LA POLICE PRÉDICTIVE

ENJEUX SOULEVÉS PAR L'USAGE DES ALGORITHMES PRÉDICTIFS EN MATIÈRE DE SÉCURITÉ PUBLIQUE

AVRIL 2019
20.18.01
ISBN 9 78 2 7371 2130 2

www.iau-idf.fr

IAU
INSTITUT D'AMÉNAGEMENT ET D'URBANISME
îledeFrance

LA POLICE PRÉDICTIVE

Enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique

Avril 2019

IAU île-de-France
15, rue Falguière 75740 Paris cedex 15
Tél. : + 33 (1) 77 49 77 49 - Fax : + 33 (1) 77 49 76 02
http://www.iau-idf.fr

Directeur général : Fouad Awada
Mission Prévention Sécurité : Sylvie Scherer, directrice
Étude réalisée par Camille Gosselin, chargée d'études urbaniste
N° d'ordonnancement : 20.18.01

Remerciements : à toutes celles et ceux qui ont accepté d'échanger et d'accorder de leur temps pour cette étude. Ce travail n'aurait pu se faire sans leurs contributions.

Sommaire

Introduction

Contrôler toute une ville à partir d'une salle de commandement, suivre des individus depuis un mur d'écrans, utiliser l'intelligence artificielle pour cibler les situations ou les comportements jugés « anormaux », ou pour orienter les patrouilles vers les territoires où de futurs délits se produiront : telles sont les promesses véhiculées par la police prédictive, et plus largement, portées par l'ensemble du mouvement *smart city* qui intègre des enjeux liés à la tranquillité et sécurité publiques. Les *big data* couplées aux techniques de l'intelligence artificielle nourrissent ainsi de nouvelles ambitions. Au niveau local, la production et la gestion de données dédiées à l'insécurité sont des pratiques répandues[1] ; néanmoins, chez nombre d'acteurs (forces de l'ordre, collectivités territoriales, sociétés privées, etc.), les nouvelles technologies alimentent les aspirations d'analyse et de prédiction des faits de délinquance. La police prédictive en constitue l'un des développements les plus attendu. Son objectif principal est d'anticiper les faits avant qu'ils ne se produisent réellement, en utilisant notamment des données ouvertes et celles produites par les services de sécurité. Cela semble possible grâce à l'usage des algorithmes et des techniques d'apprentissage automatique, couramment utilisés dans d'autres domaines comme celui de la finance ou des assurances. Les projets et expériences actuels de police prédictive tentent ainsi de produire des modèles de prévision des faits de délinquance, dans le temps et dans l'espace. La prédiction du crime n'est pas un sujet nouveau. Le champ académique s'y est déjà intéressé par le passé. Dans les années 1920, par exemple, le sociologue américain Ernest Burgess, l'un des fondateurs de l'École de Chicago, cherchait, entre autres, à "prédire" les comportements déviants en se fondant sur des variables statistiques.

L'ère des *big data*

Cette volonté prédictive prend une autre ampleur sous l'ère des *big data* qui promettent des réponses plus exhaustives et efficaces. En France, les travaux de la philosophe Antoinette Rouvroy soulignent les enjeux posés par l'enregistrement systématique de données, la multiplication des traces digitales dans notre société, concourant à « une transformation des rationalités, stratégies et tactiques de gouvernement [2]». Elle parle ainsi de « gouvernementalité algorithmique », et déconstruit « l'idéologie technique propagée par les *big data* » selon laquelle, les données permettraient d'accéder à un monde « objectivé », au réel tel qu'il est. La chercheuse insiste sur l'importance de nommer les biais inhérents aux données, qui traduisent, en partie, le système de valeurs des humains impliqués dans leur collecte, leur sélection et leurs utilisations, et qui peuvent donc refléter des discriminations racistes, sexistes ou sociales. Antoinette Rouvroy remet ainsi en question leur neutralité présumée et rappelle l'intérêt de pouvoir accéder à leurs sources. Elle met également en avant, la nécessité de comprendre la production des algorithmes et de travailler à leur transparence, c'est-à-dire d'en saisir les métriques, le poids accordé à un certain type de données. Ces métriques, décidées par des ingénieurs, doivent être explicitées, pour que puisse s'opérer une critique voire une « auditabilité » des processus algorithmiques.

En France, la mise en œuvre d'outils prédictifs dans le champ de la sécurité, rejoint la question de l'efficacité des services policiers et les préoccupations managériales qui traversent cette profession. La diffusion d'outils de gestion de la performance policière affecte l'ensemble des polices occidentales, à commencer par les États-Unis, où ils connaissent un fort développement au cours des années 1990. Les données informatisées des faits de délinquance servent notamment à établir des priorités d'action, à fixer des objectifs, à optimiser les ressources sur des secteurs géographiques précis, etc. Ces stratégies véhiculent des contraintes économiques et managériales dans lesquelles les outils technologiques, « l'innovation », tentent d'apporter des solutions. Le sujet de la police prédictive se développe ainsi dans des conditions, où, d'une part, les forces de l'ordre sont toujours plus interpellées quant à leur efficacité notamment dans un contexte de tensions sociales et de menaces terroristes récurrentes, et, d'autre part, où la réglementation se renforce quant à la protection des données à caractère personnel[3]. La police prédictive éveille ainsi bon nombre de représentations et de craintes. Pourtant l'intérêt qu'elle suscite est révélateur d'un engouement qui affecte, aussi bien, les acteurs classiques du champ de la prévention-sécurité, tant publics que privés, que les acteurs économiques.

[1] Gosselin C., Données numériques et gestion locale de la sécurité, production et usages de bases de données chez les acteurs locaux, IAU îdF, février 2018.

[2] Rouvroy A., Berns T., « Le nouveau pouvoir statistique ou quand le contrôle s'exerce sur un réel normé, docile et sans évènement car constitué de corps "numériques" … », 2010.

[3] Le Règlement européen sur la protection des données (RGPD) entré en application le 25 mai 2018, poursuit trois objectifs : renforcer les droits des personnes, responsabiliser les acteurs traitant des données et crédibiliser la régulation.

Qu'est-ce que la « police prédictive » ?

Le terme de police prédictive retenu pour cette étude ne signifie rien d'académique. Il s'agit à la fois d'un titre accrocheur (relativement explicite) et d'une mauvaise traduction de l'anglais *predictive policing*. Récemment, en France, l'expression « police prédictive » a de façon récurrente été utilisée par la presse ou par l'État, dans l'objectif notamment de promouvoir ce genre de dispositif associé à la modernisation de l'action publique. Néanmoins, quand il s'agit de donner du contenu et d'évoquer ce qui est réellement développé par les services de l'État au nom de la police prédictive, il est plus difficile de voir concrètement ce qu'elle revêt. Elle est, par ailleurs, souvent associée à des éléments de langage qui minimisent ses ambitions prédictives. En ce sens, elle est régulièrement qualifiée « d'outil d'aide à la décision », ou présentée comme « un outil parmi d'autres »[4]. Par ailleurs, les interlocuteurs rencontrés dans le cadre de cette étude prennent souvent leur distance avec la notion de « police prédictive » jugée « trop marketing » et trop éloignée des enjeux du terrain. Dans le contexte américain, elle s'inscrit dans l'histoire des réformes visant à développer la proactivité des forces de police, intervenant en amont des problèmes, et non pas dans l'urgence en réaction aux alertes lancées par les citoyens. De ce point de vue, le *predictive policing* s'inscrit donc pleinement dans une logique de prévention et d'anticipation des faits de délinquance, assez éloignée des représentations inspirées par les nombreuses fictions qui lui sont souvent associées.

Cette étude regroupe, sous le terme de police prédictive, des expérimentations qui, à l'image de celle actuellement menée au sein de la gendarmerie nationale, concerne en priorité les missions des forces de sécurité. Mais, dans une acception plus large, ce sont bien tous les dispositifs « intelligents » annoncés comme prédictifs et conçus pour renforcer la sécurisation et le contrôle des espaces publics, dont il sera question.

