analyse géographique des cambriolages à Washington D.C. qui donnait une carte colorée du jaune au rouge des

[153] H. GUILLEAU, « Vers une police prédictive responsable ? », 2017, disponible électroniquement : http://www.internetactu.net/2017/07/26/ou-en-est-la-police-predictive/
[154] RAND Report, *op. cit.* note 97, p. 119
[155] *Ibid,* « *Tactical value* »

zones à risque[156]. Bien que l'analyse soit là aussi très juste, il en résultait que plus des deux tiers de la ville étaient déclarés comme à haut-risque. Or, constater qu'une large portion de la ville est susceptible de cambriolages n'a presque aucune utilité pour la police en matière d'organisation et de stratégie sur le terrain.

Le rapport suggère en fait qu'il faudrait que les logiciels de police prédictive soient moins orientés vers la « sur-prédiction » et plus vers des techniques prenant en compte les réponses à donner face à ces risques prédits. Il faudrait donc dans une certaine mesure que les algorithmes intègrent le facteur policier en soit, les données propres à l'action et l'organisation des commissariats. Ainsi, la police prédictive prendrait tout son sens et serait réellement utile aux officiers agissant directement sur le terrain.

121. *HunchLab* - C'est notamment le but qui a été attitré au système *HunchLab*, logiciel de police prédictive utilisé aux États-Unis. Ce logiciel ne fonctionne pas sur le même modèle que PredPol. Le site internet même de HunchLab le qualifie en effet de « *système connecté de gestion proactive des patrouilles [policières]* »[157] qui a pour but non pas uniquement d'anticiper les infractions mais aussi de trouver un meilleur moyen de répondre à celles-ci. A ces fins, il faudrait notamment, selon les développeurs de HunchLab, que la stratégie policière prenne en compte les priorités de la communauté. C'est là que le logiciel intervient : en mêlant ces différents types de données, le résultat n'est pas centré uniquement sur la prédiction mais surtout sur l'efficacité de l'action policière dans la ville.

122. Rapports police-communauté - On trouve donc cette notion de lien entre la police et la communauté qui l'entoure, qui est son cadre de travail. L'importance du lien entre ces deux acteurs de la ville à des fins d'efficacité de la lutte contre la criminalité est de plus en plus présente dans la réflexion sur la police prédictive. C'est un des points qu'il paraît urgent d'intégrer dans ces techniques, au vu de leur développement croissant. Les premiers séminaires américains sur la police prédictive, de 2009 et 2010, avaient en effet mentionné cette nécessité[158].

[156] La couleur jaune représentant un risque faible, l'orange un risque moyen et le rouge un risque élevé
[157] « *Web-based proactive patrol management system* », disponible électroniquement : https://www.hunchlab.com/
[158] *Predictive Policing Symposiums*, National Institute of Justice, 2009 et 2010

La police prédictive, si elle est correctement utilisée, aurait vocation à améliorer les relations entre les forces de l'ordre et les individus ; bien que les techniques ne produisent pas toujours des chiffres satisfaisants, le critère de la neutralité de la machine pourrait avoir un effet rassurant pour les citoyens de la ville. Les exigences imposées par les textes qui encadreraient l'utilisation de ces algorithmes permettraient d'assurer une pleine transparence de la police sur son travail et les données utilisées, tissant là aussi un lien privilégié entre la police et les individus. Tout ceci à la condition, il faut le rappeler, que la police prédictive soit utilisée dans un cadre législatif stricte, qu'elle soit contrôlée et que la formation de ses utilisateurs soit adaptée.

123. Rapport police-professionnels - La notion de « communauté » ne comprend pas uniquement les individus de la ville mais aussi les professionnels entourant tout le travail pénal et donc le travail policier. Bien que développés à destination des commissariats, les algorithmes prédictifs devraient aussi être ouverts à tous ceux qui touchent de près ou de loin à la chaîne pénale ; et notamment ceux ayant trait à la réinsertion, en charge des individus en semi-liberté, en libération conditionnelle etc. Ce qui implique aussi la prise en compte des experts tels que les psychiatres. L'idée n'est pas de permettre l'utilisation de la police prédictive à tous les professionnels du monde judiciaire, mais plutôt de leur accorder un droit de regard sur les débats et problématiques l'encadrant. Qu'importe la technique utilisée, il s'agit à termes de traiter du sort de l'individu ; toutes les personnes que ce dernier est susceptible de rencontrer dans un cadre pénal devraient pouvoir être impliquées dans le processus prédictif. Car ce dernier n'a pas uniquement un impact sur l'avenir immédiat de la criminalité, mais peut en avoir un sur tout le futur judiciaire d'une personne.

La philosophie de HunchLab part donc de ce principe : les logiciels et l'intelligence artificielle peuvent certes être très utiles à la police, mais ils peuvent vraiment faire la différence dans le travail policier en intervenant sur les stratégies à adopter, pas seulement en donnant des analyses prédictives. Ce sont bel et bien les configurations de l'action policière qui doivent évoluer ; si l'IA prend en compte cette variable-là, les résultats pourraient être plus intéressants en matière d'efficacité. Car ne donner qu'une prédiction ne change pas substantiellement la manière dont la police va répondre à la menace. HunchLab se pose alors comme le concurrent principal du géant PredPol.

124. Fonctionnement de HunchLab - Les programmateurs de HunchLab travaillent dans l'optique selon laquelle la prédiction est finalement simple à établir, mais qu'elle ne devrait pas primer. La première étape est celle de la prédiction : comme tout autre algorithme prédictif, il établit après brassage et agrégation de données, une cartographie des zones où un type d'infraction pourrait être commis – HunchLab utilise les techniques prédictives de *hot spot* et spatiotemporelles. Néanmoins, à la différence des méthodes classiques de *crime mapping*, cet algorithme ne fournit pas une évaluation graduée du risque représentée par chaque zone : la prédiction n'est pas la priorité.

L'analyse ne s'arrête pas là, cette première étape n'est en fait que préliminaire. La deuxième étape consiste en la proposition aux utilisateurs – les policiers – d'une technique d'action en fonction de la zone choisie. Le but est alors que les agents reportent ensuite leur travail au logiciel : quelle méthode d'action ils ont finalement adoptée, quand, où exactement etc. Enfin, le logiciel produit un formulaire post-intervention, composé de questions auxquelles les policiers étant intervenus doivent répondre. L'intelligence artificielle est ici dotée de l'apprentissage autonome : ces données reportées sont enregistrées et intégrées, pour une analyse et des résultats futurs encore plus adaptés.

Un tel système logiciel représente un tout autre enjeu pour ses utilisateurs, qui sont alors des participants à part entière au développement du système. Pour que ce dernier les aide dans leur travail, il faut qu'eux-mêmes participent à son amélioration. La police prédictive est de manière générale la bienvenue dans les commissariats, en ce qu'elle pourrait être d'une grande aide et allègerait la police de certaines tâches chronophages – à l'image de l'analyse du Big Data. Mais il ne faut pas que la prédiction prenne le pas sur l'efficacité des officiers et agents ; elle doit aller de pair avec la mutation de leur travail. HunchLab propose donc une alternative au *predictive policing* qui est plus que souhaitable comparé à PredPol par exemple. On sort de la politique du chiffre – prédire pour mieux réduire – pour aller vers une politique participative d'efficacité et de proactivité.

Dans une interview au journal *Le Monde*, le créateur de HunchLab, Jeremy Heffner, précise que son logiciel a tout de même des biais, dont certains auxquels il a su palier[159]. En effet même si le système de *crime mapping* utilisé ici ne fait pas apparaître de graduation du risque criminel, l'algorithme a tout de même tendance à envoyer les

[159] H. GUILLEAU, *op. cit*, note 153

patrouilles vers des zones présentant un risque élevé. Ayant travaillé au développement de ce système avec les officiers de police eux-mêmes, Jeremy Heffner a intégré une part d'aléa dans l'analyse algorithmique. Celle-ci se rapproche ainsi plus du rationnel, s'éloigne un peu du côté perfectible de la machine, afin de s'apparenter à la réflexion professionnelle de la police et, surtout, pour exclure toute surinterprétation de la part des utilisateurs.

125. Transparence du logiciel - Jeremy Heffner s'attache également à ce que son logiciel reste transparent sur les données utilisées, sur son fonctionnement, ses résultats… Il travaille en effet pour l'entreprise privée *Azavea*, une « B Corp ». La « B Corporation » est une certification accordée à certaines entreprises ou entités privées dites « citoyennes » : bien qu'à but lucratif, elles agissent pour l'intérêt général, et répondent donc à des exigences strictes dans le travail qu'elles effectuent – au risque de perdre cette certification. C'est le cas d'*Azavea*, entreprise qui crée des systèmes d'analyse géographique à des fins citoyennes et d'intérêt général. On comprend donc bien qu'HunchLab doit impérativement répondre à des critères légaux, de transparence et de pédagogie. Une philosophie qui a pour vocation d'éviter la marchandisation de ces logiciels prédictifs alors même qu'ils sont censés agir pour une cause étatique et publique. C'est justement ce caractère d'aide au maintien de l'ordre public qui pourrait attirer les autorités supérieures de l'État, comme les renseignements, et les pousser à utiliser la police prédictive au niveau national.

B. L'algorithme prédictif au service des renseignements

126. Extension du local au national - Les algorithmes de police prédictive ont pour l'instant été utilisés au niveau local, sur les zones d'attribution des commissariats, et ne s'étendent pas plus loin que le périmètre de la ville. On peut voir qu'avec l'exemple de HunchLab, les développeurs et les analystes travaillent à son amélioration, prenant en compte les obstacles et problématiques rencontrés par les systèmes existants. Au vu des résultats parfois satisfaisants offerts par la police prédictive, il est sans aucun doute envisageable que son utilisation attire l'attention des niveaux supérieurs de la sûreté : l'État fédéral pour les États-Unis par exemple, ou le gouvernement et les renseignements de manière plus générale.

Or, le risque est ici de confondre travail policier et travail des renseignements. Les enjeux sont d'autant plus importants qu'ils sont décuplés si la police prédictive s'applique à l'ensemble du territoire d'un pays. Il faut envisager ici un nombre de données encore plus conséquent, un traitement de celles-ci à des fins bien plus complexes que celles d'un commissariat. Le fait que la police prédictive ne soit utilisée qu'à l'échelle des agglomérations n'est pas un hasard : plus la zone à analyser est étendue, plus le travail est complexe et le risque d'imprécisions probable.

Là où le Big Data et l'intelligence artificielle commencent à faire leur place dans le travail interétatique de lutte contre la criminalité organisée[160], il serait nécessaire de d'abord étudier leur place au niveau territorial. Car si PredPol ou HunchLab n'utilisent que certains types de données[161], les services de renseignements auraient vocation à explorer non pas certains mais tous types de données. Autrement dit, au vu du statut de ces services et du but poursuivi par leur travail, ils pourraient avoir accès non seulement à des sources peu fermées[162] mais aussi à énormément de fichiers pénaux, dont la consultation est à la base encadrée. On pourrait même envisager que les données dites « virtuelles »[163] puissent aussi être traitées, et l'accès à celles-ci facilité dès lors que l'objectif est celui de la sécurité nationale.

127. Projet prédictif national - L'idée n'est en fait pas si extravagante. En effet, une enquête Médiapart a révélé en 2015 que le Service central de renseignements criminel de la gendarmerie nationale travaillait avec l'Institut Mines-Télécom et le groupe industriel Safran à la création d'une intelligence artificielle prédictive, dotée de l'apprentissage autonome, et ce à des fins nationales et non pas locales. « *La description du projet laisse imaginer un dispositif visant à prédire l'apparition de phénomènes criminels sur l'ensemble du territoire, afin de mieux répartir les moyens des forces de l'ordre* »[164], description d'ailleurs conforme à l'idée que l'on se fait jusqu'ici de la police prédictive. Reste à savoir quelles données pourraient être utilisées, quelles techniques algorithmiques seraient programmées, et si plusieurs seraient utilisées. Des algorithmes prédictifs ayant été testés dans certains commissariats français, tel que celui de Cergy-Pontoise, l'idée de l'utilisation de logiciels prédictifs au niveau local n'apparaît pas

[160] Cf *infra* n°163 et n°166
[161] Données principalement géographique, météorologiques, temporelles …
[162] Telles que les sources Insee, sources issues de l'ONDRP …
[163] Cf *supra* n°67
[164] J. HOURDEAUX, « Gendarmes et industriels imaginent un nouveau logiciel pour prédire le crime », *Médiapart.fr*, 25 mai 2015

totalement nouveau aux yeux de la police judiciaire. Mais le projet « *Horizon* » ou « *Anticirime* », noms potentiels du système, aurait vocation à s'appliquer à l'ensemble du territoire.

128. *Palantir Technologies* - Les industriels, spécialistes et analystes travaillant pour des entreprises privées n'ont en effet pas perdu de temps dès les prémices du *predictive policing*. Là où certains se sont attelés à améliorer les techniques existantes dans les agglomérations, d'autres ont vu dans cette révolution technologique une opportunité de développement à un échelon encore plus élevé. L'entreprise *Palantir Technologies* fait partie de celles qui ont eu vocation à créer des logiciels prédictifs non seulement pour le niveau local, mais aussi pour le niveau fédéral voire les services de renseignements. Cette société est spécialisée dans l'analyse du Big Data et l'élaboration de systèmes informatiques dans une grande variété de domaines dont entre autres l'industrie automobile, les assurances, les réseaux sociaux et internet, le milieu de l'entreprise, les renseignements, l'application de la loi. Palantir construit pour chaque domaine un système logiciel spécifique de traitement et d'analyse des données. Parmi ces domaines donc, les renseignements, l'application de la loi, la défense ; pour chacun d'eux est prévu un algorithme adapté.

Le nom de l'entreprise fait d'ailleurs référence à une création de Tolkien : dans ses livres, le *palantir* représente une boule de cristal permettant de voir tout le temps, partout. Une référence un peu sombre, quand on sait que Palantir est extrêmement utile aux autorités publiques.

129. Contrat avec les autorités nationales - C'est ainsi que Palantir travaille depuis plusieurs années avec la police fédérale, les services de défense et de renseignements américains[165]. La société a su faire ses preuves tant aux yeux d'entreprises privées, de cabinet d'avocats, de sociétés d'assurance ou pharmaceutiques et ne manque donc pas de financement. Tant et si bien que depuis 2016, la France a fait appel à ses services et obtenu un contrat entre Palantir et la Direction générale de la Sécurité intérieure (DGSI). Bien loin de l'optique américaine, la DGSI souhaite utiliser la technologie Palantir afin de faciliter le « tri » des données traitées dans la lutte antiterroriste. L'ambition n'est donc pas encore à l'heure de la police prédictive.

[165] CIA, FBI, NSA, US Marines, US Air Force …

Une ambition que les autorités de Nouvelle-Orléans ont cependant eu dès 2012. C'est en effet depuis cette date que l'État américain a conclu un contrat avec Palantir afin de développer et utiliser une technologie de police prédictive. Or il s'avère que le contrat est resté secret jusqu'en 2018 : en mars dernier, un média journalistique et d'investigation américain a révélé cet accord existant depuis maintenant 6 ans, sans même que la mairie de Nouvelle-Orléans ne soit au courant[166]. Pourquoi cacher l'utilisation d'un logiciel prédictif alors même que PredPol fait fureur dans les autres agglomérations du pays ? Le contrat n'était en fait basé en 2012 que sur l'expérimentation de l'algorithme, en vue d'une commercialisation de plus grande ampleur.

L'efficacité des technologies prédictives de Palantir est encore à prouver, néanmoins à consulter le site internet de la société, elle semble avoir solution à tout problème pouvant être rencontré par un gouvernement, notamment en matière de sécurité. Il semblerait donc que son but soit désormais de développer et améliorer la technologie prédictive à des fins de renseignements et de couverture nationale. L'exemple de Palantir, qui semble être efficace au point d'être vendu dans plusieurs États différents sur la planète, montre bien qu'il est nécessaire d'encadrer strictement de telles éventualités de commercialisation de la police prédictive.

En effet si par exemple le logiciel « *Palantir Intelligence* » était commercialisé auprès des renseignements français et américains, il faudrait évidemment s'assurer d'une indépendance stricte des deux systèmes, sans risques de piratage Internet par exemple, ou de lien entre les deux plateformes de renseignements … Il est certain que ce type de technologie et d'entreprise ne se risquerait pas à ces éventualités, néanmoins il faut garder à l'esprit qu'il s'agit toujours de technologies nécessitant la plupart du temps une interface informatique et un réseau internet, faisant courir le risque d'un potentiel piratage ou bug technique.