La police prédictive aux États-Unis

En France, en 2015, de nombreux médias s'intéressent à la « prédiction du crime », à ce qui leur paraît être un réel changement de paradigme, bouleversant les modes d'interventions et les ambitions des polices. Au même moment, aux États-Unis, la police prédictive se développe et de nombreuses polices américaines ont recours à des nouveaux logiciels en ce sens. Le plus connu est développé par une *start-up,* Predpol, qui commercialise un logiciel d'anticipation des faits de délinquance. Son objectif : permettre d'orienter les patrouilles sur des zones identifiées « sensibles » et éviter le passage à l'acte du criminel. Présentée sous forme de cartes de chaleur représentant la répartition spatiale de la délinquance, l'innovation de Predpol repose sur l'usage d'un algorithme qui, pour rendre la police plus proactive, l'a fait intervenir dans les secteurs précis où se concentre le crime. Predpol n'est pas la seule société à proposer ce type de service ; la police prédictive est un véritable marché, où grands groupes et *start-up* se côtoient.

Les travaux du sociologue Bilel Benbouzid permettent à la fois d'appréhender ce marché, et de décrypter le fonctionnement des logiciels prédictifs et de leurs algorithmes. Le chercheur alerte également sur les biais de cette technique appliquée au domaine de la sécurité publique, en travaillant notamment sur l'auditabilité de l'algorithme de Predpol. Pour cela, il s'est intéressé au sens de l'algorithme, et à la façon dont l'entreprise envisage la sécurité et la criminalité. Pour Predpol, la sécurité est une quantité, et l'algorithme est envisagé comme un dosomètre qui permet de mesurer la bonne quantité de patrouilles pour prévenir le crime sur un secteur ciblé. Pour orienter les patrouilles, Predpol introduit au sein de l'algorithme des métriques qui, selon Bilel Benbouzid, s'articulent, entre autres, autour de trois dimensions :

- La contagion de la criminalité. Tenu secret par l'entreprise, l'algorithme de Predpol s'inspire d'un algorithme utilisé dans le domaine de la sismologie et plus spécifiquement dans la prédiction des répétitions des tremblements de terre[5]. L'hypothèse retenue est que le crime ne se produit pas par hasard, et que « le meilleur prédicteur » des crimes à venir résulte des crimes passés. L'entreprise ajoute également une mesure de la contagion du crime, c'est-à-dire une dépendance spatio-temporelle : les crimes sont dépendants les uns des autres et se déplacent de proche en proche. Toute l'innovation de Predpol repose sur cette idée de contagion de la criminalité, à l'origine de son discours marketing, *Predpol : More Than Just Hot Spot Policing*.

- L'optimisation des ressources policières. L'algorithme fonctionne comme un outil de gestion de l'action des policiers. Il oblige les patrouilles de police à passer 5% de leur temps disponible dans les zones à risques identifiées (des carrés rouges de 200 mètres sur 200 mètres). Ce dosage du temps

[4] Ministère de l'Intérieur, « Appel à projets d'études stratégiques et prospectives », 2018

[5] Benbouzid B., « De la prévention situationnelle au predictive policing. Sociologie d'une controverse ignorée », 2015.

de présence des policiers est effectué en temps réel et selon les secteurs de la ville. Cette rationalisation des interventions des agents de police va de pair avec une réflexion plus globale de retour sur investissement. Pour que l'algorithme puisse prioriser les interventions et orienter les patrouilles, il s'agit de calculer de façon pragmatique le coût de l'intervention de la police (agents mobilisés, durée de l'enquête, etc.), et *in fine* le coût de la criminalité pour la société civile[6].

- La quantification de « faux positifs » acceptables. Predpol introduit dans son algorithme un enjeu de justice sociale. Dans le cadre de ses missions, la police est amenée à effectuer un certain nombre de contrôles. Parmi les personnes contrôlées figurent des innocents. L'algorithme tente de répondre à la question : « jusqu'où la police peut-elle contrôler ? », c'est-à-dire qu'il cherche à calculer « une discrimination acceptable ».

Ces métriques traduisent l'orientation donnée à l'algorithme et le sens que revêt la police prédictive de Predpol, et semblent renforcer des dynamiques déjà à l'œuvre au sein de cette profession[7]. Bilel Benbouzid va même plus loin en affirmant : « D'une application construite au sein du système d'information de la police cherchant à aider les policiers à explorer des hypothèses et des intuitions, on passe à une application beaucoup plus externe qui prédit automatiquement et, partant, fait disparaître la dimension réflexive de la proactivité »[8]. Plus largement, le chercheur discute et questionne le réel changement de paradigme qui serait insufflé par la police prédictive.

Une démarche exploratoire

Cette étude constitue un premier travail sur la manière dont est défini et traité le sujet de la police prédictive en France. Initialement, l'ambition était de mettre à plat l'ensemble des dispositifs existants, d'en proposer un état des lieux tant sur leur fonctionnement que sur leurs usages concrets au sein des différentes organisations investissant le sujet : gendarmerie et police nationales, collectivités territoriales, etc. Seulement, par-delà l'effet d'annonce qu'elle peut susciter, la police prédictive est aussi considérée comme un sujet sensible, et il s'est avéré difficile d'enquêter et d'accéder aux informations. Les interlocuteurs contactés au sein de la police nationale et de certaines collectivités territoriales n'ont, par exemple, pas donné suite à nos nombreuses relances. Seuls plusieurs agents de la gendarmerie nationale ont bien voulu nous rencontrer et échanger sur le projet actuellement engagé au sein de leur administration. De ce fait, l'étude n'est pas représentative de l'ensemble des démarches entreprises dans ce secteur en France, ni même de l'ensemble des postures des acteurs de la sécurité publique. Néanmoins, elle vise à présenter les principaux enjeux soulevés par les ambitions de la police prédictive et sa mise en œuvre.

L'essentiel de l'enquête a été réalisé entre mai et septembre 2018. Au sein de la gendarmerie nationale, nous avons pu échanger sur les pratiques prédictives avec le centre de recherche de l'école des officiers de la gendarmerie nationale (CREOGN). Celui-ci nous a ouvert les portes pour obtenir les retours du service central de renseignement criminel (SCRC), en charge notamment du développement d'une plateforme prédictive. C'est ainsi que nous avons pu récolter les témoignages de commandants de groupement qui ont participé à l'expérimentation de cet outil. Nous avons par la suite recueilli des témoignages auprès d'institutions publiques telles que la commission nationale de l'information et des libertés (CNIL), la mission Etalab, et l'institut national des hautes études de la sécurité et de la justice (INHESJ), et dans le monde de la recherche. Au total, une dizaine de personnes ont été rencontrées ou interviewées par téléphone, dans l'objectif de recueillir leurs points de vue ou l'état actuel de leurs réflexions sur le développement de la police prédictive en France.

Cette étude comprend bien des limites : elle ne présente pas l'ensemble des initiatives prédictives dans le domaine de la sécurité, et elle ne prétend pas comprendre "de l'intérieur" le fonctionnement des algorithmes en tant que tels. Elle a principalement pour objectif de croiser les regards sur l'essor des outils prédictifs dans le domaine de la sécurité. Pour cela, elle revient sur la définition des termes du sujet, sur les éléments de la réglementation française concernant l'intelligence artificielle (IA), et sur la posture des acteurs tant publics que privés qui investissent ce champ (Partie I). L'étude permet aussi d'effectuer un focus sur l'expérimentation "d'analyse décisionnelle" en cours à la gendarmerie nationale et d'en souligner ses enjeux (Partie II).

[6] *The costs of crime* est un sujet récurrent dans les sociétés anglo-américaines. En fonction des types de délits (meurtres, viols, vols, etc.), de leurs conséquences et de l'implication des services de police qu'ils nécessitent, l'objectif est d'arriver à calculer de façon pragmatique le montant de ce que coûte la criminalité à la société civile.

[7] De Maillard J., *Polices comparées*, 2017.

[8] Benbouzid B., « Quand prédire, c'est gérer. La police prédictive aux États-Unis », 2018.

I. La sécurité à l'heure du prédictif

Le sujet de la police prédictive conduit à s'intéresser à l'intelligence artificielle, un champ qu'il s'agit, là aussi, de définir. L'objectif est donc à la fois d'identifier les enjeux de cette technologie associée à celui de la sécurité publique, et de préciser les postures des acteurs qui l'investissent.

1.1 Des enjeux juridiques et éthiques

L'intelligence artificielle est un sujet à la fois passionnant et inquiétant. Son développement soulève des questions d'ordre juridique et éthique, qui plus est dans le champ de la sécurité publique. De quoi parle-t-on quand on évoque l'intelligence artificielle ? Et quels sont précisément les enjeux soulevés par cette technologie ? Un premier tour d'horizon de la réglementation française est nécessaire.

1.1.1 La réglementation française

En France, l'intérêt envers l'intelligence artificielle apparaît dès les années 1970. Néanmoins, il prend un essor différent sous le coup des *big data*, qui offriraient potentiellement des données et des solutions infinies. Lorsqu'on aborde les enjeux juridiques de l'intelligence artificielle en matière de sécurité publique, on doit s'intéresser à la réglementation qui entoure les données à caractère personnel. Sur ce sujet, c'est la loi de 1978 relative à l'informatique, aux fichiers et aux libertés qui reste toujours d'actualité. Elle définit une donnée à caractère personnel comme : « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »[9] (article 2). Bien que cette définition soit inscrite dans la loi, différentes interprétations plus ou moins extensives en émanent. Pour la CNIL, compétente pour faire respecter la réglementation sur l'ensemble des dispositifs utilisant des traitements de données à caractère personnel, la notion est à prendre dans son sens le plus large.

> « Des données à caractère personnel sont des données qui se rattachent directement ou indirectement à un individu. Le "indirectement" est important. C'est tout ce qui se rattache à un individu d'une manière ou d'une autre. Effectivement on ne peut pas surveiller des individus sur le net sans exploiter leurs données à caractère personnel, car la date de naissance, le nom, l'adresse, les propos tenus sur le net, les "likes" émis sur Facebook, sont des données à caractère personnel, le champ est très large ! » (entretien n°10)

Ceci dit, la distinction parfois trop rapide, opérée entre, d'un côté les données personnelles désignées comme sensibles car directement rattachées à des individus, et de l'autre, des données géographiques, qui ne se rapporteraient qu'à des zones territoriales où se produisent des délits, apparaît moins nette. À ce titre, les adresses, et notamment celles notées au sein des procès verbaux, de surcroît lorsqu'il s'agit d'un cambriolage, sont des données à caractère personnel du moment qu'elles peuvent être, par déduction ou par recoupement, reliées à un individu.

Par ailleurs, lorsqu'il n'y a pas de traitement[10], la réglementation française et européenne reconnaît les données à caractère personnel comme un gisement à fort potentiel, notamment en matière juridique et policière, dont il faut, sans interdire, cadrer la libre circulation et l'échange afin de garantir l'efficacité des autorités compétentes[11]. Au niveau local, sans parler de transfert de données à grande échelle, nombre de policiers, mais aussi de techniciens de collectivités évoquent sans difficulté, leurs récurrentes recherches sur les réseaux sociaux (Facebook, Twitter, Instagram, leboncoin, etc.) pour saisir au mieux des éléments relatifs au climat social, ou encore rechercher des informations personnelles concernant des individus ou des renseignements sur des biens volés. Cet usage des

[9] Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 2, modifié par la loi du 20 juin 2018.

[10] On entend par traitement, une série de processus qui permet d'extraire de l'information ou de produire du savoir à partir de données brutes.

[11] Articles 4 et 7 de la directive (UE) 2016/680 du parlement européen et du conseil du 27 avril 2016 :« 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 publique et la prévention de telles menaces au sein de l'Union, et le transfert de telles données vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel […] Il est crucial […] de faciliter l'échange de données à caractère personnel entre les autorités compétentes des États membres, afin de garantir l'efficacité de la coopération judiciaire en matière pénale et de la coopération policière ».

médias sociaux paraît relativement répandu au sein des professions de la prévention-sécurité. Nos interlocuteurs évoquent aussi échanger ces informations, de façon informelle, entre partenaires.

Lorsqu'il y a traitement de données, c'est la réglementation concernant la protection des données à caractère personnel initiée par la loi de 1978 qui demeure toujours formellement applicable. Les lois et directives européennes successives[12] ont d'ailleurs entériné la régulation des traitements de données à caractère personnel, ainsi que la protection des personnes physiques à l'égard des traitements de données à caractère personnel. En d'autres termes, le traitement de données à caractère personnel n'est pas interdit, mais se doit d'être conforme. Concernant la protection des personnes physiques à l'égard des traitements de données, le droit permet à ceux dont l'utilisation de données personnelles a abouti à des effets juridiques défavorables les concernant, de demander des explications sur les critères ayant mené à cette décision : « La personne concernée devrait avoir le droit de ne pas faire l'objet d'une décision impliquant l'évaluation de certains aspects personnels la concernant, qui est prise sur le seul fondement d'un traitement automatisé et qui produit des effets juridiques défavorables la concernant ou qui l'affecte de manière significative. En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, y compris la fourniture d'informations spécifiques à la personne concernée et le droit d'obtenir une intervention humaine, en particulier d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation ou de contester la décision. Tout profilage qui entraîne une discrimination à l'égard de personnes physiques sur la base de données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux, devrait être interdit (…) [13]». Le Conseil constitutionnel, dans une décision en date du 12 juin 2018, s'est prononcé pour la première fois sur la question de l'usage des algorithmes auto-apprenants[14] comme fondement d'une décision administrative individuelle[15]. Trois conditions ont été posées :

- le traitement algorithmique et ses évolutions doivent être maîtrisés et doivent pouvoir être expliqués sous forme intelligible à la personne concernée ;
- toute décision administrative fondée sur un algorithme doit pouvoir faire l'objet d'un recours administratif ;
- l'algorithme ne doit pas porter sur des données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses, philosophiques ou syndicale, données génétiques, biométriques, de santé ou relatives à la vie sexuelle ou l'orientation sexuelle d'une personne physique).

Cette décision renforce, d'une part, les craintes à l'égard des algorithmes auto-apprenants et, d'autre part, la responsabilité des concepteurs du traitement algorithmique.

Récemment, et de plus en plus souvent, les algorithmes sont associés à des dispositifs de sécurisation, et principalement à des caméras de vidéosurveillance c'est ce qu'on appelle couramment la vidéosurveillance intelligente. Sa mise en place répond à une volonté d'anticiper les comportements dits "suspects", ou jugés "anormaux". Au moment de notre terrain d'étude, par exemple, la CNIL vient de prendre connaissance d'un projet de vidéosurveillance intelligente mené par la RATP à la station Châtelet-Les Halles, permettant de repérer des individus sur la base d'éléments de couleurs de leurs vêtements. L'algorithme utilisé détecte les masses et pixels de couleurs permettant de faciliter le repérage d'un individu dans les couloirs du métro, pour permettre son interpellation si nécessaire.

Au niveau local, les collectivités sont de plus en plus nombreuses à mettre en place des systèmes de vidéosurveillance intelligente. C'est le cas notamment du département des Yvelines ou encore des villes de Nice, Valenciennes, Marseille, Nîmes, etc. Ces dispositifs semblent se diffuser massivement dans l'objectif de renforcer le contrôle des espaces urbains. Certaines collectivités n'hésitent pas à annoncer régulièrement des innovations sur ce champ. C'est le cas de la ville de Nice, proactive quand il s'agit d'avoir recours à des dispositifs de sécurisation des espaces publics, qui a récemment communiquée sur la mise en place d'un logiciel d'analyse des émotions des passagers du tramway pour décider d'éventuelles interventions de la police municipale. « La start-up messine "Two-i" développe un logiciel permettant d'analyser "la cartographie émotionnelle" des voyageurs "en temps réel" qui va être testé et permettra à la police municipale d'intervenir si "une situation potentiellement

[12] Entre autre : Loi de 6 août 2004, loi du 7 octobre 2016 pour une république numérique, RGPD.