L'inclusion, petit à petit, de sociétés privées dans l'équation renseignements-Big Data, fait donc apparaître de nouvelles problématiques. C'est effectivement en faisant entrer un nouvel acteur en jeu dans la lutte contre la criminalité, qui plus est privé, que le risque d'atteintes et de biais est à envisager. Si un commerce de la prédiction policière venait à

[166] A. WINSTON, « Palantir has secretly been using New Orleans to test its predictive policing technology », *The Verge*, 27 février 2018, disponible électroniquement : https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd

se développer, on pourrait presque imaginer l'apparition d'un lobby dans ce secteur aux États-Unis par exemple, pays étant partisan d'un tel système. Les répercussions, alors même que la CIA et la NSA n'inspirent pas toujours la confiance des citoyens américains, pourraient être d'autant plus graves.

Les autorités des pays ayant intégré la police prédictive dans leurs commissariats ont dû s'adapter à ce nouvel outil de travail ; celui-ci ayant pour vocation d'améliorer le travail policier. Si les techniques de police prédictive font leurs preuves le jour où elles se démocratiseront, les autorités supérieures comme les services de renseignements ne tarderont pas à manifester un intérêt envers l'utilisation de ces techniques. Mais bien que la police prédictive ne soit censée impacter que le travail policier, son utilisation pourrait influer sur tout le procès pénal, voire même la phase post-sentencielle.

Section 2 : L'adaptation des acteurs du système pénal à la police prédictive

Si l'impact est avéré sur le travail des forces de police, il n'est pas aussi évident quant au reste de la chaîne pénale. Mais l'introduction de la police prédictive dans les commissariats n'impacterai pas uniquement le travail de la police. Les autres professionnels judiciaires devraient prendre en compte ces résultats algorithmiques (§1). Or, si la police prédictive venait à avoir une influence sur le travail policier et sur celui des magistrats, elle en aurait surtout une sur le mis en cause lui-même (§2).

§1 : Les enjeux éventuels pour les acteurs judiciaires

La politique pénale, bien qu'appliquée par les acteurs de la chaîne judiciaire, est conduite avant tout par le Garde des Sceaux. Celui-ci devrait potentiellement prendre en compte l'utilisation de la police prédictive si elle venait à être introduite sur le territoire (A). L'influence n'en serait que plus grande sur le travail des magistrats (B).

A. Les enjeux pour la politique pénale

130. Place du pouvoir exécutif - Parler de la politique pénale d'un État renvoie nécessairement au pouvoir exécutif ; cette politique trouve son origine dans le Gouvernement. En France, c'est le Garde des Sceaux, Ministre de la Justice, qui est

chargé de mener la politique pénale sur tout le territoire français. L'article 30 de la Constitution détermine ainsi ses attributions : « *Le Ministre de la Justice conduit la politique pénale déterminée par le Gouvernement. Il veille à la cohérence de son application sur le territoire de la République* »[167]. Néanmoins, il peut paraître surprenant d'évoquer le pouvoir exécutif dans un paragraphe traitant des « acteurs judiciaires » ; en France, la DDHC, en son article 16, prévoit le principe de séparation des pouvoirs.

Ce sous-paragraphe n'a certainement pas vocation à remettre en cause cette séparation, mais à considérer l'impact que pourrait avoir la police prédictive dans l'hypothèse où celle-ci serait introduite sur tout le territoire français. Bien que ne faisant pas partie intégrante de la chaîne pénale, celle-ci étant menée par le pouvoir judiciaire, l'exécutif à son rôle à jouer dans la conduite de la politique pénale et sécuritaire de la Nation. Ainsi l'introduction des méthodes de police analytique et prédictive auraient sans aucun doute un impact sur la politique pénale.

131. Éthique - Les premières préoccupations que devrait avoir le Gouvernement vis-à-vis de la police prédictive sont les préoccupations éthiques qu'impliquent l'utilisation de l'intelligence artificielle, les préoccupations de surveillance et de protection des données des citoyens. La France, il faut le rappeler, est un État qui se préoccupe particulièrement de la protection de ces données personnelles. Conscients des enjeux que présentent le Big Data, les différents gouvernements se succédant, et ce qu'importe leur bord politique, semblent s'y adapter constamment, en modernisant les textes existants et les réformant, pour plus de protections, tout en restant ouverts à la circulation des données. Pour obtenir de bons résultats, il est impératif de s'assurer de la qualité des données utilisées, d'entretenir la transparence des systèmes, et d'informer les citoyens du comment, pourquoi, et des fins poursuivies.

132. Surveillance - Néanmoins l'introduction de la police prédictive au niveau national implique nécessairement un accroissement de la surveillance, du type et nombre de données collectées, et donc une menace grandissante pour le droit à la protection des données personnelles. Car dans le cas de la police prédictive il n'est plus question de problématiques de traitement des données rencontrées par les entreprises privées et réseaux sociaux, mais bien du pouvoir politique, de surveillance. Le risque est toujours

[167] Article 30 de la Constitution de 1958

celui d'une mauvaise utilisation de l'intelligence artificielle, que la police prédictive tombe entre de mauvaises mains. C'est à ce titre que la politique pénale et le Gouvernement se devraient d'être extrêmement attentifs et exigeants avec les autorités utilisant dans un futur potentiel la police prédictive. Un organe de contrôle tel que la CNIL ne serait peut-être pas suffisant ; du moins, il faudrait y attacher un comité d'experts ne travaillant qu'au contrôle des activités de police, pénales, de sécurité et de sûreté, et ce tant au niveau local qu'étatique.

Les nouveaux textes européens entrant en vigueur le 25 mai 2018 sont cependant la preuve du renforcement de la protection des données personnelles des citoyens, et ce même vis-à-vis des autorités publiques. Certaines problématiques restent en suspens, notamment celles liées au terrorisme, qui doivent évoluer et être traitées dans cette ère du Big Data et de l'intelligence artificielle. Tout doit être fait pour éviter que la surveillance étatique prenne le pas sur les libertés individuelles.

133. Budget - L'introduction de la police prédictive implique aussi sans aucun doute une question budgétaire pour la politique pénale et le Gouvernement. En effet, bien qu'allégeant visiblement les policiers de certaines tâches et permettant de rééquilibrer les effectifs, pour éviter toute imprécision algorithmique, la technologie utilisée se doit d'être performante et donc certainement coûteuse. Le rapport de la *RAND Corporation* souligne néanmoins que ceci est un des mythes attachés à la police prédictive : le système utilisé doit être particulièrement puissant et complexe, et donc cher, pour être efficace[168]. En effet, si la police prédictive s'utilise au niveau local, et que des techniques telles que celles de *crime mapping* ou de *hot spot* sont utilisées, une telle technologie de pointe n'est pas nécessaire pour être précise. Les résultats peuvent être convaincants si la programmation est bien faite. Cette idée est concevable.

Or, deux failles s'ouvrent devant ce mythe trompeur, qui peut se transformer en véracité. Premièrement, la police prédictive peut certes être utilisée uniquement au niveau d'une agglomération, d'une ville : mais quid de la taille de cette ville, et surtout de son taux de criminalité ? Ces facteurs ont forcément un impact sur le niveau de précision de la technologie utilisée, et donc sur le budget nécessaire. Il en est de même si l'intelligence artificielle prédictive est envisagée dans un contexte de renseignement national, les

[168] RAND Report, *op. cit* note 97, p.118

processeurs et algorithmes utilisés se devraient d'être très puissants et donc particulièrement chers.

Mais surtout, tout logiciel, qu'il ait une dimension locale ou nationale, se doit d'être extrêmement bien protégé. L'État ne peut garantir une protection juridique des données de ses citoyens sans protéger ses propres logiciels contre tout piratage ou intrusion. Surtout quand on sait que le développement des nouvelles technologies s'accompagne parallèlement du développement de la cybercriminalité. Le budget n'est pas à négliger en matière de police prédictive : le coût pourrait dans certains cas être proportionnel à l'efficacité et à la sécurité du système.

Ainsi, le premier rôle du pouvoir exécutif, si la police prédictive venait à être utilisée sur le territoire français, serait de travailler avec le législateur à des lois encadrant strictement le traitement des données dans ce cas spécifique, l'utilisation des différentes techniques et ses limites, et d'assurer une protection informatique irréprochable aux logiciels mis en œuvre – bien que le risque zéro n'existe pas.

134. Politique du chiffre - La politique pénale de manière générale se caractérise par des réformes de la loi, de la procédure, des études du travail des professionnels et acteurs du système judiciaire. Toutes ces mesures sont en fait mises en œuvre dans un but qui est implicitement admis : la baisse de la criminalité. La lutte contre la criminalité se traduit souvent pour la politique pénale par l'évolution des chiffres relatifs à la commission de certaines infractions, aux résultats obtenus par les commissariats …

Or, il ne faudrait pas qu'en adoptant les techniques de police prédictive, les autorités publiques ou les commissariats comptent aveuglément sur celles-ci. Le risque est en effet de développer une certaine dépendance ou de trop compter sur le travail analytique et prédictif de l'intelligence artificielle pour faire baisser le chiffre du crime. C'est l'un des « mythes » souvent cités à propos de la police prédictive : elle fait systématiquement baisser les chiffres de la criminalité et de la délinquance[169]. Par exemple, si la politique pénale se concentre sur la lutte contre le trafic de stupéfiants, le risque serait de demander à tous les commissariats du territoire travaillant avec un algorithme prédictif de le programmer de telle sorte qu'il se focalise spécifiquement sur les infractions relatives à ce trafic. Ou encore que, dans cette optique de lutte contre le

[169] A titre d'exemple : RAND Report, *op. cit.* note 97, p. 118

trafic de drogues, la police intervienne automatiquement dans les zones qualifiées à risque par la machine ; sans examiner les facteurs et données utilisés derrière.

Un mauvais usage, une mauvaise connaissance et une interprétation biaisée des résultats prédictifs peuvent à coup sûr être contre-productifs. Le tout serait que l'intégration de la police prédictive dans le travail pénal ne développe pas une politique du chiffre et un besoin pressant de résultats, simplement parce qu'on a affaire à une machine.

Enfin, intégrer la police prédictive dans le système et la politique pénale implique d'adapter aussi les moyens existants et de former les acteurs du système judiciaire. Bien que souvent, les algorithmes soient programmés et créés par des spécialistes, des scientifiques, des sociétés privées, il serait nécessaire que ces spécialistes forment les professionnels du système pénal au contact des algorithmes. Cela permettrait à la police par exemple de pleinement comprendre les facteurs analysés par la machine, les types de données traitées et donc les analyses ressortant de la prédiction. Une pleine compréhension de l'outil de travail prédictif par les professionnels impliquera alors une meilleure relation de confiance avec les individus de la communauté.

La politique pénale et le pouvoir exécutif auraient donc leur place dans l'intégration de la police prédictive dans l'arsenal judiciaire français. Néanmoins, les premiers impactés seraient les acteurs de la chaîne pénale, qui entourent et succèdent le travail policier.

B. Les enjeux pour les magistrats

Les premiers acteurs de la chaîne pénale qui sont directement au contact des méthodes de police prédictive sont évidemment les policiers, les agents, les officiers, les commissariats ; le nom de ces techniques algorithmiques en est la preuve. Ces logiciels prédictifs ont donc vocation à n'impacter que le travail policier. Or, intégrer la prédiction dans le travail de la police pourrait avoir un impact sur celui de tous les autres acteurs du système pénal, à commencer par les magistrats.

135. Magistrats - En effet, dès l'enquête ces acteurs de la chaîne pénale interviennent en amont de la police. En fonction de l'infraction poursuivie, c'est le juge d'instruction

ou le Procureur de la République qui peuvent être amenés à intervenir. Dans les deux cas, l'utilisation par les officiers de police judiciaire d'une technologie prédictive pourrait avoir une incidence sur le travail de ces professionnels.

136. Juge d'instruction - Dans le cadre d'une information judiciaire et donc de la commission d'un crime, c'est le juge d'instruction qui mènera l'enquête. La question se pose de la possibilité d'utilisation d'un algorithme prédictif par ce juge ; le but de la police prédictive étant, à des fins de protection des données, de restreindre son accès. Or, il serait nécessaire d'étendre cet accès au juge d'instruction, qui ne peut comprendre les résultats obtenus par la police qu'en ayant lui aussi la possibilité d'observer l'aide fournie par la police prédictive. Mais cette dernière pourrait principalement avoir une incidence lorsqu'il s'agit de détention provisoire du mis en cause.

137. JLD - Le juge d'instruction peut dans le cadre d'une information judiciaire saisir le juge des libertés et de la détention (JLD) à des fins de détention provisoire du mis en examen. Le JLD peut alors accepter la détention provisoire, la refuser, ou ordonner une alternative comme le placement sous contrôle judiciaire ou sous bracelet électronique. Quelle incidence pourrait avoir la police prédictive sur cette décision ? La mise en examen supposant l'existence d'indices graves ou concordants prouvant l'implication de la personne, la question se pose de savoir si une donnée issue d'analyses prédictives peut être considérée comme un indice grave ou concordant. Mais au-delà de la valeur de cette analyse, la police prédictive pourrait tout simplement influencer la décision finale du JLD – voire même la saisine initiale par le juge d'instruction.

Dans l'hypothèse de l'utilisation par la police, à l'origine, d'une technique prédictive du comportement, la production d'un score de risque criminogène pourrait largement influencer la décision de détention provisoire. L'exemple de l'algorithme désormais qualifié de « raciste » aux États-Unis, à Fort Lauderdale, montre bien qu'un score peut être non seulement biaisé, mais peut en plus avoir un impact sur la décision d'un juge. On pourrait même imaginer qu'en fonction du score donné par l'intelligence artificielle prédictive, le JLD graduerait sa décision. Plus le score serait élevé, plus la personne serait susceptible d'être détenue provisoirement ; un score plus bas mais néanmoins significatif pourrait influencer une décision de mise sous contrôle judiciaire ou bracelet électronique. Or, les méthodes prédictives basées sur le comportement de l'individu sont à manipuler avec d'extrêmes précautions.

Dans l'hypothèse d'un travail policer fondé sur une analyse prédictive de *crime mapping*, le risque serait moins important. Néanmoins il existerait toujours un risque pour la décision du juge des libertés et de la détention. Si par exemple une zone de la ville est considérée comme particulièrement criminogène par l'algorithme, et que le mis en examen est domicilié dans cette zone, le juge pourrait vouloir en quelque sorte l'éloigner de cet environnement délinquant, afin d'éviter toute « mauvaise influence » sur l'individu déjà considéré comme dangereux. La solution pour un juge d'instruction ou un JLD serait donc de le placer en détention, le bracelet électronique ou le contrôle judiciaire n'étant pas suffisants pour l'éloigner de cette zone.

Il faut cependant rappeler l'obligation d'impartialité et d'indépendance des magistrats et juges, qui ne fonderaient évidemment pas leur décision uniquement sur une seule donnée policière. L'enquête menée par le juge d'instruction et par la police judiciaire fournit en effet plusieurs indices qui, cumulés, permettent au juge d'adapter sa décision.

138. Procureur de la République - Pour l'instant, la police prédictive se révèle être principalement utilisée pour l'anticipation d'infractions délictuelles. Dans un tel cas le juge d'instruction n'intervient pas, la police judiciaire mène l'enquête sous la direction du Procureur de la République, qui peut intervenir et diriger cette enquête lui-même ; la police se trouve alors sous son autorité. Cette dernière ne peut intervenir qu'avec son accord. Il est donc possible que le Procureur ordonne l'utilisation d'une technique de police prédictive. En outre, dans cette hypothèse, il faudrait que le Procureur puisse avoir accès à l'algorithme utilisé dans le commissariat et sache s'en servir, au risque, le cas échéant, de détourner cette utilisation.

L'enquête étant menée à charge et à décharge par le Procureur de la République, il ne doit pas se laisser influencer dans la direction des investigations. Bien qu'à termes il décide du déclenchement de l'action publique ou du classement sans suite, il ne faudrait pas qu'une analyse logicielle fonde sa décision. Les mêmes exemples précédemment cités peuvent être réutilisés ici. On voit bien que l'utilisation de résultats prédictifs aux États-Unis par la *prosecution*, autrement dit le procureur, pourrait être biaisée, surtout lorsqu'il s'agit de techniques relatives au comportement de la personne. Bien que le système judiciaire français et sa philosophie soient fondamentalement différents du modèle anglo-saxon, encore une fois le risque zéro n'existe pas. D'autant plus que la programmation

algorithmique et l'intelligence artificielle, si elles sont très précises, inspirent la neutralité et donc la confiance. Et ce, parfois à tort.

Au-delà des magistrats professionnels, qui justement grâce à leur expérience pourraient prévenir et éviter ces biais, la présentation de résultats prédictifs pourraient influencer un procès pénal soumis à la décision d'un jury populaire.

139. Procès pénal - En outre, quelle valeur donner à des résultats de police prédictive ? A quel titre auraient-ils leur place dans le procès pénal ? Il serait pour l'instant difficile de leur donner une valeur probatoire, mais nécessaire de les présenter s'ils ont eu un impact sur l'organisation de l'enquête et de la police judiciaire. A supposer que ce soit un officier de police judiciaire (OPJ) qui présente ces résultats prédictifs, il serait impératif que ce dernier ait une connaissance irréprochable du logiciel. Si ce n'est pas le cas, il faudrait presque envisager de faire appel à des experts – techniciens, scientifiques, programmateurs … — à la barre pour faire pleinement comprendre comment les résultats de l'algorithme ont pu influencer l'enquête. Au même titre que la médecine légale, la psychologie, la psychiatrie, l'analyse ADN, qui sont parties intégrantes de l'affaire pénale, l'analyse algorithmique nécessite des connaissances techniques spécialisées.