[13] Article 38, directives 2016/680

[14] La CNIL définit les algorithmes auto-apprenants comme des algorithmes au comportement évolutif dans le temps, en fonction des données qui leur ont été fournies. « Ces algorithmes « auto-apprenants » relèvent du domaine de recherche des systèmes experts et de l'« intelligence artificielle ». Ils sont utilisés dans un nombre croissant de domaines, allant de la prédiction du trafic routier à l'analyse d'images médicales ». Cf. lien URL : https://www.cnil.fr/fr/definition/algorithme

[15] Décision du conseil constitutionnel du 12 juin 2018, lien URL : https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm

problématique voire dangereuse" est mise en évidence »[16]. La société explique que son système permet de « prévoir des comportements », c'est-à-dire que le logiciel serait capable, à partir des émotions qu'il a détectées, de dire si une situation peut ou non devenir dangereuse. Cette annonce a suscité beaucoup de réactions et d'inquiétudes à l'égard des libertés individuelles et du droit à l'anonymat[17].

Les systèmes biométriques, c'est-à-dire les techniques informatiques permettant de reconnaître un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales, sont de plus en plus souvent évoqués quand il est question d'innovation en matière de sécurité. Les données biométriques peuvent comprendre la reconnaissance de l'ADN, des empreintes digitales, de l'iris, du contour de la main ou encore de la reconnaissance faciale ou vocale. Elles reposent sur une réalité biologique permanente et unique permettant l'identification d'une personne[18]. La biométrie reste, en France, un sujet très strictement encadré par la loi. Le règlement européen, entré en vigueur en mai 2018, renforce le régime juridique des données biométriques. Elles font ainsi l'objet d'une définition[19] et sont consacrées comme des données particulièrement sensibles, au même titre que les données concernant la race, la santé, les opinions politiques ou religieuses, ou encore celles relatives à l'orientation sexuelle. Leur traitement est interdit sauf exception spécifiquement encadrée. De plus, la mise en place d'un dispositif biométrique doit répondre à des obligations et doit recueillir le consentement de l'ensemble des utilisateurs. La CNIL recommande que les données biométriques soient aussi maintenues sous le contrôle exclusif de la personne concernée. Jusqu'à présent, les systèmes biométriques se développaient principalement pour le contrôle d'accès à des locaux, des ordinateurs, ou des applications informatiques sur certains lieux de travail. Ces dernières années, par exemple, de nombreux smartphones ou tablettes ont intégré un système de reconnaissance digitale. Au lieu de taper un code pin, les propriétaires déverrouillent leurs appareils avec leurs empreintes digitales. Dorénavant, les systèmes biométriques intègrent des dispositifs de gestion et de sécurisation des espaces publics.

Pour le moment, le logiciel "Two-i" de Nice ne semble pas vouloir associer les émotions à l'identité des individus qu'il détecte, et la CNIL n'a, à ce jour, fait aucun commentaire à son sujet. La reconnaissance faciale n'est cependant plus une aspiration lointaine. C'est une technologie expérimentée que certains acteurs souhaitent réellement utiliser. Elle vise, sur la base des traits du visage, à identifier une personne (à reconnaître un individu à partir d'une image, d'un fichier, ou d'une base de données), ou à authentifier une personne (à vérifier que l'identité d'un individu correspond bien à ce qu'il prétend être). Dans le milieu aéroportuaire par exemple la reconnaissance faciale est déjà utilisée pour, entre autre, réduire les temps d'attente provoqués par les mesures renforcées de sécurité et de contrôle des passagers. Depuis juillet 2018, la société Gemalto a mis en place des sas de reconnaissance faciale des passagers dans les aéroports de Roissy et Orly. Ces sas fonctionnent d'abord en récupérant les données biométriques inscrites au sein des puces électroniques des passeports biométriques (délivrés en France depuis 2009, et qui stockent la photographie et deux empreintes digitales de son détenteur). Une fois le sas ouvert, une caméra vérifie la correspondance entre le visage qu'elle filme et les données du passeport. En février dernier, la ville de Nice annonce cette fois tester la reconnaissance faciale sur la voie publique à l'occasion de son carnaval annuel. L'expérimentation menée sur deux jours et encadrée par la CNIL, ne concerne que des personnes volontaires. À l'aide des caméras de vidéosurveillance, l'objectif est d'identifier des individus dans la foule à partir d'une photographie. Le développement de cette technologie n'est pas sans provoquer un certain nombre de craintes, ou du moins de questionnements. Récemment, la police chinoise a fait beaucoup parler d'elle en indiquant qu'elle pouvait s'appuyer sur plus de 170 millions de caméras placées sur la voie publique et d'un dispositif de reconnaissance faciale lui permettant de reconnaître un individu qui traverse la rue. Autant d'éléments qui amènent aussi à considérer les risques que peuvent engendrer ces techniques. Comme l'écrit la CNIL *: «* la donnée biométrique n'est pas une donnée d'identité comme les autres. Elle n'est pas attribuée par un tiers ou choisie par la personne. Elle est produite par le corps lui-même et le désigne de façon définitive. Le mauvais usage ou le détournement d'une telle donnée peut alors avoir des conséquences graves »[20].

En France, le droit des « fichiers » actuel est strict concernant l'usage de l'intelligence artificielle et le traitement de données à caractère personnel, et il s'est vu récemment renforcé par la réglementation

[16] Nakache D., « "Two-i", la biopolitique au pouvoir à Nice », *Médiapart*, le 9 janvier 2019.
[17] *Ibid*.
[18] Définition et règlementation de la biométrie par la CNIL : https://www.cnil.fr/fr/biometrie
[19] RGPD, art.4-14: « Les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ».
[20] Lien URL : https://www.cnil.fr/sites/default/files/typo/document/Communication-biometrie.pdf

européenne. Pourtant, force est de constater que certains acteurs, soucieux de se faire une place sur le marché des innovations tant sécuritaires que numériques, bousculent ces limites. Dans le champ de la sécurité publique, l'intelligence artificielle interroge la nature même du renseignement criminel, et la pertinence de l'information produite pour lutter contre la délinquance. Des questions qui, au vu des enjeux, ont tout intérêt à être discutées et rendues publiques.

1.1.2 Les défis éthiques de l'intelligence artificielle

Récemment, les enjeux éthiques posés par l'intelligence artificielle s'affichent comme la principale préoccupation. L'éthique figure comme un champ infra-juridique, sur lequel doit s'envisager une réflexion morale, venant répondre à la question : au-delà du droit, sur quels systèmes de valeurs repose le développement de l'intelligence artificielle ?

En décembre 2017, la CNIL publie une synthèse du débat public qu'elle a animé dans le cadre de la mission de réflexion éthique sur les algorithmes et l'intelligence artificielle prévue par la loi[21]. Ce rapport vise à clarifier à la fois les termes et notions usités dans ce domaine, ainsi que les enjeux juridiques et éthiques que soulèvent leurs usages. La CNIL définit l'intelligence artificielle comme « le grand mythe de notre temps » comprenant l'ensemble des « théories et techniques "consistant à faire faire à des machines ce que l'homme ferait moyennant une certaine intelligence" (Marvin Minsky). On distingue IA faible (IA capable de simuler l'intelligence humaine pour une tâche bien déterminée) et IA forte (IA générique et autonome qui pourrait appliquer ses capacités à n'importe quel problème répliquant en cela une caractéristique forte de l'intelligence humaine, soit une forme de « conscience » de la machine)[22]».

À la suite, le député Cédric Villani se voit confier par le premier ministre une consultation publique sur l'intelligence artificielle, devant servir de feuille de route au gouvernement sur ce sujet. Son rapport sort en mars 2018. Il se prononce notamment en faveur d'une ouverture renforcée des données publiques et privées et du développement de la recherche dans le domaine de l'intelligence artificielle. Il identifie des secteurs économiques et industriels sur lesquels il invite à se concentrer. La sécurité publique y figure au côté de la défense, l'écologie, la santé, ou encore les transports et la mobilité. Dans ces secteurs, l'État est appelé à jouer un rôle fondamental. Le rapport identifie deux façons de travailler des données à des fins de prédiction de la délinquance, en mobilisant :

- des données géographiques pour identifier des zones à risques, où des délits sont plus susceptibles de se produire,
- des données sociales et comportementales des individus dans l'objectif d'identifier de potentiels criminels et/ou victimes.

Dans les deux cas, Cédric Villani estime que les enjeux éthiques et les limites techniques doivent conduire à investir ce sujet avec prudence[23]. Le lendemain de la publication de ce rapport, le Président Emmanuel Macron organise une conférence au Collège de France intitulée « IA for Humanity » afin de préciser la stratégie du pays dans ce domaine. Il annonce, entre autres, un plan d'1,5 milliard d'euros sur l'ensemble de son quinquennat. Il se positionne favorablement pour la circulation des véhicules autonomes, ainsi que pour la création « d'une expertise mondiale indépendante » portant principalement sur les enjeux éthiques soulevés par l'intelligence artificielle.

De façon récurrente, le sujet de la police prédictive est évoqué, et c'est sous l'angle des enjeux ou "défis" éthiques qu'il apparaît plus spécifiquement. L'expérience Predpol est souvent citée en exemple voire en contre-exemple, car sont surtout pointés les différents risques qu'elle comporte : atteintes aux libertés fondamentales, faillibilité du système, dilution de la figure d'autorité traditionnelle et déresponsabilisation des personnels dans leur prise de décision, répartition discriminante de l'offre de sécurité publique, incapacité à évaluer l'efficacité réelle de l'outil, etc. La police prédictive représente un outil de modernisation de l'action publique, en même temps qu'elle attise un certain nombre de craintes. Certains de nos interlocuteurs regrettent parfois ce positionnement mitigé de la part des représentants de l'État :

[21] Loi du 7 octobre 2016 pour une république numérique. Cette loi s'articule autour de trois axes : la circulation des données et du savoir, la protection des individus dans la société du numérique et l'accès au numérique pour tous.
[22] CNIL, *Comment permettre à l'homme de garder la main ?, Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, décembre 2017.
[23] Villani C., *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, 2018, p.150.

> « En France le sujet [la police prédictive] ne prend pas. Si on lit le rapport Villani, ils se sont contentés d'écrire ce qu'ils ont entendu dire. Les problèmes éthiques, oui, il y a des dérives possibles, une rupture d'égalité territoriale. Aux États-Unis, on peut faire des programmes discriminants, c'est un risque, mais il y a une évaluation derrière, car la police publie ses données, et il y a des associations qui alertent sur des cas de discriminations et d'abus de pouvoirs. En France, on n'expérimente pas, mais on n'évalue pas non plus ! » (entretien n°8)

Si, dernièrement, l'intelligence artificielle apparaît comme un sujet porteur, les inquiétudes qu'elle suscite sont fortes, *a fortiori*, lorsqu'elle est associée à la sécurité publique. Le spectre de la surveillance généralisée, le risque de reproduction de biais discriminants, ou encore la violation des données personnelles et libertés fondamentales, sont autant de dangers identifiés. Cette question éthique ne traverse pas seulement la France, de nombreux autres pays européens, tout comme les États-Unis s'y intéressent.

Au-delà du cadre légal et de la conformité juridique, la CNIL soulève des enjeux éthiques et érige deux principes concernant le traitement de données à caractère personnel[24] :

• Un principe de loyauté : le droit à l'information, la loyauté à l'égard des personnes dont l'algorithme va utiliser les données nécessitent de travailler la transparence et la traduction du sens de l'algorithme, pour en retour, recueillir le consentement des personnes concernées. Ce principe prend aussi en compte les effets collectifs des algorithmes, qui ne doivent pas être en contradiction avec « les grands intérêts collectifs » comme le renforcement ou la reproduction de discriminations. Il se heurte aux algorithmes auto-apprenants dont le comportement peut devenir opaque, y compris pour leurs propres concepteurs.

• Un principe de vigilance : le caractère évolutif et potentiellement imprévisible des algorithmes, notamment auto-apprenants, nécessite de les appréhender dans toute leur complexité. Ce principe vise entre autre à reconsidérer la confiance excessive envers les outils de l'intelligence artificielle, et à se soucier des phénomènes de déresponsabilisation qu'ils peuvent entraîner.

Dans le cadre de cette étude, les interlocuteurs rencontrés au sein de la CNIL ajouteraient volontiers un troisième principe transversal qu'ils identifient comme fondamental :

> « Le plus grand principe, c'est le principe de finalité. C'est le plus important, c'est ce qui fait la loi informatique et libertés de 1978. On n'interdit pas la collecte de données à caractère personnel, mais elles doivent être collectées pour une finalité établie et précise. Dès lors qu'on utilise des données pour un tout autre objectif que celui initialement prévu, sans prévenir les personnes ou sans avoir leurs consentements, c'est là qu'on sort du cadre. La collecte de données est une sorte d'autorisation que l'on accorde pour que les données soient utilisées pour une unique finalité. » (entretien n°10)

Ce principe de finalité est régulièrement au centre des actions menées par la CNIL qui rappelle à l'ordre nombre d'acteurs (conseil régional, groupes d'assurance et de retraite complémentaire, etc.) que « de manière générale les données ne doivent pas être réutilisées pour des finalités non prévues ».

Enfin, comme dans tout secteur, l'éthique figure aussi comme une stratégie de différenciation dans le marché mondialisé et concurrentiel de l'intelligence artificielle. Ainsi l'affirment deux journalistes du Monde : « La France et l'Europe, elles, se voient en championnes de l'éthique dans l'IA face aux Américains et aux Chinois »[25]. L'éthique est aussi un secteur prometteur, où convergent les intérêts portés à la fois par des acteurs publics et privés.

1.2 Un intérêt croissant pour la police prédictive

Dans le contexte actuel, la sécurité publique est une préoccupation constante que la menace terroriste ravive régulièrement. Dans ce domaine, le prédictif, bien qu'encore à ses prémices en France, figure comme un champ innovant et laisse peu insensible. Au-delà de l'écho médiatique, il intéresse les acteurs classiques du champ de la prévention/sécurité, et plus largement, ceux qui cherchent à investir le marché de la sécurité comme celui du numérique. Néanmoins, par-delà l'effet d'annonce, il est difficile de voir concrètement ce que recouvrent ces nouveaux dispositifs et leurs réels usages.

[24] CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, 2017.
[25] Piquard A., Tual M., « L'éthique dans l'intelligence artificielle, année zéro », *Le Monde*, 05/10/2018.

1.2.1 Le positionnement des pouvoirs publics et des acteurs privés

Ce champ de la police prédictive est porté de façon ambivalente par la sphère publique. Le 4 juin 2015, une première question ″officielle″ est posée au parlement par la sénatrice de la Haute-Vienne, Marie-Françoise Perol-Dumont, et fournit des détails sur le projet développé au nom de la police prédictive en France. Elle s'adresse au ministre de l'Intérieur – Bernard Cazeneuve à l'époque – et demande des explications concernant la création d'une nouvelle division au sein de la gendarmerie nationale. La réponse apporte quelques éléments quant à la façon dont l'État appréhende le sujet :

> « Actuellement, une étude exploratoire portant sur plusieurs infractions et espaces territoriaux est menée afin de déterminer le modèle scientifique prédictif le plus adapté. L'objectif recherché est la constitution d'une aide à la décision (« analyse décisionnelle »), au profit du commandant d'unité territoriale, notamment à des fins de prévention de la délinquance. […] Le modèle devra être en mesure d'apporter des réponses correspondant à différents critères de temps (année, mois, semaine, jour) et d'espace (département, arrondissement, commune, îlots regroupés pour l'information statistique), afin de permettre la révélation du ou des modèles le(s) plus pertinent(s) pour le territoire.[26]»

Cette réponse permet de poser les objectifs visés par le déploiement d'un tel dispositif. Mais on perçoit déjà beaucoup de réserves à l'idée d'annoncer clairement qu'il s'agit d'un outil prédictif.