Là où outre-Atlantique le jury populaire, dans un procès pénal, doit baser sa décision sur la culpabilité « *beyond reasonable doubt* »[170], les jurés en France doivent se fier à leur intime conviction au vu des éléments leur étant présentés, et à rien d'autre. Il ne faudrait donc pas qu'un résultat algorithmique, sous prétexte qu'il est prédictif et neutre, chamboule cette intime conviction construite par le juré grâce aux éléments du procès et ses propres croyances.

Enfin, bien que cette technologie ne soit pas encore pleinement considérée dans le procès pénal, la justice prédictive pourrait être le *continuum* de la police prédictive. La mise en relation des deux intelligences artificielles aurait un impact encore plus puissant sur ces acteurs du système judiciaire, décuplant ainsi les risques précédemment cités.

[170] Au-delà du doute raisonnable, du simple doute.

L'utilisation de la police prédictive n'aurait donc pas uniquement un impact sur ses utilisateurs directs, à savoir les forces de police. Elle présente en effet des enjeux importants pour tout le reste de la chaîne pénale succédant au travail policier, tant pour les magistrats professionnels que populaires. Or, si leur travail est influencé par la police prédictive, le corollaire de ce constat est qu'il y aura nécessairement un impact sur le mis en cause et son futur pénal.

§2 : Les enjeux de la police prédictive pour le suspect et le mis en cause

Le suspect visé par une enquête ou des poursuites suite à l'aide d'une technique de police prédictive, pourrait voir le procès pénal et son futur sentenciel impacté (A), mais tout aussi bien son futur post-sentenciel (B).

A. L'impact envisageable au stade pré-sentenciel

La mise en œuvre des différentes méthodes analytiques de police prédictive permettrait un travail policier plus proactif et efficace, si elles sont utilisées à bon escient. Il serait certes louable d'obtenir des résultats positifs, et de nouvelles techniques policières satisfaisantes en matière d'efficacité. Néanmoins, aucune méthode ne peut se targuer d'être sûre et productive si elle présente une menace pour un quelconque droit ou liberté des individus. Et en particulier pour les individus dont elle traite : les personnes susceptibles d'être impliquées pénalement.

140. Présomption d'innocence - L'utilisation de la police prédictive peut effectivement influencer le travail policier, et donc le biaiser et impacter le mis en cause. Le droit le plus menacé dans le cadre prédictif est de ce fait le droit à la présomption d'innocence. Car en effet, en fonction du résultat et de l'analyse donnée par l'algorithme, les officiers pourraient avoir tendance à considérer un individu précis comme suspect. Or, jusqu'à décision du juge pénal, cet individu est censé être présumé innocent avant d'être considéré comme suspect. C'est donc principalement ce droit qui peut être menacé dans le cadre de la police prédictive, et ce tant par les techniques de *hot spot* que par les techniques de scores.

Dans l'hypothèse d'une analyse géographique ou spatiotemporelle du crime par le logiciel, l'intuition de la police pourrait être poussée à la suspicion. Un comportement « bizarre » lors d'une patrouille dans un voisinage censé être à haut risque criminogène pourrait être trop vite interprété comme suspect. Le risque est que la prédiction prenne ici le dessus sur la constatation et l'analyse professionnelle.

Dans le deuxième exemple d'analyse du risque de la personne, l'établissement d'un score de risque criminogène pourrait en lui-même être attentatoire à la présomption d'innocence. Dans l'hypothèse d'un score élevé, cela reviendrait en fait à considérer une personne comme constamment « suspecte ». Bien qu'étant un droit subjectif, l'enregistrement de données dans un fichier pénal – tel que le TAJ, le FIJAIS – est au début obligatoire, et ce jusqu'à un éventuel effacement. Or, si la police prédictive venait à se fonder en partie sur ces fichiers pénaux de données pour établir un score, l'atteinte à la présomption d'innocence n'en serait que plus grande encore.

Car non seulement l'établissement du score étiquèterait l'individu comme suspect, mais cela pourrait de plus influencer une décision d'arrestation, voire l'enquête, comme il a été vu précédemment. Indirectement, cette enquête pourrait alors être menée uniquement à charge …

141. Procès pénal - Si la police prédictive a une influence sur le processus pré-procès, elle peut en avoir une sur le procès en lui-même et sur le sort de l'accusé. Tout d'abord, le mis en cause pourrait se voir confronté directement à l'analyse faite par l'intelligence artificielle – comment contredire un score établi par une machine ? On voit ici tout l'enjeu pour la défense et ses avocats de l'introduction d'une analyse prédictive dans le procès pénal. On retrouve les mêmes problématiques que dans le cadre du travail des magistrats. Hormis qu'ici, ces problématiques se retournent contre le sort de l'accusé. Si un score donné par un algorithme prédictif est présenté au procès, la personne sur le banc de la défense est catégorisée, aux yeux de la salle d'audience, comme délinquante. Cela pourrait inspirer à son égard, avant même qu'une décision ne soit prise sur son cas, une sorte de méfiance à son encontre.

142. Peine - Ce qui montre que la police prédictive peut aussi avoir un impact sur le prononcé voire le *quantum* de la peine encourue. L'établissement d'un score prédictif de risque criminogène pourrait indirectement rallonger la peine encourue, afin de palier

à ce soi-disant risque que l'individu représente. A l'inverse, les débats pourraient prendre une autre tournure avec l'influence de la police prédictive. La défense pourrait justement jouer sur le fait que l'individu, vivant dans un voisinage qualifié par l'algorithme prédictif comme à haut risque criminogène, était influencé par un environnement délinquant. Le *hot spot* dans lequel l'accusé vit pourrait être interprété, par exemple par un jury, comme un mauvais environnement socio-économique et criminogène et comme une fatalité pour le mis en cause. Néanmoins ce seraient plutôt les techniques d'analyse de la personne et de prédiction comportementale qui poseraient problème vis-à-vis du droit au procès équitable de l'individu encourant la peine.

Les techniques de prévision de la récidive se développent et s'illustrent par des calculs de scores, permettant aux chercheurs et sociologues d'imaginer des algorithmes prédictifs du risque de récidive que peut présenter une personne. Cependant, la police prédictive a vocation à aller plus loin que ça et prédire le potentiel violent d'une personne alors même qu'elle n'a encore jamais commis d'infraction violente[171]. En Californie, dans la ville de Fresno, la police tente de développer le logiciel *Beware*, qui a vocation à prédire et calculer le potentiel violent d'un individu grâce à un certain nombre de données, et ce indépendamment de la question de la récidive[172]. L'utilisation d'un tel score à l'audience dans l'hypothèse de poursuites pénales de l'individu ne ferait pencher la balance qu'en sa défaveur au regard des magistrats et du jury.

Une fois l'individu condamné ou non et fixé sur son avenir pénal, on pourrait penser que l'influence de la police prédictive s'arrêterait à la fermeture du procès. Or, c'est tout l'enjeu du Big Data et de l'apprentissage autonome : l'intelligence artificielle garderait en mémoire cet individu et continuerait d'analyser ses données, résultats et chiffres.

B. <u>Des enjeux éventuels au stade post-sentenciel</u>

Là où les méthodes de police prédictive pourraient impacter le procès pénal et la peine encourue par un mis en cause, elles pourraient en outre le suivre toute sa vie et le réduire à cette caractéristique pénale et délinquante.

---

[171] Cf *supra* n°91
[172] J. JOUVENAL, « The new way police are surveilling you: Calculating your threat 'score'", *The Washington Post*, January 10th 2016, disponible émectroniquement : https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?noredirect=on&utm_term=.164c052bc7c0

Le problème de la police prédictive peut alors être considéré comme un problème pour le condamné au stade de la détention et même plus précisément au stade de la sortie de prison ; en bref, au niveau de la réinsertion. Les réformes pénales françaises, et notamment depuis 2014, tentent de se concentrer sur ce but de réinsertion comme facteur de réduction de la criminalité – faire sortir l'individu du cercle délinquant pour lui permettre de se réinsérer et lui enlever cette étiquette qui le suit parfois trop longtemps.

143. Réinsertion - L'intelligence artificielle peut permettre de recenser et suivre efficacement les personnes placées en liberté conditionnelle, soumises au sursis avec mise à l'épreuve, à l'assignation à résidence sous surveillance électronique, sous contrôle judiciaire, placées sous surveillance électronique mobile etc. Les conditions de ces mesures sont en effet que la personne informe régulièrement les autorités compétentes de leurs changements d'emploi ou d'adresse par exemple. L'utilisation d'un logiciel peut s'avérer utile dans de telles hypothèses.

Ces mesures sont parfois mises en place pour éviter la sortie sèche de détention et anticiper la réinsertion dans la vie sociale des détenus. Or, se savoir constamment surveillé, qui plus est par une machine qui semble anticiper et calculer tout pas de travers, n'aide pas forcément à la réinsertion et à ce que l'individu y participe.

144. Étiquette délinquante - Il en va de même pour toute personne condamnée mais ayant définitivement purgé sa peine : prison, amende, personnes dont le sursis prend fin. Alors même qu'elles se seraient acquittées de leur obligation pénale, un algorithme prédictif pourrait avoir gardé en mémoire ces facteurs « défavorables », produisant par exemple un score qui serait biaisé et les catégoriserait longtemps comme « à risque ». Score qui, là encore, engendrerait une surveillance plus accrue de la part des forces de l'ordre. On retomberait qui plus est dans l'étiquetage constant de la personne comme étant « suspecte » aux yeux de la police, pour peu qu'elle se trouve au surplus dans une zone à fort taux criminogène.

Les fichiers de police, comme mentionné précédemment[173], présentent déjà de tels enjeux pour ceux dont les données y sont inscrites. La problématique tourne

[173] Cf *supra* n°39

principalement autour de la durée de conservation des données de ces individus dans tel ou tel fichier pénal, ainsi que de leur droit d'effacement. Mais, à supposer que ces fichiers soient reliés à un logiciel doté du *machine learning*, les droits et libertés des individus n'en seraient qu'encore plus menacés. Il serait nécessaire d'instaurer un cadre légal de durée de traitement de leurs données, d'éthique de l'algorithme.

La police prédictive et ses effets s'apprécient principalement au niveau national ; PredPol n'a pas encore dépassé les frontières américaines. Mais l'intelligence artificielle a cette caractéristique qui est qu'elle s'étend très vite à tous les domaines, et surtout d'attirer la curiosité de l'Homme. Déjà, le traitement automatisé de données commence à s'installer dans certaines institutions extra-étatiques, européennes. Les nouvelles technologies présentent de nouveaux enjeux ; il en est de même pour le monde socio-économique, diplomatique et politique. De nouvelles formes de criminalité émergent, d'autres se renforcent. C'est le cas du terrorisme, qui a fait émerger une lutte internationale contre cette forme de criminalité transfrontalière. Les États ont donc désormais besoin d'échanger des données, de les faire circuler outre-frontières pour pouvoir lutter efficacement contre ce fléau. Les problématiques apparaissent donc similaires à celles existant au niveau national ; cependant, elles sont décuplées au niveau transnational. Les États n'ont pas tous les mêmes législations, systèmes juridiques et judiciaires, et certains ont vocation à adopter la police prédictive beaucoup plus vite que d'autres.

Chapitre II
L'influence de la police prédictive sur les politiques de lutte contre la criminalité internationale

L'introduction d'algorithmes prédictifs pourrait être envisagée dans un futur plus si lointain par les autorités nationales de certains États. Mais les enjeux de la criminalité internationalisée, comme le terrorisme, dépassent les frontières. Ajoutés aux enjeux du Big Data et de la technologie, les États ont dû réagir et envisager rapidement les problématiques de transfert de données au niveau transnational (Section 1). Or, l'idée de la police prédictive a fait son chemin dans les esprits ; ses théories commencent elles aussi à s'internationaliser (Section II).

Section 1 : La circulation des données entre États

Certaines puissances ont parfois vocation à coopérer dans les domaines pénaux, de la sécurité et de la défense ; ne serait-ce que par leur passé d'alliés. Ainsi des traités internationaux sont parfois nécessaires pour généraliser certains principes – la protection des données s'est globalisée (§1). Outre les recommandations d'entités internationales et les coopérations entre puissances, l'Union européenne a rapidement encadré la circulation des données entre ses États membres dans le cadre de la lutte contre la criminalité (§2).

§1 : Les coopérations internationales pour la circulation des données

Des organisations et entités internationales ont pris l'initiative de poser des recommandations sur la protection des données personnelles, qu'il est fortement conseillé de prendre en compte dans le droit interne des États (A). Certains États, à l'image de la France et les États-Unis, ont même eu la vocation d'aller plus loin et d'encadrer leurs échanges de données faits dans le cadre pénal (B).

A. Les textes internationaux

Bien que n'ayant pas toujours un caractère coercitif et contraignant, les textes internationaux posent des principes à valeur universelle, ayant vocation à pousser les États les ayant ratifiés à intégrer ces principes dans leur ordre juridique national. La plupart du temps d'ailleurs, les États parties à une convention ou un traité international sont déjà détenteurs de textes internes prévoyant les mêmes droits, libertés, ou du moins ont des valeurs directrices similaires.

145. DUDH - C'est le cas notamment des différents textes de l'Organisation des Nations Unies (ONU). La Charte des Nations Unies de 1945 ayant vocation à organiser les différentes composantes de cette institution, il n'a fallu que peu de temps avant que soit ratifiée une convention relative aux droits et libertés universels de l'individu. Ainsi le 10 décembre 1948, les 58 États parties à l'Assemblée générale de l'époque ont ratifié la Déclaration Universelle des Droits de l'Homme, « *idéal commun à atteindre par tous les peuples et toutes les nations »*[174].

146. Ratification et application - Les États ayant ratifié la Déclaration lui accordent ensuite la valeur juridique voulue dans leur droit interne ; en France, les principes et textes internationaux priment sur la loi, mais pas sur la Constitution. Ils ont, quoi qu'il en soit, un rôle à jouer dans le droit et la jurisprudence française et un impact considérable. De manière générale, les États européens ayant déjà une culture intégrative des normes européennes et du droit de l'Union, les textes ratifiés en droit international – non européens – sont rapidement intégrés à l'ordre juridique interne et ont une influence sur le droit. Tel est le cas par exemple du Royaume-Uni, qui possède son propre texte interne sur les droits de l'Homme, le *Human Rights Act*[175].

Mais s'agissant des traités internationaux ratifiées par le Royaume-Uni, et notamment la Déclaration universelle des droits de l'Homme, le système anglo-saxon a souvent tendance à ne pas les ériger au même rang que la France le fait. Ces textes internationaux ont soit valeur de loi – et donc pas de *precedent* – soit sont interprétés directement par les juges, souvent de sorte que la disposition internationale ne soit pas contraire au droit

[174] Préambule de la Déclaration universelle des droits de l'Homme de 1948
[175] Texte écrit en 1998 sous l'impulsion de la ratification du Royaume-Uni de la Convention européenne des droits de l'Homme.

interne. Ainsi la Déclaration universelle des droits de l'Homme n'a, en Angleterre, pas de valeur contraignante.

Une telle position est d'ailleurs relativement spécifique au système de Common Law et donc applicable aux pays appliquant le droit anglo-saxon. Les États-Unis avaient d'ailleurs précisé dès la ratification de la Déclaration de l'ONU qu'elle n'aurait pas de valeur juridique contraignante en droit interne américain. Positions tout de même étonnantes quand on sait que le Royaume-Uni et les États-Unis font partie des cinq États fondateurs de l'ONU et sont membres permanents du Conseil de Sécurité.

147. Vie privée - Parmi les différents articles de la Déclaration universelle des droits de l'Homme est prévu le droit au respect de la vie privée. L'article 12 de la Déclaration dispose que « *nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation* » et que « *toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* »[176]. On remarque que ce texte est similaire aux textes français protégeant le droit à la vie privée mais aussi à l'esprit du *Bill of Rights* américain par exemple. La mention de « l*'immixtion* » dans son domicile ou sa correspondance rappelle le quatrième amendement de la Constitution américaine qui prohibe toute perquisition injustifiée et sans mandat.

148. Pacte relatif aux droits civils et politiques - La Déclaration universelle des droits de l'Homme tend à énoncer les droits considérés comme fondamentaux ; toute personne humaine dans le monde nait détentrice de tels droits et libertés. L'ONU a cependant ressenti le besoin de proposer un texte qui protègerait les individus contre des atteintes plus précises et graves, et prohiber certains actes qui pourraient être perpétrés par un État. Ainsi le 16 novembre 1966, l'ONU a voté son Pacte international relatif aux droits civils et politiques, contenant entre autres la prohibition de la torture, le droit à la vie, la prohibition de l'esclavage, l'égalité devant les tribunaux et la justice … Autant de principes qui, au lendemain des guerres mondiales et dans un contexte de Guerre Froide, étaient indispensables d'écrire noir sur blanc au regard des Nations Unies.