Depuis, les représentants de l'État s'expriment régulièrement sur le développement de l'intelligence artificielle. À cette occasion, des références au champ de la police prédictive ou de l'analyse prédictive sont effectuées. Au lancement de la police de sécurité du quotidien (PSQ), le prédictif est cité comme un chantier d'avenir pour les forces de sécurité françaises. Le ministre de l'Intérieur Gérard Collomb présente ses propositions pour « une police numérique », lesquelles recouvrent un large ensemble d'éléments portant à la fois sur l'évolution de la délinquance (cybercriminalité, ″uberisation du cambriolage″, etc.) et la nécessité de doter les policiers et gendarmes de moyens adéquats (mis à disposition de smartphones, tablettes, équipement de caméras-piétons, etc.). La police prédictive y est annoncée, mais peu de choses sont avancées sur le fond. La presse relaie l'information, en associant police prédictive, dispositifs de vidéosurveillance intelligente ou encore reconnaissance faciale[27]. Tout semble être investi de front, mais il s'avère difficile de définir ce qui est concrètement travaillé.

L'engouement suscité par l'intelligence artificielle se traduit dans toutes les sphères de la sécurité, comme l'illustre l'ouverture « d'un cycle supérieur sur l'intelligence artificielle » mené par le centre des hautes études du ministère de l'intérieur (CHEMI), pour « permettre de visiter la problématique de l'IA dans le domaine de la sécurité (vidéosurveillance, exploitation de fichiers, signaux de basse fréquence) […] L'enjeu est majeur : créer au sein du ministère une véritable communauté de projets et d'échange afin de ne pas manquer de tirer pleinement profit de l'enjeu de l'IA, qui va marquer la dynamique des organisations sur la période 2020-2030 [28]». Plus largement, c'est l'ensemble des instituts de recherche rattachés au ministère de l'Intérieur et à celui de la Défense qui témoignent un fort intérêt pour les possibilités offertes par l'intelligence artificielle et plus particulièrement par la police prédictive. À l'instar de l'Institut national des hautes études de la sécurité et de la justice (INHESJ), du centre de recherche de l'école des officiers de la gendarmerie nationale (CREOGN), ou encore du CHEMI, qui ont dernièrement multiplié les conférences, séminaires, ateliers-recherches, appels à projets sur les enjeux soulevés par l'usage des algorithmes prédictifs dans le domaine de la sécurité[29] avec, là aussi, une focale dédiée aux questions éthiques et juridiques.

De leur côté, les acteurs privés cherchent, également à se positionner sur ce qui leur paraît être un marché prometteur, en plein essor. En outre, sans chercher l'exhaustivité, il recouvre des acteurs aux parcours, aux positionnements et aux statuts divers :

- Les grands groupes : à l'image d'Engie Ineo, spécialisé dans le domaine du génie électrique, qui se tourne vers des solutions dites « intelligentes ». Cette entreprise cible principalement les acteurs des territoires (collectivités locales notamment) et propose des

[26] Lien URL : https://www.senat.fr/questions/base/2015/qSEQ150616562.html

[27] Hérard P., « Surveillance : le réseau français ″intelligent″ d'identification par caméras arrive », *TV5 Monde*, mis en ligne le 09.06.2018. Lien URL : https://information.tv5monde.com/info/surveillance-le-reseau-francais-intelligent-d-identification-par-cameras-arrive-242520

[28] Site internet du CHEMI consacré à la création du Cycle supérieur d'intelligence artificielle du ministère de l'intérieur. Lien URL : https://allchemi.eu/course/view.php?id=307

[29] Entre autres : « Sécurité et justice : le défi des algorithmes », le 27 juin 2017 par l'INHESJ ; « Algorithmes prédictifs : quels enjeux éthiques et juridiques ? », le 26 septembre 2017 par le CREOGN ; « Police prédictive, journée d'étude professionnelle », le 24 janvier 2018 par le CHEMI ; « Quand prédire c'est gérer. La police prédictive aux USA », le 22 janvier 2019 par l'INHESJ, etc.

solutions clés en main pour faire face « aux nouveaux défis sécuritaires ». IBM présente des logiciels d'analyse prédictive, notamment dans le domaine de la police (la publicité américaine consacrée à son logiciel de « predictive police » a suscité de nombreux commentaires[30]) et a affirmé avoir approché le ministère de l'Intérieur français. Ou encore Palantir, société américaine spécialisée dans le traitement de données de masse, qui a récemment annoncé travailler pour la direction générale de la sécurité intérieure (DGSI) et Airbus[31]. Les grands groupes français, tels que Safran ou Thalès, spécialisés dans le domaine de la défense accompagnent les changements dans ce domaine.

- Les petites entreprises ou *start-ups* : comme « Two-i » (cité *supra*), ou Spallian qui se spécialise dans la vente de logiciels de gestion et d'analyse de données auprès des collectivités territoriales. Sans parler des nombreuses *start-ups* étrangères qui impulsent et présentent régulièrement des nouveautés techniques sur ce marché mondialisé, à l'image de Faception, société israélienne très controversée qui affirme développer un logiciel qui associe aux traits du visage humain des caractéristiques comportementales, et qui permettrait de repérer des criminels, dont des terroristes[32].

Pour le moment, il est difficile d'analyser la dynamique de ce marché compétitif. On imagine que cette concurrence a certainement un impact sur les solutions proposées. Par ailleurs, le marché de la sécurité n'est pas propre à l'ère des *big data*. Il a, ces dernières décennies, accompagné les politiques publiques de sécurité, en répondant aux nouvelles obligations et réglementations (vidéosurveillance, études de sécurité publique, agents de sécurité privée, logiciel de gestion et d'analyse de données, cartographie de l'insécurité, etc.) voire en participant à la surenchère sécuritaire actuelle. Dans ce contexte, acteurs publics et privés semblent œuvrer de concert à la mise en place de dispositifs prédictifs.

1.2.2 Quelques démarches concrètes

Tout en respectant le cadre de la réglementation française, certains acteurs travaillent, parfois depuis plusieurs années, sur des machines prédictives pour mieux connaître les origines des phénomènes de délinquance.

À l'Observatoire national de la délinquance et des réponses pénales (ONDRP), un géo-statisticien utilise depuis plusieurs années en collaboration avec l'université de Rutgers (New Jersey, États-Unis) un algorithme prédictif. Aux États-Unis, cet algorithme sert à plusieurs polices américaines. En France, il est expérimenté à partir des données de la direction de la sécurité de proximité de l'agglomération parisienne (DSPAP).

> « J'utilise l'algorithme RTM (Risk Terrain Modeling) depuis plus de 8 ans. […] Aujourd'hui, c'est une appli web, beaucoup plus puissante qu'avant, mais c'est le même principe : cela rejoint la prévention situationnelle, c'est-à-dire qu'on repère les éléments contextuels, environnementaux qui font que ça se passe là. Les causes du crime, ce sont les inégalités, la pauvreté, le chômage, une hérédité, etc. et c'est aussi un contexte favorable au sens médical, au sens médecine du terme. Donc en analysant un contexte, en identifiant les facteurs qui aggravent le risque, on peut prévoir pour un environnement similaire ce qui peut éventuellement se produire […]. » (entretien n°8)

L'ONDRP utilise ainsi une extraction du logiciel de rédaction des procédures de la police nationale (LRPPN), qui comprend des données localisées de commissions de faits, pour identifier des variables environnementales communes par type de faits de délinquance. L'objectif étant de créer des associations entre facteurs contextuels et événements délictuels, afin de mieux anticiper leur commission mais aussi d'allouer les ressources (humaines et matérielles) adéquates. L'algorithme, en fonction des types de délits, permet d'attribuer une valeur de vulnérabilité aux lieux, en fonction de ses caractéristiques contextuelles répertoriées[33]. Depuis plusieurs années, l'outil est régulièrement alimenté par les données fournies par la DSPAP ; néanmoins, notre interlocuteur à l'ONDRP déplore des points de blocage, à commencer par les données elles-mêmes :