Là encore, les différents États ayant ratifié le Pacte ont émis à tour de rôle des réserves spécifiques, n'intégrant que certains articles dans leur arsenal juridique … Ainsi les États-Unis, dont certains États appliquent encore la peine de mort, ont pu émettre des

[176] Article 12, alinéa 1 et 2, Déclaration universelles des droits de l'Homme, ONU, 1948

réserves et déclara ce texte non-exécutoire dans le droit interne. Il n'en reste pas moins que ce Pacte de l'ONU relatif aux droits civils et politiques est invocable devant la Cour Pénale Internationale, un État ou un dirigeant pouvant être accusé devant celle-ci d'une violation d'un des principes contenus dans ce texte, alors-même que cet État-là y est partie.

149. Vie privée - On trouve dans ce Pacte de l'ONU, parmi ces droits indispensables et la protection contre les éventuels abus de l'État, la protection de la vie privée et familiale. L'article 17 du texte est en fait un copier-coller littéral de l'article 12 de la Déclaration universelle des droits de l'Homme, à l'exception de l'ajout du terme « *illégal* » dans le premier alinéa, à la suite des termes « *arbitraires* » et « *atteintes* ». L'ajout de ce terme relatif à l'illégalité montre le caractère spécifique de ce texte : il a vocation à s'appliquer dans chaque État et donc à s'adapter aux législations internes – un État peut qualifier tel acte d'immixtion dans la vie privée comme illégal, alors qu'un autre peut ne pas le considérer comme tel.

Jusqu'ici, les textes de l'ONU – institution internationale dont les textes sont les plus ratifiés – n'avaient donc pas eu vocation à prévoir la protection des données personnelles. Néanmoins, tout comme la CEDH à l'origine, en 1948 et 1966, cette préoccupation n'est pas encore très présente dans les esprits – la technologie informatique a certes fait son apparition, mais pas les problématiques relatives aux données.

150. Assemblée générale - Les Nations Unies n'ont donc pas encore abouti à la rédaction d'un traité sur la protection des données personnelles, ni dans le cadre privé ni dans le cadre public ou pénal. Néanmoins, les États de l'Assemblée générale en sont venus à un accord et cette dernière a pris une résolution le 14 décembre 1990, énonçant les principes généraux en matière de fichiers personnels informatisés. Bien que n'ayant pas une valeur juridique aussi importante que les autres textes onusiens, cette résolution s'est cependant avérée très utile pour un bon nombre d'États, qui ont pu poser les bases de la protection des données de leurs citoyens sur leur sol.

L'Assemblée générale a ainsi tenu à conseiller quelles « *garanties minimales* » devraient être prévues par les États dans leur droit interne pour assurer une bonne protection des données à caractère personnel pouvant être contenues dans des fichiers informatisés, voire automatisés. Parmi ces principes, ceux de licéité, de loyauté, de

finalité des procédés de traitement des données, le principe d'exactitude de celles qui sont utilisées et le droit des personnes d'au moins y avoir accès. Le texte précise aussi que ce genre de fichier doit éviter tout traitement discriminatoire et surtout être sécurisé, afin d'éviter toute perte ou accès non-autorisé aux données. Enfin, la résolution mentionne le thème de transfert de données entre États, dès lors que chacun d'eux prévoit dans son droit interne des garanties équivalentes de protection de la vie privée[177].

Tant de textes de l'ONU qui auraient notamment pu guider les États-Unis vers une meilleure protection de la vie privée, du moins leur intégration dans l'arsenal juridique américain aurait permis une plus grande précision quant à l'importance de la protection et de la garantie de ce droit. La résolution de 1990 de l'Assemblée générale n'a cependant pas été écrite en vain, ayant beaucoup inspiré les États-Unis dans la rédaction de certains textes législatifs relatifs à la protection des données personnelles dans le secteur privé.

151. OCDE - D'autres institutions ou organes internationaux ont pu depuis les années 1980 éditer des recommandations à l'attention des États de la planète quant à la protection des données personnelles. C'est le cas par exemple de l'Organisation de coopération et de développement économiques (OCDE), qui a le 23 septembre 1980 publié des lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel. Ce texte a été modernisé en 2013. Bien qu'ayant vocation à principalement s'appliquer à des configurations privées, de traitement des données par les entreprises, l'OCDE pose des principes qui se veulent directeurs dans l'utilisation des données personnelles. Mais l'organisation a surtout travaillé à poser des axes concernant l'échange et la circulation de données au niveau international et entre États.

Le principe est d'ailleurs que les membres de l'OCDE devraient faciliter cet échange et « *l'assistance mutuelle lorsqu'il s'agit des questions de procédure et d'échange réciproque d'information* »[178]. Ces termes étant très généraux, on pourrait y voir justement une volonté d'ouverture à l'interprétation : il pourrait s'agir par exemple de l'échange d'informations dans un but pénal ou de coopération entre États dans la lutte

[177] Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, adoptés le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990
[178] Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, OCDE, 23 septembre 1980, Partie cinq

contre la criminalité. Ainsi même si ces recommandations auraient plus vocation à s'appliquer dans un contexte commercial, les principes énoncés dans le texte pourraient être applicables dans le secteur public du traitement des données.

L'OCDE résume finalement bien dans ce texte les déboires du droit international lorsqu'il s'agit de la protection des données : « *à l'échelon international, on se préoccupe avant tout de parvenir à un consensus au sujet des principes fondamentaux sur lesquels doit reposer la protection des personnes physiques* »[179].

Les différentes institutions internationales, notamment l'ONU, ont vocation à indiquer aux États sur quels principes ils devraient se mettre d'accord pour assurer une protection des données individuelles, afin d'envisager de meilleurs échanges de ces données. Certains États ont d'ailleurs pu en venir à établir des pactes spécifiques entre eux, afin d'encadrer les flux transfrontières de données ; cas notamment de la France et des États-Unis. Reste à savoir si ces États sont prêts à coopérer en matière pénale et si oui, comment – l'État américain ne faisant pas partie de l'Union européenne.

B. Les coopérations entre États

Il faut ici envisager des coopérations étatiques, au sein desquelles l'un des États ne fait pas partie de l'Union européenne. Un tel cas de figure existe notamment entre les États-Unis et la France par exemple. Au-delà de la non-appartenance des États-Unis à l'Union européenne, c'est la profonde différence de leurs systèmes judiciaires et pénaux qui peut compliquer la conciliation. La France et les États-Unis ont pu au fil du temps conclure des accords de différentes formes, et qui ne leur sont pas toujours propres ; certains partenariats sont issus d'une négociation et de textes européens, d'autres sont plus diplomatiques, faisant preuve d'une volonté de la part des deux États de renforcer la coopération dans la lutte contre la criminalité et le terrorisme.

152. Accord USA-UE - Il existe donc un texte européen depuis 2016 qui lie les États membres de l'Union et les États-Unis sur le plan de la protection des données personnelles dans le cadre pénal. Avec la recrudescence des actes terroristes, notamment en Europe, les États des différents continents sont parfois – voire souvent – amenés à travailler ensemble pour lutter contre cette criminalité. Les États-Unis étant une des plus grosses

[179] *Ibid,* « aspect internationaux de la protection des données individuelles et des banques de données »

puissances mondiales, il fut nécessaire d'arriver à un accord concernant le transfert de données personnelles dans le cadre de cette lutte anticriminelle.

Les deux puissances en sont donc arrivées à conclure un accord sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière[180]. Conscientes des disparités pouvant exister entre les différents systèmes politiques et judiciaires des États, les deux parties précisent à plusieurs reprises dans cet accord qu'il n'a pas vocation à remplacer les éventuels textes et accords internationaux déjà existants. En outre, la forme étatique et fédérale des États-Unis est prise en compte.

Cet accord permet principalement de faciliter l'échange de données dans le cadre d'enquêtes ou de procédures pénales, parfois effectuées dans l'urgence et demandant une rapidité plus importante, tout en protégeant le droit à la vie privée des individus. Le texte prévoit donc une coopération entre les autorités compétentes de chaque État. Dans l'exemple de la France, l'autorité compétente dans un cadre pénal pourrait être le Procureur de la République et celle des États-Unis serait les procureurs fédéraux ou étatiques. Néanmoins il est certain que les procureurs ne pourraient pas directement communiquer entre eux ; le Ministère de la Justice français et l'*Attorney General* américain feraient office d'intermédiaires.

L'accord entre l'Union européenne et les États-Unis mentionne des principes qui sont maintenant propres et indispensables à la protection des données à caractère personnel. Ainsi la finalité doit être exclusivement pénale et judiciaire, le transfert et la conservation de ces informations doivent être sécurisés au maximum, une durée de conservation doit être prévue par les parties, les données sensibles pouvant être sujettes aux biais discriminatoires sont protégées. En outre, l'article 15 traite des décisions automatisées : celles-ci ne peuvent être la base unique d'une décision préjudiciable pour une personne, du moins elle doit pouvoir obtenir une intervention humaine dans le droit interne. Cet article a tout son intérêt dans le droit américain, qui intègre petit à petit la police prédictive dans ses mœurs sans avoir toujours prévu d'encadrements juridiques.

[180] Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, Journal officiel de l'Union européenne, 10 décembre 2016

On voit qu'il n'est pas si évident de prévoir un cadre général de protection des données soumises au transfert dans un cadre pénal entre un État européen et l'État américain. Finalement, c'est la voie diplomatique qui est privilégiée dans les grandes lignes en ce qui concerne cette circulation des informations, mais les deux parties s'accordent à dire que cet échange diplomatique et juridique se doit d'être fait dans le respect des garanties de protection des données à caractère personnel.

153. Accords France États-Unis - Hormis cet accord auquel sont soumis les États européens signataires, rien n'indique qu'ils ne peuvent ensuite négocier directement leurs propres partenariats avec les États-Unis. La France a ainsi pu conclure plusieurs ententes avec l'État américain dans le cadre pénal et de protection de certaines données échangées à des fins judiciaires.

Il existe entre ces deux pays un accord bien plus vieux que celui de l'Europe en matière pénale. La France et les États-Unis ont en effet conclu en 1998 un traité d'entraide judiciaire en matière pénale[181], afin de faciliter notamment l'échange d'informations d'investigations et l'échange diplomatique dans les cas où une coopération serait à mettre en œuvre. Ce texte encadre les cas de figure où il serait nécessaire pour l'un des deux pays d'obtenir des informations sur la personne poursuivie, de demander des perquisitions, des comparutions etc. Bien qu'étant relativement complet et les procédures de demande d'entraide encadrées, le texte ne prévoit pas vraiment de protection spécifique pour les particuliers qui pourraient faire l'objet de poursuites, ni de protection de leurs données échangées dans le cadre de cette entraide.

Il semblerait donc que la France applique désormais principalement l'accord européen qu'elle a ratifié, dans le cadre de l'échange de données et de la protection de celui-ci. C'est notamment par le biais d'Interpol que se font les demandes d'informations dans le cadre pénal. Dans son propre droit interne, l'État français a encadré les éventuels transferts de données vers un État ne faisant pas partie de l'Union européenne, dans la loi Informatique et Libertés. Ainsi, au même titre que le texte européen, il faut que l'État non-partie à l'UE présente dans son droit interne des garanties équivalentes ou suffisantes à celles de la France pour qu'un transfert soit envisagé. Des exceptions sont prévues à cette condition, notamment la nécessité de sauvegarde de la vie d'une personne, des raisons d'ordre public ou encore la nécessité d'exercice des droits de la défense.

[181] Traité d'entraide judiciaire en matière pénale entre la France et les États-Unis, 10 décembre 1998

L'Assemblée nationale relevait à juste titre dans un rapport que les États-Unis présentaient « *une législation et une organisation (...) plus faibles en cours toutefois d'amélioration* »[182]. C'est en effet ce qui a compliqué et ce qui peut toujours compliquer les accords de protection des données, tant en matière pénale, privée et commerciale, entre les deux États. Suite aux révélations faites par Edward Snowden par exemple, la Cour de Justice de l'Union européenne et la France dans le même temps, ont invalidé le *Safe Harbor*, texte américain qui était censé protéger les données à caractère personnelle transférées par l'UE vers des entreprises européennes. L'Union et les États-Unis sont finalement arrivés à un nouveau texte en juin 2016, le *Privacy Shield* ou « Bouclier de protection des données ».

Dans le cadre pénal cependant, l'État français s'émancipe parfois des règles européennes, sans pour autant en changer les principes de protection des données personnelles. La France et les États-Unis ont donc eu vocation récemment à s'accorder sur l'échange de certaines données qui sont souvent collectées dans un contexte judiciaire.

En 2016, la France a donné son approbation quant à l'échange des données dactyloscopiques et génétiques avec l'État américain, indépendamment des procédures européennes. « *L'accord tend à permettre la consultation mutuelle et automatisée des fichiers ADN et des systèmes d'identification dactyloscopiques, selon un système de concordance/sans concordance (« hit/no hit »)* »[183] décrit l'Assemblée nationale ; ce qui engendre pour la France une ouverture de l'accès aux fichiers FNAEG et FAED. Le Préambule du texte dispose en outre que ces échanges d'informations doivent se faire dans le respect des droits à la vie privée et à la protection des données personnelles ; un article 10 est aussi consacré à cette protection.

Les coopérations policières et pénales se développent donc entre l'Union européenne et les États-Unis, mais les différents membres de l'Union, dont la France, concluent aussi indépendamment des accords avec l'État nord-américain. Au-delà des traités internationaux, les États de la planète ont vocation à s'entraider dans la lutte contre la

[182] Ass. Nationale, Rapport sur le projet de loi autorisant l'approbation de l'accord sous forme d'échange de lettres entre le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique relatif au renforcement de la coopération en matière d'enquêtes judiciaires en vue de prévenir et de lutter contre la criminalité grave et le terrorisme, 27 janvier 2016
[183] *Ibid.*

criminalité, en facilitant et protégeant les flux de données. L'Union européenne a néanmoins ses propres textes encadrant les échanges entre ses membres, mais aussi ses propres institutions.

§2 : La circulation des données dans l'espace liberté, sécurité et justice

La circulation des données œuvrant souvent à des fins de coopérations pénales, le législateur européen a dû encadrer ces échanges (A). Outre les textes, l'Union européenne dispose de ses propres institutions de lutte contre la criminalité, qui facilitent la coopération interétatique (B).

A. L'encadrement européen de la circulation des données en matière pénale

La suppression du troisième pilier a laissé place à l'espace de liberté, sécurité et justice au sein de l'Union européenne, faisant muter la coopération pénale et judicaire entre les États membres. La directive 2016/680, applicable dès le 25 mai 2018, a donc vocation à répondre aux objectifs poursuivis dans ce cadre-là, la circulation des données entre États s'avérant de plus en plus indispensable à la lutte contre la criminalité, surtout avec l'augmentation du nombre d'actes terroristes en Europe.

Cependant, le texte en matière pénale accompagnant le RGPD ne fait que renforcer le cadre juridique en matière d'échange de données personnelles en matière pénale. En effet, l'Union a pu à plusieurs reprises dans le passé écrire ses propres règles en matière de circulation de données dans un contexte de coopération judiciaire.

154. Traité de Prüm et principe de disponibilité des données - Tel est le cas de la décision Prüm[184], texte de 2005 dont l'initiative venait à l'origine de la Belgique, l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche. Ce texte, visant à renforcer la coopération entre États dans l'espace LSJ, a ensuite été transposé en partie en droit communautaire et ratifié par une vingtaine d'États. Car en effet, le grand apport de ce traité tient à la coopération en matière d'échange de données utiles dans le cadre policier et judiciaire : les données génétiques, digitales et minéralogiques. Le

[184] 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, dite décision Prüm

Conseil précise en effet dans le texte qu'à la suite du Conseil européen de Tampere d'octobre 1999, il est apparu nécessaire « *de renforcer l'échange d'informations entre les autorités compétentes des États membres aux fins de la détection des infractions et des enquêtes en la matière* »[185].

155. ADN - Ainsi, un État demandeur peut contacter un autre État afin de comparer un profil ADN avec ceux de son fichier national d'empreintes génétiques, et ce dans le cadre d'une enquête policière par exemple. Comme le précise l'article 3 du Traité de Prüm, il n'est pas question d'ouvrir librement la consultation des fichiers ADN, mais bien de créer des points de contact dans chaque État membre pour que la consultation se fasse au cas par cas.

Mais justement, quid du cas dans lequel une concordance venait à apparaître ? Un tel cas de figure implique effectivement une communication des données personnelles de la personne à laquelle appartient l'empreinte génétique. Ce texte n'aurait aucun sens s'il était seulement question de comparaison de fichiers ADN sans ensuite que les États ne communiquent les résultats obtenus … L'article 5 du texte prévoit donc qu'en cas de concordance entre les ADN, « *la transmission d'autres données disponibles à caractère personnel et d'autres informations relatives aux données indexées est régie par le droit national de l'État membre requis, y compris les dispositions relatives à l'entraide judiciaire* »[186].

Par exemple, si la France venait à comparer une empreinte génétique trouvée par les autorités allemandes et que la comparaison avec le fichier FNAEG faisait ressortir une concordance, c'est la loi de l'État français qui viendrait à s'appliquer quant à la transmission des données personnelles de la personne. Le Traité de Prüm a instauré le principe de disponibilité des données dans le cadre de la coopération judiciaire de l'Union européenne.

156. Casier judiciaire - Moins d'un an après, dans cette optique de renforcement de la coopération dans le cadre de l'espace LSJ, est entrée en vigueur une décision-cadre étendant cette idée de disponibilité des données aux casiers judiciaires[187]. Ce texte ajoute

[185] *Ibid,* (2)
[186] *Ibid,* article 5
[187] Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres

aussi des dispositions quant à l'échange d'informations sur les condamnations pénales. La décision-cadre régit notamment l'échange d'informations lors d'une condamnation dans un État membre d'un ressortissant d'un autre État membre. Outre ces règles, elle permet la circulation d'informations contenues dans le casier judiciaire d'une personne. Ainsi des données à caractère personnel peuvent être transmises entre les États signataires quant à certains de leurs ressortissants ayant été impliqués pénalement.

Les textes européens ont donc eu vocation jusqu'ici à renforcer voire construire les bases de l'espace liberté, sécurité et justice, et de la coopération dans le cadre policier, judiciaire et pénal. Les fichiers relatifs aux empreintes génétiques, digitales, ou le casier judiciaire sont en général des fichiers présents dans tous les États et qui peuvent donc s'avérer utiles pour la lutte contre la criminalité – voire même le terrorisme – s'ils sont comparés.

157. Nouvelle directive de protection des données au pénal - Reste qu'il était nécessaire d'encadrer plus globalement les flux de données entre États dans un contexte pénal – le Big Data ne présentant pas que des enjeux pour les entreprises privées, mais aussi pour les autorités publiques dont la police, les acteurs judiciaires et le cadre pénal en général. La hausse du nombre d'actes terroristes en Europe rend le renforcement de la coopération entre États de l'Union d'autant plus indispensable.

De ce fait, la directive 2016/680 est venue poser un cadre légal plus général des échanges de données entre autorités répressives et policières des États de l'Union européenne : « *il convient de faciliter le libre flux des données à caractère personnel entre les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publiques et la prévention de telles menaces au sein de l'Union (…) tout en assurant un niveau élevé de protection des données à caractère personnel* »[188]. Le Chapitre V de la directive traite de ce thème.

La directive semble prendre en compte le caractère urgent que présente parfois la menace terroriste et prévoit notamment qu'un transfert de données personnelles peut s'effectuer sous certaines conditions sans l'autorisation préalable d'un autre État, à savoir lorsque ce transfert « *est nécessaire aux fins de la prévention d'une menace grave et immédiate pour la sécurité publique d'un État membre ou d'un pays tiers ou pour les*

[188] Directive 2016/680, *op. cit.* note 19, §4 de la directive

intérêt essentiels d'un État membre et si l'autorisation préalable ne peut pas être obtenue en temps utile »[189].

De plus, la Commission ouvre la possibilité au transfert de ces données personnelles vers un « pays tiers » ou une organisation internationale, dès lors que la finalité pénale est recherchée, et que ce pays ou organisation présente un système offrant les mêmes garanties de protection que l'État européen. Une telle procédure est cependant possible uniquement après décision favorable de la Commission. Là encore, des exceptions sont prévues, similaires à celles des textes antérieurs : sauvegarde des intérêts vitaux ou légitimes de la personne, prévention d'une menace grave et immédiate pour la sécurité publique d'un État.

Enfin, cette directive, dans un article 40, précise que les institutions européennes et les États membres de l'Union, ont vocation à s'ouvrir à l'élaboration et à l'adhésion à des coopération internationales sur le plan pénal et le partage des données individuelles, dès lors que ces dernières sont suffisamment protégées par les autres entités.

Ainsi, les États membres de l'Union disposent d'une multiplicité de textes leur permettant de communiquer des données personnelles à des fins pénales et répressives. Néanmoins la coopération a vocation à aller encore plus loin ; l'Union dispose de ses propres plateformes et institutions permettant la circulation des données se devant d'être disponibles dans le cadre pénal.

B. Les institutions pénales européennes intervenant dans la circulation des données

158. SIS - L'une des plus grosses créations en matière de coopération policière et judiciaire fut le Système d'information Schengen (SIS). Prenant la forme d'une base informatique – et donc automatisée – de données, le SIS contient pas moins de 64 millions de signalements à son actif[190]. Il recense, via le signalement des États faisant partie de l'espace Schengen, les données relatives aux personnes recherchées en vue d'une procédure pénale, faisant l'objet d'un mandat d'arrêt, aux personnes disparues, celles

[189] *Ibid,* article 35(2)
[190] Chiffres de l'année 2016, disponibles électroniquement : https://ec.europa.eu/france/news/20161212_decodeursue_systeme_information_schengen_fr

interdites de séjour, mais est aussi relatives aux objets et véhicules volés ou faisant l'objet d'une saisine.

159. SIS II - Cette base informatique contient donc un grand nombre de données à caractère personnel, tel que l'identité de la personne, mais aussi sa photo voire ses empreintes digitales. Ces données-ci ont été introduites plus tard grâce à ce qui peut être considéré comme l'extension du SIS, le Système d'information Schengen II (SIS II). Les signalements mais surtout le droit d'accès à ce système n'appartient qu'aux autorités compétentes des États parties. En France, cela comprend donc les autorités judiciaires, de police nationale, militaires, de gendarmerie, de douane, les agents de préfecture et de l'administration centrale du Ministère de l'Intérieur, les agents du Ministère des affaires étrangères. Les plateformes Europol et Eurojust ont elles aussi accès à ces informations.

Le système dispose d'une base nationale dans chaque État membre, placé en France sous l'autorité de la Direction générale de la police nationale du Ministère de l'Intérieur. Le SIS reste cependant un système très protégé, contenant un très grand nombre de données, parfois sensibles. Étant un fichier européen, il est entouré de règles dont la garantie du droit de consultation aux personnes inscrites et du droit de rectification. En outre, servant à la recherche et l'identification de personnes sur tout le territoire européen, ces dernières ont la garantie que leurs informations seront effacées de la base de données dès lors que la procédure mise en œuvre prendra fin.

Le SIS s'est avéré très efficace et utile pour les États membres, et a notamment servi dernièrement à la détection de l'entrée et la sortie de djihadistes sur le territoire européen. La Commission européenne précise sur son site internet que le SIS a été consulté près de 4 milliards de fois en 2016 et a permis l'arrestation de 23 000 personnes sur une seule année[191]. Ce système, conjugué au Traité de Prüm, s'avère être un outil féroce contre la criminalité internationale et pour la détection d'infractions pénales.

Dernièrement, la Commission européenne a eu vocation à renforcer le SIS, notamment en ce qui concerne le signalement de personnes impliquées dans des infractions terroristes, mais aussi concernant les garanties de protection des droits et libertés fondamentaux des personnes concernées. On voit ainsi que les enjeux du Big Data et de l'automatisation de certains secteurs impactent toutes les plateformes et systèmes européens ; la protection des données personnelles est à amplifier constamment.

[191] *Ibid.*

160. Europol - D'autres systèmes européens permettent la facilitation de la circulation des données entre États de l'Union européenne. Parmi eux, Europol, qui possède son propre système informatique de données relatives à certaines menaces contre la sécurité des États : le terrorisme, le trafic international de stupéfiants, le blanchiment d'argent, la fraude organisée, la contrefaçon de l'euro, le trafic de migrants. En bref, la plupart des infractions caractéristiques de la criminalité organisée ou internationale. Cette plateforme permet l'échange de renseignements et de données entre les autorités de police des différents États membres dans ces domaines-là, et ouvre son système informatique aux autorités compétentes, qui peuvent tout autant l'alimenter.

Europol travaille aussi très régulièrement à l'analyse de la criminalité, mène des investigations, analyse les résultats donnés par les États, et rend des rapports à leur intention afin de faire évoluer les techniques et moyens de lutte contre la criminalité et d'améliorer la sécurité sur le territoire européen.

Dans son dernier rapport de 2016-2017, Europol a annoncé le développement d'un nouvel outil de travail automatisé de détection et d'analyse du crime organisé. « *Le système parcourt et analyse le flux d'informations de toutes les sources pertinentes, incluant les sources ouvertes, les sources de droit et les bases de données (tant publiques que juridiques)* ». Ces informations sont ensuite analysées et croisées, tout en tenant compte de leur fiabilité, leurs compatibilités et leur traçabilité. On voit là les prémices d'une intelligence artificielle au sein d'Europol, qui pourrait à termes être dotée de l'apprentissage autonome et produire des analyses bien plus poussées et en temps réelle de la criminalité organisée. A se demander si l'analyse prédictive ne pourrait pas être introduite … La base informatique de données d'Europol étant l'une des plus fournies d'Europe, son analyse par l'intelligence artificielle permettrait de faire ressortir d'autant plus d'informations quant aux caractéristiques de la criminalité organisée.

161. Eurodac - Outre le SIS et le système Europol, le système d'information Eurodac permet le recensement d'empreintes digitales au niveau européen, notamment en rapport avec les demandes d'asiles. Les États membres peuvent ainsi faire des demandes de consultation voire de comparaison avec cette base de données. Depuis 2013, cette consultation est ouverte sous certaines conditions aux autorités étatiques menant des investigations, ou travaillant dans le but de la détection et la prévention d'actes terroristes

ou autres infractions pénales graves. Ainsi, de plus en plus de fichiers européens s'ouvrent aux États afin de faciliter la coopération judiciaire et policière, pour lutter contre la criminalité organisée et internationale et aider à la détection et la prévention d'infractions. Tous les outils sont disponibles pour tenter de s'y retrouver dans le Big Data, l'automatisation des systèmes étant indispensable au vu de la quantité de données qu'ils contiennent.

La recrudescence du nombre d'actes terroristes, la proximité du continent européen avec les pays étant victimes du djihadisme et les problématiques telle que l'immigration illégale, font de l'Europe un carrefour du développement de la criminalité organisée internationale. Les États de l'Union européenne et leurs citoyens étant les premières victimes de cette délinquance, de plus en plus violente ou parfois financière, il est nécessaire de renforcer la coopération pénale et judiciaire entre ces États membres mais aussi les moyens des institutions européennes. D'autant plus que ces menaces se conjuguent avec les nouveaux enjeux du Big Data et de l'intelligence artificielle, parfois difficiles à appréhender par les institutions et plateformes de lutte contre la criminalité ; les flux de données à cette échelle sont encore plus importants qu'au niveau étatique.

L'utilisation potentielle de l'intelligence artificielle – à l'image d'Europol – est à accueillir avec prudence mais pourrait néanmoins s'avérer utile dans l'analyse des données se croisant dans les fichiers pénaux européens. La dimension de ces fichiers a d'ailleurs dépassé le cadre européen ; cette criminalité internationale, et surtout le terrorisme, ont fait naître le besoin de fichiers partagés au niveau international. Aussi, quand on voit que l'intelligence artificielle s'immisce dans le travail pénal et judiciaire européen, qui laisserait entrevoir l'expérimentation de techniques prédictives, la question se pose de savoir si elle aurait sa place dans la lutte contre le terrorisme et la criminalité organisée.

<u>Section 2</u> : Les enjeux de la police prédictive pour la lutte contre la criminalité organisée : l'exemple du terrorisme

La hausse du nombre d'actes terroristes, tant en Orient qu'en Occident, a fait de la lutte contre cette criminalité une cause internationale et interétatique. La violence des attaques et la radicalisation engendrent parfois le renforcement de politiques sécuritaires

par les dirigeants des États. Ces derniers en sont d'ailleurs venus à des accords transnationaux de circulation des données aux seules fins de la lutte contre le terrorisme (§1), fichiers qui permettent parfois un peu plus que la lutte mais bien la surveillance. Surveillance qui pourrait avoir vocation un jour, à se transformer en une volonté de prédiction des attentats. L'idée de l'utilisation de l'intelligence artificielle entre États pour de sûreté pourrait émerger ; faudrait-il laisser la police prédictive dépasser les frontières (B) ?

§1 : Le flux de données interétatique dans la lutte contre le terrorisme

Différents accords ont vu le jour entre les États concernant la circulation des données ; certains se sont spécialisés dans la lutte contre le terrorisme. Un premier constat a été fait : empêcher et surveiller certains flux de capitaux aiderait à lutter contre le financement de cette criminalité transfrontalière (A). La surveillance a dépassé les mouvements financiers ; certains États ont initié des coopérations avec le secteur privé, notamment du tourisme, pour surveiller les mouvements de personnes (B).

A. L'accord TFTP : la surveillance des données financières terroristes

Dans la lutte contre le terrorisme et la criminalité organisée de manière générale, les autorités répressives se sont toujours entendues, qu'importe l'État, sur un facteur à combattre avant tout : les sources de financement. Des interventions armées, policières, militaires, peuvent être ordonnées par les gouvernements des pays luttant contre cette criminalité cependant, si les effectifs baissent ou que les participants sont punis, il n'en reste pas moins que si le financement subsiste, les organisations criminelles continuent de prospérer.

Chose que les États-Unis ont très vite comprise, au lendemain des attentats du 11 septembre 2001. Ces derniers ont engendré, il est bien connu, un grand nombre de prises de décisions et un accroissement de la surveillance de la part de l'administration Bush – président des États-Unis à l'époque – qui n'a pas toujours consulté les citoyens et dont certaines n'ont pas été annoncées publiquement. L'idée de combattre les organisations terroristes en leur coupant les vivres à la source reste majoritairement partagée ; mais attiser la haine des citoyens contre son propre gouvernement reste un atout pour les

terroristes … Car trop souvent depuis 2001, des lanceurs d'alertes ont découvert et fait ressortir des pratiques et programmes tus par les autorités américaines, soulevant l'indignation nationale voire internationale.

162. Affaire Swift - Parmi ces révélations, celle à propos du suivi des mouvements financiers mis en œuvre par le gouvernement américain de l'époque. En 2006, un groupement de journaux a révélé que la CIA et le Trésor américain possédaient mais surtout se servaient d'un programme leur permettant l'accès à toutes sortes d'informations bancaires de la base de données des transactions SWIFT, la *Society for Worldwide Interbank Financial Telecommunication*. Ce programme porte le nom de *Terrorist Financing Tracking Program* (TFTP), et a donc une visée claire de collecte de ces données bancaires à des fins de lutte antiterroriste.

Cette société SWIFT, au siège belge, a deux serveurs dans le monde : l'un en Europe et l'autre aux États-Unis. Comme le soulève Raoul Ueberecken, Conseiller justice et affaires étrangères au Luxembourg en 2010, « *il importe de préciser que par le biais du TFTP, le département du Trésor n'accède pas aux données détenues par Swift sur les banques de données de la société (…). Mais il y a un transfert en vrac de données commerciales de Swift vers les serveurs du département du Trésor. Même si les injonctions administratives ne visent pas toutes les données de Swift (…), elles concernent néanmoins des millions de messages financiers. Les recherches proprement dites se font par les autorités américaines sur les serveurs du département du Trésor, alimentés avec les données Swift* »[192].

Cet accord, qualifié de secret par la presse américaine, se sert donc de données d'une société européenne, parfois, il semblerait, contre sa politique de confidentialité. Mais ces révélations font surtout scandale en Europe : alors même que l'Union européenne possède sa propre réglementation de protection des données personnelles, des institutions américaines les violent allègrement sous couvert de la lutte contre le terrorisme. L'affaire Swift fait état de la différence de régime juridique profonde existant entre la plupart des États membres de l'Union européenne et le système de Common Law des États-Unis. Néanmoins, la lutte contre le financement du terrorisme doit pouvoir se faire, et pour cela, le traitement et la surveillance de certaines transactions sont indispensables. La mise en

[192] R. UEBERECKEN, « Un feuilleton à rebondissements : l'affaire Swift », *Revue du Marché commun et de l'Union européenne*, 2010, p.566

place de négociations commence donc à se faire entre des représentants européens et le Trésor américain, afin de mettre en place un cadre légal et de restaurer la confiance des citoyens européens.

163. Accord TFTP - Ces négociations ont finalement mené à une décision commune d'accord entre l'Union européenne et les États-Unis, afin d'autoriser et d'encadrer le traitement et la circulation des données Swift européennes vers l'État américain, et ce à des fins de lutte contre le terrorisme. Un premier accord a été conclu en 2009, texte qui a néanmoins eu vocation à ne s'appliquer que dans l'urgence et sur la courte durée de neuf mois, du fait de l'entrée en vigueur du traité de Lisbonne[193]. Certaines dispositions de ce dernier imposant de nouvelles règles en matière de conclusion de ce type d'accords, un nouveau texte devait être rédigé pour 2010 afin de répondre à ces obligations.