[30] https://vimeo.com/44838239
[31] https://www.lesechos.fr/09/12/2016/lesechos.fr/0211580858432_la-dgsi-signe-un-contrat-avec-palantir--une-start-up-financee-par-la-cia.htm
[32] https://www.faception.com/
[33] Cf. site de l'université de Rutgers, présentant le Risk Terrain Modeling Diagnostics Software : http://techfinder.rutgers.edu/tech/Risk_Terrain_Modeling_Diagnostics_Software_(RTMDx)

> « Ce sont des données administratives, mais elles ne sont pas utilisées sur un plan opérationnel ou analytique. La donnée analytique demande quand même un certain nombre de variables et d'informations. […] Même le lieu n'est pas toujours renseigné dans les données, parfois il n'apparaît pas, ni l'adresse, ou alors, on a juste "Paris". Mais Paris, ce n'est pas un lieu, c'est trop grand ! La notion de lieu, le lieu géographique de l'intervention, rien que ça c'est compliqué à avoir ! »

L'exploitation des résultats de l'algorithme RTM est donc contrainte. Au-delà de la qualité informative de la donnée, c'est aussi son usage par l'institution policière qui peut poser problème :

> « On [les services de police] est surtout sur du *reporting*, on leur demande des éléments statistiques, ils les crachent, mais analysent très peu ces éléments pour comprendre les phénomènes. On constate que ça monte, que ça descend, où ça monte, où ça descend, mais il n'y a pas de structure analytique derrière, on ne répond jamais au pourquoi. »

En outre, la mise en place d'outil prédictif se heurte à l'expérimentation sur le terrain, pour tester et évaluer le dispositif :

> « Par exemple, cela veut dire que s'il se passe quelque chose au point A, et qu'on intervient sur le point A, il y a des chances pour que cela se déplace sur un point B. Donc l'idée est de mettre des agents sur le point B et d'attendre pour voir si quelque chose arrive. S'il n'arrive rien, cela voudra dire qu'on se sera trompé, et ça ce n'est pas possible à entendre. Car cela voudra dire qu'on aura immobilisé un véhicule et des agents et ce n'est pas possible dans le système actuel, on tombe directement dans des questions de gestion des services et de ressources humaines. »

En se basant, d'une part, sur les faits de délinquance informatisés, d'autre part, sur les conditions contextuelles du passage à l'acte, l'algorithme RTM rejoint le cadre analytique de la prévention situationnelle[34]. Ce sont d'ailleurs, ces données contextuelles qui, associées aux données passées de la délinquance, permettent de produire du prédictif, ce qui fait dire à notre interlocuteur :

> « Si vous n'avez que des données professionnelles [soit des chiffres de la délinquance produites par les services de police], vous faites du prédictif rétrospectif, c'est-à-dire que vous allez vous baser sur le passé. Avec les données contextuelles, on peut faire du prédictif. Si on connaît les variables qui sont favorables à la délinquance, on a même plus besoin des données professionnelles. »

Par ailleurs, une autre démarche prédictive a récemment été relayée par la presse. Il s'agit du projet porté par la ville de Marseille, lancé fin 2016 et intitulé « Big data de la tranquillité publique ». Son annonce a fait l'objet d'un important traitement médiatique et l'élue en charge s'est également beaucoup exprimée à son sujet. Le projet vise à collecter et à croiser de nombreuses sources informatiques afin d'aider les agents de la police municipale dans leurs missions quotidiennes. L'aspect prédictif est mis en avant, la ville explique sur son site internet qu'il s'agit « de recueillir, auprès de partenaires institutionnels du territoire, des données précieuses pour essayer de prévenir certains événements avant qu'ils ne se produisent [35]». Il s'intègre dans une politique plus large de renforcement et de modernisation des forces de police municipale, comprenant l'augmentation des effectifs, leur armement, ou encore le déploiement continu des dispositifs de vidéosurveillance, etc. Pour financer son projet d'analyse prédictive, la ville de Marseille bénéficie de fonds versés par le FEDER (les fonds européen de développement économique et régional) et par le département des Bouches-du-Rhône, à hauteur de 600 000 euros chacun. Pour le mettre en œuvre, la ville a passé un marché avec l'entreprise Ineo digital (filiale d'Engie Ineo). Elle profite de cette occasion pour afficher son ambition d'être « résolument tournée vers l'avenir », tout en mettant « les nouvelles technologies et le numérique au service de ses habitants ». Présenté publiquement le jour de l'entrée en vigueur du RGPD, l'application se présente sous forme d'un agenda. Le principe est de croiser l'ensemble des données de la municipalité et de futurs partenaires afin d'anticiper d'éventuels troubles sur la voie publique. Un algorithme a été développé pour évaluer le niveau de risque d'une situation et la bonne adéquation des dispositifs prévus. Chaque jour est estampillé d'une couleur verte, orange ou rouge, et l'algorithme attribue une note de dangerosité allant de 1 à 10. Pour le moment, il semble que seules les données détenues par la mairie soient utilisées (marchés, police municipale, événements, centre de supervision urbain, travaux, etc.). Mais la ville veut développer sa plateforme et intégrer les données de partenaires tels que les opérateurs téléphoniques, les hôpitaux, les pompiers, la police nationale ainsi que les données des réseaux sociaux[36], etc.

[34] La prévention situationnelle peut être brièvement définie comme l'ensemble des actions menées en matière d'aménagement pour la sécurité.

[35] Lien URL : http://prevention.marseille.fr/s%C3%A9curit%C3%A9-et-pr%C3%A9vention/big-data-de-la-tranquillite-publique

[36] Legros C., « À Marseille, le *big data* au service de la sécurité dans la ville », *Le Monde*, 08.12.2017.

Du côté des associations de défense des droits et des libertés fondamentales face au développement du numérique, le projet marseillais interpelle, et plus largement, la mise en œuvre de l'ensemble des dispositifs dits « intelligents ». C'est le cas, de la Quadrature du Net[37], qui met en garde contre les dangers que comporte le projet marseillais concernant à la fois la reproduction de biais discriminants, la mise en péril des libertés fondamentales et de la protection des données à caractère personnel, mais aussi sur l'imbrication des acteurs privés et publics dans la mise en œuvre de ces nouvelles « technologies de contrôle social[38] ». Plus largement, c'est le développement de la surveillance policière *via* les *big data*, qui inquiète cette association, qui régulièrement alerte sur le développement des « *smart cities* policières ». Dans le projet de la ville de Marseille, la Quadrature du Net a notamment attiré l'attention de la CNIL sur la volonté de réexploiter des données portant sur les hospitalisations. La commission envisage au moment de notre étude de suivre la démarche de la collectivité, dans une logique d'accompagnement, notamment auprès du correspondant informatique et libertés dont la ville s'est dotée.

> « De fait, entre ce que l'élu dit et ce qu'il a dans le marché public, et ce qu'il y aura au lancement, ça n'a rien à voir avec la police prédictive. C'est plutôt de l'ordre de l'anticipation de la gestion lors de grands événements publics. Mais il y a l'infrastructure, ce n'est pas fini et donc derrière, il faut rester vigilant. » (entretien n°10)

C'est en effet une première étape qui soulève des questions majeures si, à l'avenir, des dispositifs similaires venaient à se « banaliser » et si l'ensemble des collectivités territoriales et acteurs publics décidaient d'y avoir recours.[39]

***

Ce premier tour d'horizon permet de définir, dans le contexte français, la manière dont est investi le champ de la police prédictive. À la différence des États-Unis, la réglementation française est rigoureuse et, pour le moment, il n'est pas question de faire du profilage de futurs criminels, ou d'anticiper la récidive à partir des données judiciaires. Mais les aspirations à la prédiction sont là, aussi bien pour prévenir les comportements déviants à partir des émotions, que pour anticiper les désordres urbains en recourant aux caméras de vidéosurveillance intelligente, ou encore en analysant les phénomènes de délinquance à partir de variables contextuelles. Plus ou moins avancées, ces expériences sont en œuvre et continuent d'être développées. Néanmoins, dans le champ de la police prédictive, et plus largement en matière d'intelligence artificielle, se pose la question de l'expérimentation (tout en respectant le cadre juridique) et surtout de l'évaluation des dispositifs.