C'est en juillet 2010 que les deux parties se sont finalement entendues sur une rédaction. Le Conseil de l'Union européenne a publié sa décision d'application de l'accord le 13 juillet 2010[194]. L'Union européenne, dans le préambule de ce texte, admet l'efficacité du système TFTP, et la nécessité de lutte contre le financement du terrorisme par ce biais. Elle rappelle néanmoins qu'il est nécessaire que ces transferts de données se fassent « *sous réserve de la stricte observation des garanties relatives au respect de la vie privée et à la protection des données à caractère personnel* »[195], rappelant ses nombreux textes prévoyant une telle protection. L'Union n'omet pas non plus de rappeler, sans la mentionner directement, sa directive de 1995 relative à la protection des données, selon laquelle les établissements financiers qui seraient amenés à communiquer les données bancaires de certains clients, se doivent d'informer ces derniers de cette possibilité.

L'accueil de cet accord fut très mitigé, en ce que les différences de législations et de politiques antiterroristes entre les deux parties sont relativement différentes ; les détracteurs de ce texte se sont inquiétés d'un laxisme de la part des institutions

[193] Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis d'Amérique aux fins du programme de surveillance du financement du terrorisme, Journal officiel de l'Union européenne, 13 janvier 2010, Article 15
[194] Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, Journal Officiel de l'Union européenne, 27 juillet 2010
[195] *Ibid.*

européennes, vis-à-vis des États-Unis, surtout au vu des nombreux scandales relatifs à la surveillance accrue et gardée secrète par ses institutions. Surtout que cet accord ne marche en quelque sorte que dans un sens, l'Union européenne ne disposant pas d'un système similaire à celui du Trésor américain. Les institutions européennes tentent de rester vigilantes dans le cadre de cet accord : en 2013, suite aux révélations d'Edward Snowden à propos de la NSA, le Parlement européen a adopté une résolution en faveur de la suspension provisoire de l'accord TFTP. Cette résolution n'est restée qu'une menace cependant, n'aboutissant à aucune suspension concrète.

Ainsi, ce texte permet de garantir que « *les données de messagerie financière faisant référence à des transferts financiers et les données connexes qui sont stockées sur le territoire de l'Union européenne par les fournisseurs de services de messagerie financière internationale (...), sont fournies au département du Trésor des États-Unis, exclusivement aux fins de la prévention et de la détection du terrorisme ou de son financement, ainsi que des enquêtes ou des poursuites en la matière* »[196]. Dans la logique de cet article, seules les autorités pénales et de sécurité publique américaines peuvent être réceptrices de ces données et les utiliser dans un but uniquement de lutte antiterroriste. Il en va de même pour les autorités des États membres de l'Union ; en outre Europol et Eurojust peuvent aussi avoir accès à ces informations.

Aux fins de garantie de protection des données à caractère personnel, des dispositions sont prévues afin d'encadrer la durée de conservation, le droit de consultation et d'effacement des données de la part de la personne concernée et bien sûr la protection et la sécurité de ces données durant le transfert, le traitement et la conservation.

164. Traitement automatisé - Comme pour tout accord de ce type concernant le traitement des données personnelles, la question du traitement automatisé doit se poser. La mise en place d'un tel système TFTP aux États-Unis à des fins de lutte contre le financement du terrorisme pourrait très bien s'ouvrir vers du datamining dans un futur proche, pour plus d'efficacité. Or cette potentialité a été prévue par les deux parties dès 2010, dans l'article 5 : « *le TFTP ne prévoit pas l'exploration de données ni aucun autre type de profilage algorithmique ou informatisé, ou de filtrage* ». A savoir que la version en langue anglaise du texte parle bien de « *datamining* ». On peut se demander si l'Union

[196] *Ibid,* article 1(a)

européenne n'aurait pas voulu anticiper ici une éventuelle introduction de l'intelligence artificielle dans ce système TFTP. En effet, les années 2010 sont aux États-Unis les débuts de l'apogée de PredPol – bien que n'ayant pas encore totalement fait ses preuves, plusieurs villes sont enclines à l'adopter. L'introduction d'un tel article est donc intelligente en ce que l'État américain semble céder facilement ou du moins plus rapidement à l'expérimentation de l'intelligence artificielle dans le milieu judiciaire. Prévoir une disposition empêchant l'utilisation du datamining et de l'analyse algorithmique permet d'anticiper des biais dans ce traitement de données. Si une telle prise d'initiative venait à être proposée, les parties n'auraient pour seul choix que le débat diplomatique et la modification de l'accord.

Le principe de proportionnalité semble être particulièrement respecté dans ce texte, de nombreuses dispositions protégeant les données personnelles et anticipant toute atteinte potentielle. Un tel accord était nécessaire, afin aussi de conserver les relations diplomatiques ayant toujours existé entre les deux parties. Mais l'Union a conscience des différences profondes existantes entre ses États membres et le système américain – en veut pour preuve la directive de 1995 de protection des données à caractère personnel, les États-Unis n'ayant pas de texte garantissant autant de protections.

Enfin, les rédacteurs européens de l'accord se sont posés la question de la création d'un système similaire au sein de l'Union européenne – potentialité prévue dans l'accord lui-même[197]. Le coordinateur de la lutte contre le terrorisme pour l'Union européenne, Gilles de Kerchove, a notamment plaidé en la faveur de la création d'un tel système au sein de l'Union, ce qui selon ses mots, complèterait l'échange d'informations. Proposition qui n'a pas abouti à ce jour, auquel cas il faudrait que les parties renégocient un nouvel accord.

L'accord de 2010 est donc toujours en vigueur entre les États-Unis et l'Union européenne. Il a été le premier accord en matière de transferts de données aux fins de lutte contre le terrorisme, semé d'embuches, mais confirmant le fait que ces deux parties, malgré leurs différences, peuvent s'entendre sur un tel thème. Avec l'entrée en vigueur de la directive 2016/680 relative à la protection des données personnelles dans le contexte pénal, la question se pose cependant aujourd'hui de savoir si l'accord TFTP ne

[197] *Ibid*, article 11

nécessiterait pas d'être réformé, pour s'adapter au droit européen actuel. Qui plus est, les perspectives que présentent le Big Data et l'intelligence artificielle – prédictive ou pas – sont encore plus grandes qu'elles ne l'étaient en 2010, ces domaines évoluant à une vitesse exponentielle.

Les États-Unis et l'Europe ont réussi à s'accorder sur un moyen de lutte contre le financement du terrorisme ; néanmoins la surveillance de ces données bancaires n'est pas la seule indispensable à cette lutte. Sont apparus avant 2010 les premiers débats, d'abord au Royaume-Uni, quant à la conservation et le traitement des données des passagers de compagnies aériennes, par les autorités publiques, à des fins de lutte contre la criminalité transnationale.

B. Le fichier PNR : la surveillance des voyages suspects

La criminalité organisée présente ce caractère type qui est qu'elle s'étend très souvent à l'international. Le suivi des mouvements financiers suspects est donc primordial, en ce qu'ils permettent justement une prise de contact sans avoir à se déplacer, sans se rencontrer et donc risquer d'avoir affaire aux autorités d'un pays poursuivant un groupe criminel. Cependant ce type de criminalité, et en particulier le terrorisme, implique de plus en plus non pas uniquement les mouvements de capitaux, mais les mouvements de la personne physique. Le terrorisme en est la preuve, ne serait-ce qu'avec l'endoctrinement djihadiste qui se fait dans certains pays, pour ensuite perpétrer des actes de terreur sur d'autres continents. Pour cela, il est nécessaire de se déplacer soit même ; les moyens de transports ne manquant pas dans notre monde moderne.

165. PNR commercial - Lors de la réservation d'un vol chez une compagnie aérienne, le client doit délivrer un certain nombre de données nécessaires à cette réservation. Certains itinéraires de voyages nécessitant de réserver les vols chez plusieurs compagnies différentes, des accords existent entre ces sociétés commerciales afin de pouvoir communiquer ces données entre elles. Ce partage de données relatives à la clientèle s'est étendu petit à petit à plusieurs acteurs du commerce du tourisme autres que les compagnies aériennes. Est donc apparue ce que ces entreprises ont appelé le *Passenger Name Record* (PNR), le registre de données de passagers. De plus en plus de données personnelles se sont ajoutées à ce PNR, comme l'affiliation religieuse, les

préférences et goûts des passagers, un handicap éventuel, des informations relatives à la famille … afin que les compagnies touristiques puissent effectuer un profilage commercial des clients, pour adapter la communication. L'utilisation d'un PNR se fait aussi par les compagnies de transport autres qu'aériennes, comme les compagnies maritimes.

166. Directive PNR de 2004 - Il n'a fallu alors que peu de temps aux autorités de certains pays, notamment au Royaume-Uni, mais aussi à l'Europe, pour voir une opportunité dans cette exploitation commerciale des données. Dès 2004, le Conseil européen a fait entrer en vigueur une directive obligeant les sociétés de transport à communiquer ces données issues du PNR aux autorités[198]. Le Royaume-Uni a été, lui, le premier État à mettre en place de manière indépendante un système complet PNR permettant aux autorités nationales d'exiger une communication des données par les sociétés de tourisme et de transport. Le système *e-borders* enregistrait non seulement toutes ces données relatives au passager, mais aussi les informations relatives à l'enregistrement de la personne, de bagages supplémentaires éventuels, et à l'embarquement.

La directive de 2004, établie dans le strict respect des dispositions de la directive de 1995 de protection des données à caractère personnel, permet aux autorités de contrôle des frontières des États membres d'imposer aux compagnies de transport de leur communiquer les données contenues dans le PNR. Néanmoins, cette directive n'avait vocation à s'appliquer que pour la lutte contre l'immigration clandestine. Avec la recrudescence de la menace terroriste, l'usage du PNR s'est avéré évident.

167. Résolution du Parlement européen - L'Europe a cependant pris son temps avant de mettre en place l'utilisation des données PNR par les autorités publiques et judiciaires, une telle pratique étant en contradiction avec certaines dispositions de la directive protégeant les données à caractère personnel des individus. Le Parlement européen en est finalement arrivé à la publication d'une résolution en 2008[199] autorisant l'utilisation du PNR à des fins répressives, résolution adoptée par le Sénat français le 30

[198] Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers
[199] Résolution du Parlement européen du 20 novembre 2008 sur la décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record) à des fins répressives

mai 2009. A la suite de cette résolution, de nombreuses propositions ont émané des institutions européennes afin d'émettre un texte final autorisant et encadrant l'utilisation des données PNR dans un cadre judiciaire et surtout de lutte contre le terrorisme. Désireuse de faire concorder un tel texte avec les exigences de protection des données personnelles, sa rédaction a mis du temps.

168. Accords avec des États tiers - L'entrée en vigueur d'une nouvelle directive n'a donc pas été immédiate, paradoxalement aux différents accords que l'Union européenne a pu conclure avec d'autres États. En effet, en 2012, l'Union a successivement renouvelé deux accords d'échange de données PNR dans le cadre de la sécurité publique avec l'Australie[200] puis les États-Unis[201]. Ces accords existaient bien avant 2012, mais nécessitaient une refonte.

169. Directive PNR finale - C'est finalement sous l'impulsion des réformes européennes relatives à la protection des données que l'Union a, dans le même temps, rédigé une directive sur le traitement des données PNR à des fins de lutte contre le terrorisme. Ainsi, une nouvelle directive a été publiée en 2016[202] et est entrée en vigueur dans le même temps, prévoyant non seulement l'utilisation du PNR dans des buts de lutte contre le terrorisme et la criminalité grave, mais créant en plus un système « API » dans chaque État membre, *Advanced Passenger Information*, contenant les données relatives à l'enregistrement et l'embarquement des passagers. Depuis, la France possède son propre système « API-PNR », « *traitement automatisé de données à caractère personnel (…) mis en œuvre par les ministres de l'intérieur, de la défense, chargé des transports et chargé des douanes* »[203].

170. Système API-PNR - Ce système API-PNR, liant donc deux « jeux » de données personnelles, permet aux autorités judiciaires d'effectuer un rapprochement avec des fichiers de police ou pénaux dans le cadre d'une enquête par exemple, ou de détection

[200] Accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, Journal Officiel de l'Union européenne, 14 juillet 2012
[201] Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure, Journal officiel de l'Union européenne, 11 juillet 2012
[202] 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
[203] Article R232-12 du Code de la sécurité intérieure

du terrorisme. On comprend tout l'intérêt de ce système et de la nécessité de son encadrement. Des données relatives à une personne fichée dans un des registres de la police française pourraient par exemple être comparées avec des données API-PNR et mener les autorités à constater des déplacements suspects, récurrents, ou alarmants et ainsi anticiper potentiellement des actes répréhensibles ou terroristes. Parallèlement cependant, son encadrement et ses limites doivent être définis sans ambiguïtés, car il est question ici de surveiller en quelque sorte les mouvements, les faits et gestes des personnes. De plus, au vu des données qui peuvent être contenues dans le PNR, certaines se doivent d'être classées, selon la législation européenne, comme « sensibles » et être manipulées avec précaution.

L'une des problématiques du Big Data prend toute son ampleur dans le cadre international et européen : les menaces criminelles se multipliant, le terrorisme frappant de plus en plus souvent et s'adaptant aux nouveaux enjeux mondiaux, les différentes institutions étatiques, européennes et internationales doivent répondre à ces nouvelles attaques. La circulation des personnes devenant un élément majeur de la criminalité transfrontalière, le meilleur moyen de suivre ces allers et venues s'est trouvé être l'utilisation de données officiellement enregistrées dans le cadre du voyage : les informations détenues par les compagnies de tourisme. La surveillance s'est donc étendue avec la création des accords et textes PNR.

L'enjeu le plus important reste cependant que ces données, qu'elles soient bancaires, commerciales ou policières, sont inexorablement destinées à être soumises au traitement automatique et à l'intelligence artificielle. Celle-ci facilite toute tâche trop laborieuse pour l'Homme ; dans la lutte contre le terrorisme, forme de criminalité internationale et qui dépasse les frontières, les États et les institutions internationales se doivent d'être solidaires. Or, de plus en plus d'autorités publiques sont enclines à introduire des formes d'*Intelligence Led Policing*, l'intelligence artificielle voire la police prédictive dans leurs services. Systèmes qui pourraient dépasser, eux aussi, les frontières.

§2 : Se projeter vers une intelligence artificielle « transfrontière » ?

171. Constat européen de l'arrivée de la police prédictive - En 2016, le Réseau Européen de Prévention de la Criminalité[204], l'ECPN, a publié un rapport sur le thème de la police prédictive, constatant l'arrivée de celle-ci dans plusieurs États européens. Fort de ce constat, l'ECPN a tenu à proposer des recommandations quant à l'introduction de la police prédictive au sein des services de police. Parmi ces recommandations, l'ECPN considère qu'il faudrait que la Commission européenne suggère des standards uniformisant l'éventuelle utilisation de ces techniques prédictives. On retrouve ici l'anticipation européenne en matière de protection des données et d'automatisation des activités régaliennes des États.

En effet, il s'agirait, selon l'ECPN, d'encadrer les pratiques de police prédictive alors même qu'elles n'ont pas encore atteint tous les États membres. Proposer des lignes de conduites directrices en matière de police prédictive permettrait effectivement d'anticiper ses biais. Si chaque État développe de manière indépendante ses propres pratiques prédictives, les coopérations pourraient s'avérer difficiles. Si l'on considère un jour l'uniformisation, la mise en commun, ou la création d'une « police prédictive européenne », les débats pourraient être longs. Des lignes de conduite à suivre émanant de la Commission européenne permettraient surtout de poser les limites de la police prédictive à ne pas dépasser. Car c'est tout l'enjeu de la généralisation de la pratique prédictive : n'étant même pas encore née dans certains pays, elle tend à s'étendre et se développer dans des secteurs inattendus.

172. Nécessité des sources de données - La viabilité de la police prédictive repose sur l'alimentation en data, sur le flux de données. Les différents États de la planète l'ont bien compris. Les accords s'avèrent donc nécessaires entre eux pour s'y retrouver dans cette jungle du Big Data et ils se multiplient de plus en plus. On en veut pour preuve le nombre d'accords que l'Europe a pu conclure avec les pays anglo-saxons en matière de circulation de données, à des fins de lutte contre le terrorisme et la criminalité transfrontalière. L'engouement des États-Unis pour la police prédictive montre qu'il ne serait pas impossible qu'elle se généralise au niveau fédéral d'ici peu – notamment au vu du gouvernement actuel – et donc qu'elle soit utilisée à des fins antiterroristes.

[204] *European Crime Prevention Network*

L'exemple d'Europol utilisant désormais un système d'analyse des données qui lui sont fournies prouve bien que l'automatisation voire même l'apprentissage autonome prend des proportions bien plus importantes que l'on ne voudrait l'imaginer. Cependant au vu du nombre de données et de tous les types de données qu'une plateforme comme Europol reçoit et doit traiter chaque jour, l'utilisation de nouvelles technologies s'avère presque indispensable. Celles-ci permettent tout de même d'atteindre des résultats satisfaisants en matière d'efficacité du traitement, de statistiques et de prévention du crime. Ces nouvelles technologies sont d'autant plus utiles à une échelle telle que celle d'Europol, couvrant un territoire aussi grand que celui de l'Europe, une multiplicité d'États et toujours plus d'individus.

Le rapport de l'ECPN précise par exemple dans ses recommandations qu'en matière de police prédictive, il n'y a pas de raison qu'il y ait de trop grandes barrières législatives, tant qu'on ne s'approche pas trop près des droits des individus. En d'autres termes, le droit le plus important à respecter reste la protection des données personnelles et la garantie de celui-ci ne doit en aucun cas être réduite par la police prédictive. Hormis ce facteur législatif, la police prédictive ne rencontrerait en principe pas d'autres obstacles de cette taille. De la même manière, le rapport de la RAND Corporation suggère dans ses pièges à éviter de ne pas négliger les droits et libertés individuels en utilisant la police prédictive. Un consensus existe donc déjà sur le fait que la protection de la vie privée doit primer sur l'utilisation de la police prédictive.

173. Police prédictive et terrorisme - Or, le terrorisme reste une forme de criminalité transfrontalière et le combat contre celle-ci est nécessairement interétatique. Si la police prédictive venait à dépasser le niveau local et atteignait le niveau fédéral, il ne faudrait que peu de temps avant que d'autres États, européens par exemple, n'adoptent la même approche. Dès lors, si chaque État venait à utiliser la police prédictive en matière de terrorisme, l'idée d'accords interétatiques à des fins de lutte internationalisée pourrait vite apparaître.

Une question subsiste : comment intégrer la prédiction dans l'équation antiterroriste ? Donner une réponse serait prématuré, les différences de législations sur la protection des données étant encore trop disparates entre les États. De plus, bien que le constat précédent

soit rassurant[205], on peut se demander si la nécessité de lutte contre le terrorisme ne pourrait pas prendre le dessus sur certains de ces droits et libertés. En effet, certaines mesures – parfois légitimes – très récentes en matière de lutte contre la radicalisation et contre le risque terroriste montrent que lutter contre cette criminalité implique parfois la nécessité d'atteintes à certains principes, comme le droit d'aller et venir, ou la réinsertion. On en veut pour preuve la nouvelle loi de sécurité intérieure du 30 octobre 2017 généralisant certaines dispositions de l'état d'urgence, la suppression de certaines peines plus douces ou mesures alternatives pour les terroristes, le renforcement du suivi et de la surveillance de ceux-ci. Il ne serait donc pas impossible que le droit à la protection des données à caractère personnel de ces individus s'amenuise dans le cas où l'efficacité de la police prédictive contre le terrorisme venait à être prouvée.

De tels abus ont trop souvent été constatés, notamment aux États-Unis durant la période post 11 septembre 2001. Internationaliser la police prédictive signifie aussi octroyer encore plus de pouvoirs ; pouvoirs qui sont parfois détournés et utilisés à mauvais escient. Le tout premier travail à effectuer serait, entre les États, de réfléchir soit à des uniformisations, ou du moins à des accords de protection des données et des droits individuels lors de l'utilisation de l'intelligence artificielle à des fins antiterrorsites.

174. Qualité des données - L'un des biais de la police prédictive reste aussi la qualité des données utilisées. Andrew Guthrie Ferguson souligne par exemple que certes, le Big Data ne fait que grandir, néanmoins l'accès aux nouvelles technologies et les plateformes alimentant les sources de données ne sont pas accessibles à tous[206]. « *Bien que les partisans et les opposants tendent de manière générale à voir cette révolution* [la police prédictive] *comme se totalisant et étant universelle, la réalité est que des milliards de personnes restent en marge de celle-ci car elles ne sont pas couramment actives dans ces activités que le big data et les techniques analytiques ont vocation à enregistrer* »[207], ces personnes n'ayant pas les mêmes moyens sociaux et financiers pour accéder à ces activités. Cela crée donc des disparités dans la surveillance : les autorités ne se servent

[205] En matière de protection de la vie privée.
[206] A.G. FERGUSON, *op. cit* note 79, p.178
[207] « *Although proponents and skeptics alike tend to view this revolution as totalizing and universal the reality is that billions of people remain on its margins because they do not routinely engage in activities that big data and advanced analytics are designed to capture* », J. LERMAN, « Big Data and Its Exclusions », *Stanford Law Review Online*, 56, 2013

nécessairement que des données disponibles, ou alors à l'inverse du peu de données dont elles peuvent bénéficier, au risque de faire une analyse biaisée et précipitée.

Mais à l'inverse, la police prédictive tend à se concentrer pour l'instant sur un seul type de criminalité, en général les atteintes aux biens comme le vol ou le cambriolage, ou sur les crimes violents. On en vient à oublier d'autres types de criminalités comme la criminalité en col blanc. Or, la criminalité financière dépasse très souvent les frontières, comme l'exil fiscal. Au même titre que le terrorisme – bien que ces deux types de criminalités ne soient évidemment pas comparables – la délinquance en col blanc a tout intérêt à faire l'objet d'entraides étatiques et d'accords de partage de données. Les mouvements de capitaux caractérisant la plupart des infractions de cette criminalité, l'automatisation du traitement de ce type de données à un niveau international pourrait être une idée intéressante. La police prédictive serait alors conçue dans une dimension autre que la dimension locale certes, mais poursuivrait un but tout autre. Si l'intelligence artificielle « interétatique » venait à apparaître au sein d'organisations internationales, comme Europol, il faudrait en effet cloisonner ses attributions et définir très précisément quelles infractions anticiper.

L'utilisation du conditionnel est de mise ici en ce qu'une police prédictive transfrontière paraît à juste titre utopiste, dangereuse, voire impossible. Néanmoins fut un temps, les hypothèses d'Alan Turing étaient considérées comme folles ; désormais, l'existence d'une intelligence artificielle à proprement parler est un constat. Fut un temps, il existait plus d'opposants que de partisans aux outils internationaux que nos États possèdent maintenant pour lutter contre la criminalité et la barbarie.

Conclusion Partie II

Les exploits technologiques dont fait partie l'intelligence artificielle ont vocation à améliorer la vie de l'être humain, dans un grand nombre de secteurs d'activités. Telle est la philosophie derrière la police prédictive : améliorer le travail de la police en le rendant plus proactif. Inclure des logiciels prédictifs dans les commissariats aurait ainsi un impact non seulement sur leur travail de terrain, d'intervention, mais aussi sur les travaux d'enquêtes. En outre, si le travail et les résultats policiers se voient influencés par la police prédictive, cette dernière pourrait à coup sûr impacter tout autant le reste de la procédure pénale et de ses acteurs, à commencer par les magistrats et les parties au procès.

Cette hypothèse est à envisager dans le cas où ces techniques algorithmiques atteindraient l'ensemble du territoire d'un État. Si tel était le cas, les renseignements ne tarderaient pas à adopter ce nouvel outil.

Il est de plus avéré que les États travaillent déjà entre eux à l'échange de données dans le cadre de la lutte contre la criminalité transfrontalière : il est nécessaire de faciliter le flux de données tout en protégeant les droits et libertés des individus. Ainsi, des accords comme celui sur le PNR ont vocation à accélérer les procédures de lutte contre le terrorisme. Mais cet accord ouvre aussi de nouvelles perspectives prédictives. En effet, ces données étant issues de base commerciales, les sociétés privées ont souvent recours au profilage commercial. Or, une telle pratique pourrait s'avérer utile pour les États, afin d'anticiper le risque que pourrait présenter un individu, outre ses déplacements potentiellement suspects.

La ligne est effectivement fine entre les pratiques d'aujourd'hui, et l'innovation de demain en matière de police prédictive, qui pourrait à termes s'internationaliser.

Conclusion générale

La science a toujours eu vocation à servir la Justice. Les domaines d'expertise se sont multipliés au sein du procès pénal : médecine, psychiatrie, génétique, balistique … Il serait presque difficile de les dénombrer. L'exemple est aussi valable concernant les domaines informatiques et technologiques.

Dès la démocratisation des ordinateurs et d'internet, la police a dû se rendre à l'évidence : les délinquants et criminels s'adaptent aux évolutions technologiques, savent en tirer profit, voire en faire un terrain d'action. Ces ordinateurs et leurs processeurs sont des « boîtes à trésor » renfermant souvent des éléments indispensables à l'incrimination ou la relaxe. La facilitation des échanges grâce au monde virtuel accélère tout processus, permet l'anonymisation. Les formes de criminalité internationalisée en sont les premières bénéficiaires dans le monde pénal.

L'automatisation atteint dans la sphère judiciaire un niveau bien plus élevé que la simple informatisation des fichiers de police. Cette désormais connue intelligence artificielle a dépassé les plateaux de jeu de go ou d'échecs ; la sphère publique commence à y voir une utilité. Car ce sont bel et bien aux travaux d'Alan Turing que les scientifiques essaient de donner suite : recréer un cerveau artificiel le plus proche possible de celui de l'Homme. Les premiers travaux sur les réseaux de neurones furent un exploit.

Néanmoins, la technologie d'aujourd'hui semble même dépasser les capacités innées du cerveau humain. L'intelligence artificielle sert désormais l'Homme dans des tâches qui le dépassent, ou du moins l'aide à simplifier et améliorer ses activités. Telle a été la vocation première de la police prédictive ; analyser les données fournies à l'algorithme, afin de rendre le travail policier le plus proactif et neutre possible. Au point que l'on s'est imaginé que la machine corrigerait tous les biais des autorités répressives.

Au vu du succès américain de PredPol, une police prédictive « 3.0 » ne saurait tarder à apparaître. L'idéal dépeint dans le livre de Philip K. Dick semble alors ne plus être une simple utopie : la police prédictive voudrait que l'intelligence artificielle anticipe les faits et gestes de l'Homme.

Une ironie souvent représentée dans le cinéma et la littérature, en ce que la machine aurait vocation à savoir mieux que quiconque analyser son propre créateur. Alors même qu'il existe encore des zones d'ombre sur le cerveau humain, l'humanité voudrait le recréer artificiellement. Or, si l'effectivité d'une machine si puissante semble de plus

en plus possible, elle reste une création de l'Homme et sera donc toujours marquée de son sceau.

Les atteintes aux données à caractère personnel sont les premiers exemples de ces biais que la révolution technologique peut engendrer : le Big Data s'est formé parce que les individus alimentent des plateformes, sans toujours s'être doutés que leurs données circulaient dans ce monde virtuel. Ce Big Data et l'intelligence artificielle ont déjà été détournés à des fins commerciales, voire politiques, à la recherche d'un intérêt précis, mais au détriment de la vie privée des personnes.

Quelle serait la réaction populaire si ces données étaient utilisées à des fins de surveillance permanente ? La police prédictive, si elle n'est pas encadrée par les dirigeants étatiques et manipulée avec précaution, pourrait conduire à sa propre fin. Ou pire encore, tomber entre de mauvaises mains. Car le risque est aussi de faire un retour en arrière vers le déterminisme. En vouant une confiance aveugle à la machine, on pourrait en oublier le libre-arbitre et les facteurs socio-économiques, pour suspecter à tort une personne « à risque ».

Cette technologie prédictive et la circulation des données n'ont cependant pas que des mauvais côtés. Elles ont en effet un potentiel considérable pour le milieu pénal, judiciaire et la sécurité publique. Les États du monde entier faisant face à des problématiques terroristes, la facilitation des échanges de données s'avère toute aussi utile à la prévention et à la lutte contre cette criminalité transfrontalière. L'entraide est certaine et nécessaire ; mais l'harmonisation est encore lointaine. Les accords se multiplient mais ils pourraient être encore plus efficaces si les États protégeaient de façons égales leurs données. Le risque reste en effet que certaines données personnelles soient utilisées dans le cadre d'une politique beaucoup trop sécuritaire, faussant l'équilibre indispensable entre respect des droits fondamentaux et protection de la sécurité publique.

Car le grand enjeu pour les acteurs pénaux est la célérité des progrès sur l'intelligence artificielle. La police prédictive se nourrit de ces progrès, qui vont à une vitesse parfois trop importante pour que les autorités judiciaires ne puissent s'adapter à temps. Néanmoins, les entités juridiques et répressives ont désormais conscience de cette rapidité ; elles ne peuvent qu'anticiper.

En effet, l'anticipation semblerait être la seule clef de la bonne utilisation d'une technologie qui se veut – ironiquement – prédictive.

L'automatisation et l'introduction de l'intelligence artificielle dans tous les corps de métier effraient en ce que la machine pourrait remplacer l'Homme. Il est évident qu'elle ne le pourra jamais dans certains domaines, où il faut qu'elle reste un outil plus qu'une doublure : la justice pénale en est l'exemple parfait.

De l'instinct policier en passant par la rhétorique de l'avocat, de la sagesse du juge en passant par les libertés du justiciables, il est de ces qualités qu'on ne pourra jamais retranscrire artificiellement.

L'arrivée de la police prédictive dans le milieu pénal, couplée à celle de la justice prédictive, se doit d'être modérée dans ce pan du droit des plus humains qu'il soit. Au risque que la machine, comme le disait Stephen Hawking, mène à la perte de l'Homme.

Bibliographie

Ouvrages généraux

• A. BENSOUSSAN, *Règlement européen sur la protection des données : textes, commentaires et orientations pratiques*, 2ème Edition, Ed. Bruylant, 2018
• G. DESGENS-PASANAU, *La protection des données personnelles*, 2ème édition, LexisNexis, 2015
• S. GUNICHARD et T. DEBARD, *Lexique des termes juridiques*, 21e édition, Dalloz, 2014

Ouvrages spéciaux

• A. BAUER, C. SOULLEZ et A.M. VENTRE, *Mieux contrôler les fichiers de police pour protéger les libertés*, Rapport au Ministère de l'intérieur, Paris, La documentation française, 2009
• A.G. FERGUSON, *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement*, New York, New York University Press, 2017
• A.M. TURING, Computing Machinery and Intelligence, *Mind*, 1950
• CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, Luxembourg, 2014
• J.J. LAVENUE et B. VILLALBA, *Vidéo-surveillance et détection automatique des comportements anormaux. Enjeux techniques et politiques.*, Collection Espaces Politiques, Presses Universitaires du Septentrion, 2011
• SOUS LA DIRECTION DE C. CASTETS-RENARD, *Quelle protection des données personnelles en Europe ?*, Collection Europe(s), Editions Larcier, 2015

Articles de doctrine

• A. ROUSSELET-MAGRI, « Les perquisitions "informatiques" à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données », *RSC*, février 2018, n°4, pp. 659-676
• B. WARUSFEL, « Procédure pénale et technologie de l'information : De la Convention sur la Cybercriminalité à la Loi sur la sécurité quotidienne », *Droit & Défense*, 2002

• C. CASTETS-RENARD, « Quels liens établir entre les USA et l'UE en matière de vie privée et protection des données personnelles ? », *Dalloz IP/IT*, 2016, p.115
• D. THOMAS, « Le nouveau fichier national des auteurs d'infractions terroristes », *AJ Pénal*, novembre 2015, n°11, p.523
• M. GAMBARAZA et A. RODD, « Le statut juridique de la déclaration universelle des droits de l'Homme dans les États de droit anglo-saxon », *Droits fondamentaux*, 2010, n°8
• M. LENA, « Les attentes liées à l'entrée en vigueur du Traitement des antécédents judiciaires », *AJ Pénal*, décembre 2013, n°12
• M. QUEMENER, « Les dispositions en lien avec le numérique de la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme », *Dalloz IP/IT*, décembre 2017, n°12, p.657
• PIERRE-YVES MAROT, « Fonctions et mutations des fichiers de police », *AJ Pénal*, février 2007, p.61
• RAOUL UEBERECKEN, « Un feuilleton à rebondissements : l'affaire Swift », *Revue du marché commun de l'Union européenne*, 2010, p.566
• SYLVIE PEYROU-PISTOULEY, « L'affaire Marper c/ Royaume-Uni : un arrêt fondateur pour la protection des données dans l'espace liberté, sécurité, justice de l'Union européenne », *RFDA*, juillet 2009, n°4, p.741
• VIRGINIE GAUTRON, « FNAEG : l'inertie gouvernementale sanctionnées par la CEDH », *AJ Pénal*, septembre 2017, n°9, p.391
• VIRGINIE GAUTRON, « Usages et mésusages des fichiers de police : la sécurité contre la sûreté ? », *AJ Pénal*, juin 2010, n°6, p.266
• YANNICK MEILLER, « Intelligence artificielle, sécurité et sûreté », *Sécurité et Stratégie*, 2017, vol. 4, n°28, pp.75-84

Articles anglo-saxons

• A. RUMMENS, W. HARDYNS et L. PAUWELS, « The use of predictive analysis in spatiotemporal crime forecasting: Building and testing a model in an urban context », *Applied Geography*, 2017, n°86, pp.255-261
• A. WINSTON, « Palantir has secretly been using New Orleans to tests its predictive policing technology », *The Verge*, February 2018, <https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd>

• A.A. BRAGA, D. WEISBURD et B. TURCHAN, « Focused Deterrence Strategies and Crime Control. An Updated Systematic Review and Meta-Analysis of the Empirical Evidence », *Am. Soc. Of Crim*., 2018, vol. 17, n°1, pp.205-250
• A.G. FERGUSON, « Policing Predictive Policing », *Emory L. J.*, 2017, vol. 94, n°5
• A.G. FERGUSON, « Predictive Policing and Reasonable Suspicion », *Emory L. J.*, 2012, vol. 62, n°259, pp.259-325
• A.G. FERGUSON, « Predictive Prosecution », *Wake Forest L. Rev*., 2016, vol. 51, p.705
• A.M. TURING, « Computing Machinery and Intelligence », *Mind*, 1950
• B. BÎRZU, « Prevention, detection, investigation and prosecution of terrorist offenses and other serious crimes by using Passenger Name Record (PNR) data. Critical opinions. De lege ferenda proposals », *Perspectives of Business L. J.*, November 2016, vol. 5, n°1, pp.195-206
• B. CLIFTON, S. LAVIGNE et F. TSENG, « Predicting Financial Crime: Augmenting the Predictive Policing Arsenal », *The New Enquiry*, April 2017
• B. HEATON, « Predictive Policing a Succes in Santa Cruz, Calif. », *Gov. Tech*., October 8th 2012, <http://www.govtech.com/public-safety/predictive-policing-a-success-in-santa-cruz-calif.html>
• B. HEATON, « Behavioral Data and the Future of Predictive Policing », *Gov. Tech*., 2012, <http://www.govtech.com/Behavioral-Data-and-the-Future-of-Predictive-Policing.html>
• B. PEARSALL, « Predictive Policing: The Future of Law Enforcement? », *NJ Journal*, n° 266
• B. POSTON, « Crime in Los Angeles Rose in All Categories in 2015, LAPD Says », *L.A. Times*, 2015, <http://www.latimes.com/local/crime/la-me-crime-stats-20151230-story.html>
• C. BLASI CASAGRAN, « The future EU PNR System: Will Passenger Data be Protected? », *European J. of Crime, Criminal L. and Criminal Justice*, 2015, vol. 23, pp.241-257
• C.B. SANDERS et J. SHEPTYCKI, « Policing, crime and "big data"; towards a critique of the moral economy of stochastic governance », *Crime Law Soc. Change*, January 2017, n°68, pp.1-15
• E. NISSAN, « Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement », *Al & Soc*., 2017, n°32, pp.441-464

• E.E. JOH, « The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing », UC Davis Legal Studies Research Paper, *Harvard Law & Policy Rev.*, 2015, n°473
• EDITORIAL BOARD, « Editorial: Who will kill or be killed in violence-plagued Chicago? The algorithm knows », *Chicago Tribune*, May 2016, <http://www.chicagotribune.com/news/opinion/editorials/ct-gangs-police-loury-algorithm-edit-md-20160510-story.html>
• G. BECKER, « Crime Punishment: An Economic Approach », *University of Chicago and National Bureau of Economic Research,*1974
• G. ZANFIR, « EU and US Data Protection Reforms. A comparative View », The 7th Edition of the International Conference, *European Realities and Perspectives*, 2012
• G.O. MOHLER ET AL., « Randomized Controlled Field Trials of Predictive Policing », *Journal of American Statistics Association*, 2015, n°1399
• INTERNATIONAL ASSOCIATION OF CRIME ANALYSTS, « Definition and Types of Crime Analysis. », White Paper 2014-01, Overland Park, October 2014
• J. LERMAN, « Big data and Its Exclusions », *Stanford L. Rev. Online*, September 3rd 2013, n°56
• M. REZA KEYVANPOUR, M. JAVIDEH et M. REZA EBRAHIM, « Detecting and investigating crime by means of data mining: a general crime matching framework », *Procedi Computer Science*, 2011, n°3, pp.872-880
• M.S. SCOTT, « Focused Deterrence of High-Risk Individuals *»,* Response Guide n°13 *Center for Problem-Oriented Policing*, 2017
• P. AICHROTH *et al.*, « Benefits and Pitfalls of Predictive Policing », Conference Paper, 2015
• P.J. BRANTINGHAM, M. VALASIK et G.O. MOHLER, « Does Predictive Policing Lead to biased Arrests? Results From a Randomized Controller Trial », *Statistics and Public Policy Journal*, 2018, vol. 5, n°1
• S. D. JOHNSON *et al.*, « Space-Time Patterns of Risk: A Cross National Assessment of Residential Burglary Victimization », *J. Quant Crimin.,* 2007
• S. GOEL *et al.*, « Combatting police discrimination in the age of big data », *New Crim. Law Rev.*, 2017, n°181
• W. WELLS et L. WU, « Proactive policing effects on repeat and near-repeat shootings in Houston », *Police Quarterly*, vol. 14, n°3, pp.298-319

Rapports

• A.A. BRAGA, « SMART Approaches to Reducing Gun Violence », Bureau of Justice Assistance, U.S. Department of Justice, 2014

• B. CHABANEL, « Big Data et action publique : l'exemple de la police prédictive », Lyon, Données et services, Direction de la prospective et du dialogue public, mars 2016

• C. VILLANI, « Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne », 8 septembre 2017

• Rapport d'information n°4113 sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police, D. BATHO et J.A. BENISTI, Assemblée Nationale

• Report from the Commission to the European Parliament and the Council, on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, EUROPEAN COMMISSION, COM(2017) 29 final, January 2017

• Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, EUROPEAN COMMISSION, COME(2017) 31 final, January 2017

• Predictive Policing Recommendation paper, EUROPEAN CRIME CONVENTION NETWORK, ECPN, 29 novembre 2016

• Europol Review 2016-2017, European Union for Law Enforcement Cooperation, 2017

• INSTITUT NATIONAL DES HAUTES ETUDES DE LA SECURITE ET DE LA JUSTICE, « Vers une police 3.0 : enjeux et perspectives à l'horizon 2025 », 27e session nationale « Sécurité et Justice », Groupe de diagnostic stratégique n°3, 2016 2015

• J. BACHNER, « Predictive Policing. Preventing Crime with Data and Analytics », Center for advanced Governmental Studies, Johns Hopkins University, 2013

• Compte rendu de la deuxième séance du 11 février 2014, J.O. DEBATS ASSEMBLEE NATIONALE

• J.M. CAPLAN et L.W. KENNEDY, « Risk Terrain Modeling Compendium for Crime Analysis », Newark, New Jersey, Rutgers Center on Public Security, 2011

• J.E. ECK *et al.*, « Mapping Crime: Understanding Hot Spots », U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 2005

• META Group, « Controlling Data Volume, Velocity and Variety », 2001

• Intelligence-Led Policing Report, M. PETERSON, Department of Justice, 2005
• Predictive Policing Symposiums, NATIONAL INSTITUTE OF JUSTICE, 2010 2009
• P. AICHROTH *et al.*, « Benefits and Pitfalls of Predictive Policing », 2015
• P. PERROT, « What about AI in criminal intelligence? From predictive policing to AI perspectives », 2017, n°16
• Rapport n°386 sur le projet de loi autorisant l'approbation de l'accord sous forme d'échange de lettres entre le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique relatif au renforcement de la coopération en matière d'enquêtes judiciaires en vue de prévenir et de lutter contre la criminalité grave et le terrorisme, P. BAUMEL, Assemblée Nationale, 27 janvier 2016
• Rapport n° 3443 fait au nom de la Commission des affaires étrangères sur le projet de loi autorisant l'approbation de l'accord sous forme d'échange de lettres entre le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique relatif au renforcement de la coopération en matière d'enquêtes judiciaires an vue de prévenir et de lutter contre la criminalité grave et le terrorisme, P. BAUMEL, Assemblée nationale, 27 janvier 2016
• SHELBY COUNTY DISTRICT ATTORNEY GENERAL, « Four Area Hotels Closed for Business Following "Operation Heartbreak Hotel" », 2008
• U.S. DEPARTMENT OF JUSTICE, « The National Criminal Intelligence Sharing Plan », Washington D.C., October 2003
• W. L. PERRY *et al.*, « Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations », RAND Corporation, 2017

Textes

- **Nationaux**

• Article 230-6 du Code de procédure pénale
• Code de la sécurité intérieure, Article 5232-12
• Constitution de 1958
• Décret n°85-1203 portant publication de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 15 novembre 1985
• Loi n°2004-801 modifiant la loi du 6 janvier 1978, 6 août 2004
• Loi n°2011-264, 14 mars 2011
• Loi n°2016-1321 pour une République numérique, 7 octobre 2016

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

- **Européens**

• Accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, 14 juillet 2012, Journal officiel de l'Union européenne

• Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance de financement du terrorisme, 27 juillet 2010, Journal officiel de l'Union européenne

• Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis d'Amérique aux fins du programme de surveillance du financement du terrorisme, 13 janvier 2010, Journal officiel de l'Union européenne

• Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) per les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007), 4 août 2007, Journal officiel de l'Union européenne

• Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite en la matière, 10 décembre 2016, Journal officiel de l'Union européenne

• Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère de la sécurité intérieure, 11 août 2012, Journal officiel de l'Union européenne

• Charte des droits fondamentaux de l'Union européenne, 7 décembre 2000

• Convention européenne de Sauvegarde des droits de l'Homme, 1953

• Convention pour la protection des données à caractère personnel (STE n°108), 28 janvier 1981

• Décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (Décision de Prüm), 23 juin 2008, Conseil de l'Union européenne

• Décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, 23 juin 2008, Conseil de l'Union européenne
• Décision relative à la conclusion entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme du financement du terrorisme (2010/412/UE), 13 juillet 2012, Conseil de l'Union européenne
• Décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, 27 novembre 2008, Conseil de l'Union européenne
• Décision-cadre 2009/315/JAI concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres, 26 février 2009, Conseil de l'Union européenne
• Décision-cadre 2009/315/JAI concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres, 26 février 2009, Conseil de l'Union européenne
• Directive (UE) 2016/680 du 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 des données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, 27 avril 2016, Parlement européen et conseil
• 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, 27 avril 2016, Parlement européen et conseil
• Directive 2004/82/CE concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, 29 avril 2004, CONSEIL DE L'UNION EUROPEEN
• Directive européenne n°95/46/CE 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, 24 octobre 1995, Parlement européen et conseil
• Recommandations Rec(87)15, septembre 1987, Comité des ministres
• Règlement (CE) n°1987/2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), 20 décembre 2006, Parlement européen et Conseil

• Règlement (UE) 2016/679 du relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), 27 avril 2016, Parlement européen et Conseil
• Traité sur le fonctionnement de l'Union européenne, Lisbonne, 2007

- **Internationaux**

• Déclaration universelle des droits de l'Homme de 1948, Assemblée Générale des Nations Unies
• Résolution 45/95, 14 décembre 1990, Assemblée Générale des Nations Unies
• Résolution sur la décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record) à des fins répressives, 20 novembre 2008, Parlement européen

- **Américains**

• Code of Federal Regulations
• Treaty on mutual legal assistance in criminal matters between the United States of America and France, December 1998, Department of State, United States of America
• United States Bill of Rights, 1789, J. MADISON

Jurisprudence

- **Nationale**

• Cass. Crim. Arrêt Isnard, 22 janvier 1953
• Cons. constit.., Décision n°99-416 DC loi portant création d'une couverture maladie universelle, 23 juillet 1999
• Cons. constit., Décision n°2010-25 QPC, 16 septembre 2010
• Cons. constit., Décision n°2012-652 DC, 22 mars 2012
• Cons. constit., Décision n°2016-611 QPC, 10 février 2017
• TGI Grenoble, 3 octobre 2017, n°2204/17CJ
• Cons. constit., Décision n°2017-670 QPC, 27 octobre 2017
• Cons. constit., Commentaire de la décision n°2017-670 QPC du 27 octobre 2017
• Cons. constit., Décision n° 2017-682 QPC, 15 décembre 2017

- **Européenne**

• CJCE, Osterreichischer Rundfunk, 20 mai 2005, Aff. C-405/00 et C-139/01

• CEDH, Vetter c. France, 31 mai 2005, n°58842/00

• CEDH, GRANDE CHAMBRE, S. et Marper c. Royaume-Uni, 4 décembre 2008, n°30562/04

• CEDH, B.B. c. France, 17 décembre 2009, n°5335/06

• CEDH, M.K. c. France, 18 avril 2013, n°19522/09

• CJUE, Digital Rights Ireland, 8 avril 2014, Aff. C-293/12 et C-594/12

• CEDH, Brunet c. France, 18 septembre 2014, n°2101/10

• CJUE, Digital Rights Europe, 8 avril 2015, Aff. C-293/12 et C-594/12

• CEDH, Aycaguer c. France, 22 juin 2017, n°8806/12

• CEDH, Ben Faiza c. France, 8 février 2018, n°31446/12

- **Américaine**

• U.S. Supreme Court, Meyer v. Nebraska, 1923, 262 U.S. 390

Articles de presse

• H. GUILLEAU, « Vers une police prédictive responsable ? », 2017, <http://www.internetactu.net/2017/07/26/ou-en-est-la-police-predictive/>

• J. ANGWIN *et al.*, « Machine Bias », *Propublica*, mai 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

• J. HOURDEAUX, « Gendarmes et industriels imaginent un nouveau logiciel pour prédire le crime », *Médiapart.fr*, mai 2015.

• J. JOUVENAL, « The new way police are surveilling you: Claculating your threat "score" », *The Washington Post*, janvier 2016, <https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?noredirect=on&utm_term=.d3d5cce516a7>. .

Sites internet

• https://www-01.ibm.com/software/analytics/spss/11/na/cpp/

• http://www.cil.cnrs.fr/CIL/spip.php?rubrique362

• https://www.cnil.fr/fr
• https://www.larousse.fr/dictionnaires/francais
• https://www.hunchlab.com/
• http://www.predpol.com/
• http://www.palantir.com/

Divers

• CNRS Le Journal, « L'héritage d'Alan Turing », Hors-série mai 2012
• 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 », Strasbourg, Conseil de l'Europe, 15 février 2018
• OCDE, « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel », 23 septembre 1980

Index

Table des matières

Résumé

La Justice pénale doit faire face aux nouveaux enjeux culturels, géopolitiques, juridiques mais aussi technologiques de notre monde moderne. Ces derniers s'illustrent principalement par l'émergence du Big Data et les progrès en matière d'intelligence artificielle. Les sources et flux de données se multiplient, bénéficiant souvent au secteur privé, qui peut adapter ses stratégies commerciales. Mais le Big Data s'avère aussi utile pour les autorités publiques : le traitement des données personnelles permet la surveillance voire la prévention de certains profils et comportements. Grâce à l'utilisation de l'intelligence artificielle, il devient beaucoup plus simple de s'y retrouver dans cet ensemble de méga données. C'est ainsi que sont apparues des techniques de prédiction, et notamment au service du travail policier. Prônant l'amélioration, l'efficacité et la proactivité, la police prédictive est parfois érigée au rang d'utopie. Les États-Unis, précurseurs de ces techniques, ont malheureusement été le théâtre des biais de la machine. Qui plus est, la police prédictive commence à passer les frontières européennes ; l'Union européenne assurant cependant une meilleure protection des données à caractère personnel que l'État américain. Si les techniques prédictives venaient à se démocratiser, elles pourraient aller au-delà du simple niveau local. Assisterait-on à la montée d'une l'intelligence artificielle transfrontière ? La police prédictive, au potentiel majeur pour les acteurs judiciaires, est cependant à manipuler avec une extrême précaution.

Mots-clés : algorithme, Big Data, criminalité internationale, données à caractère personnel, fichiers de police, flux de données, intelligence artificielle, police prédictive

Abstract

In our modern world, criminal justice has to face new cultural, geopolitical, legal challenges as well as technological ones. The latter mainly illustrates the rise of Big Data and the artificial intelligence related progresses. The data sources and streams multiply and often benefit the private sector, that can adjust its commercial strategies. But it turns out Big Data can also be useful to the public authorities: personal data processing provides surveillance and even prevention of some profiles and behaviors. Thanks to artificial intelligence work, analyzing these massive data groups becomes a lot easier. That is how the prediction techniques appeared, including in the field of policing. Because predictive policing theories advocate improvement, efficiency and proactivity, they are sometimes seen as utopic. The United-States have been pioneers of these methods but, unfortunately, have also been a great theatre of machine bias. Furthermore, predictive policing is starting to cross the European borders; the European Union is however more protective of personal data than the U.S. are. If predictive techniques came to democratize, they could exceed the local level. Are we spectators of an artificial intelligence rise to the cross-border level? Predictive policing has a major potential for judiciary actors, however it should be handled very carefully.

Key words: algorithm, Big Data, transnational crime, personal data, police files, data stream, artificial intelligence, predictive policing