[37] La Quadraturne du Net est une association qui vise à défendre « nos droits et libertés fondamentales à l'ère du numérique et propose des alternatives pour un internet libre, décentralisé et émancipateur ». Lien URL : https://www.laquadrature.net/fr

[38] La Quadrature du Net, « La surveillance policière dopée aux *Big Data* arrive près de chez vous ! », 20 mars 2018 ; « La *Smart City* policière se répand comme traînée de poudre », 6 juillet 2018.

[39] *Ibid*.

II. Les prémices de la police prédictive en France

En 2015, la gendarmerie nationale annonce travailler sur le champ de la police prédictive, à la suite nombreux sont les médias à s'emparer du sujet : « la police prédictive débarque en France », « Pour éviter les crimes, la gendarmerie combine analytique et *big data* », « la gendarmerie expérimente une méthode d'analyse prédictive en matière de délinquance », « la gendarmerie a un nouveau logiciel pour prédire les délits », « Faut-il faire confiance à la police prédictive ? »[40], etc. Presque tous font référence au récit de science-fiction de *Minority Report,* pour illustrer leurs propos. Pourtant, cette référence qui se rapporte davantage à une critique de la répression policière des années 1970 est, à bien des égards, éloignée des enjeux que pose l'expérimentation menée par la gendarmerie nationale.

En France, la police prédictive semble principalement investie par les gendarmes. Du côté de la police nationale, il est difficile de savoir comment est appréhendé le sujet, nos sollicitations étant restées sans suite. Pourtant, au vu de certaines déclarations, les services du ministère de l'Intérieur semblent intéressés par le sujet, mais il est impossible d'affirmer ce qui, concrètement, est en cours d'élaboration. Par ailleurs, la gendarmerie et la police nationales ne travaillent pas ensemble sur le thème du prédictif, chaque administration fonctionne en silo sur ce sujet.

Cette présentation de l'expérimentation menée au sein de la gendarmerie nationale s'appuie sur des retours d'expériences à la fois riches et contrastés. L'accès aux informations a parfois été difficile, et malgré notre insistance, certains acteurs n'ont pas souhaité s'exprimer ou approfondir nos échanges. C'est à la fois révélateur de la difficulté d'étudier cette institution mais aussi de la sensibilité que revêt le sujet de la police prédictive. Nous tenons encore une fois à remercier ceux qui ont accepté d'échanger avec nous. Leurs propos, retranscrits ici, ont été anonymisés.

2.1 L'expérience de la gendarmerie nationale

C'est en 2013 que la gendarmerie nationale engage une réflexion sur l'analyse prédictive portant sur certains faits de délinquance. Cette démarche vise à adapter les méthodes prédictives aux enjeux de la sécurité publique. L'un des fondateurs du projet explique : « À l'origine, l'idée était que la gendarmerie et la sécurité ne passent pas à côté de l'intelligence artificielle ».

2.1.1 Genèse d'une réflexion prédictive

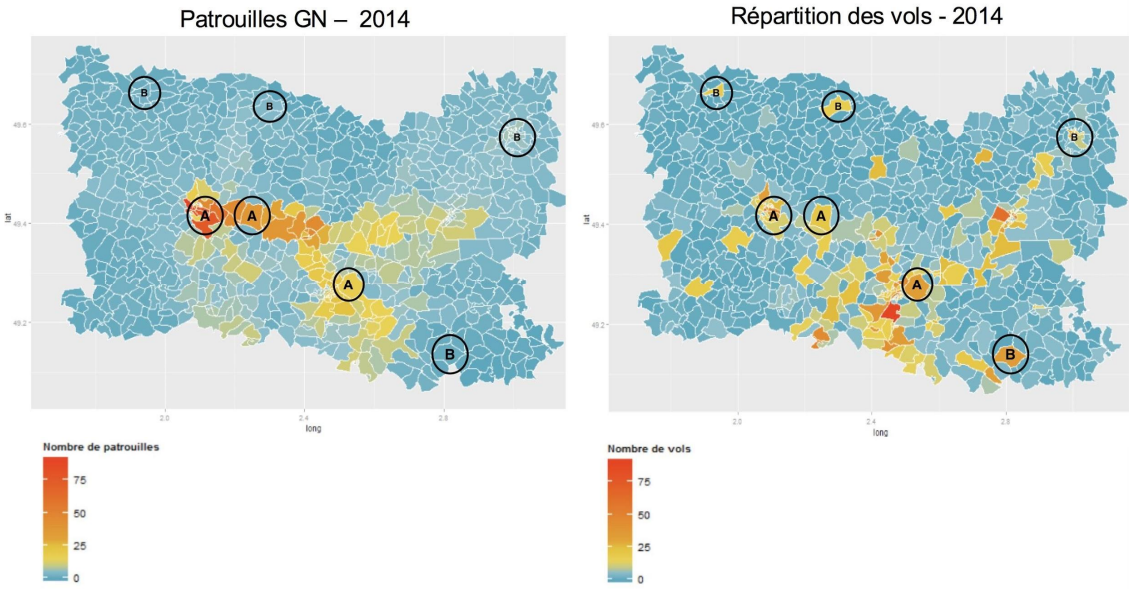
L'expérience prédictive de la gendarmerie est initiée par un petit noyau de gendarmes, scientifiques de formation, et férus d'intelligence artificielle. En 2015, une première démarche prédictive est officiellement lancée avec la mission Etalab, placée au sein de la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC). Cette dernière est interpellée par le service des technologies et des systèmes d'informations de la sécurité intérieure (ST(SI)^2). L'enjeu est de tirer profit des data-sciences et d'expérimenter des techniques d'apprentissage automatique à l'échelle d'un département sur un type de délit ciblé. Un data-scientist est ainsi missionné et c'est le département de l'Oise qui est choisi, car particulièrement exposé aux vols de véhicules. Par ailleurs, parce qu'elle représente la première expérience prédictive des forces de sécurité en France, la démarche fait l'objet d'une communication importante. Les médias se saisissent du projet et la revue de la gendarmerie nationale lui consacre un article[41]. Cette démarche prédictive s'appuie sur les données des bases de dépôts de plaintes de la police et de la gendarmerie (LRPPN et LRPGN) concernant les vols liés aux véhicules. Au départ, il semble que les deux administrations aient été, ensemble, partie prenante dans ce premier projet prédictif.

[40] Bourgoin N., « la police prédictive débarque en France », *alterinfo.net*, octobre 2016 ; Leblal S., « Pour éviter les crimes, la gendarmerie combine analytique et big data », *Le monde informatique*, janvier 2016 ; Lagneau L., « La gendarmerie expérimente une méthode d'analyse prédictive en matière de délinquance », *Opex360*, octobre 2016 ; Polloni C., « La gendarmerie a un nouveau logiciel pour prédire les délits », *Le novel obs*, mai 2015 ; Lefebvre C., « Faut-il faire confiance à la police prédictive ? », *Le point*, septembre 2016.

[41] Gauthier F., « Prédire les vols de voiture ? », 2017.

Le data-scientist a d'abord observé la plus ou moins bonne adéquation entre les zones de patrouilles et les zones de vols de voitures. Puis, pour définir les zones les plus « sensibles », il a retenu l'IRIS comme découpage géographique[42]. Le territoire a ainsi été divisé en 799 territoires. La base de données a, ensuite, été alimentée par plus de 600 variables socio-démographiques (taux de chômage, scolarisation des jeunes, nombre de commerces de proximité, âges moyens des habitants, etc.) et des indicateurs concernant les circonstances temporelles des vols (météo, fréquence des vols, etc.).

Adéquation entre patrouilles de gendarmes et vols de véhicules



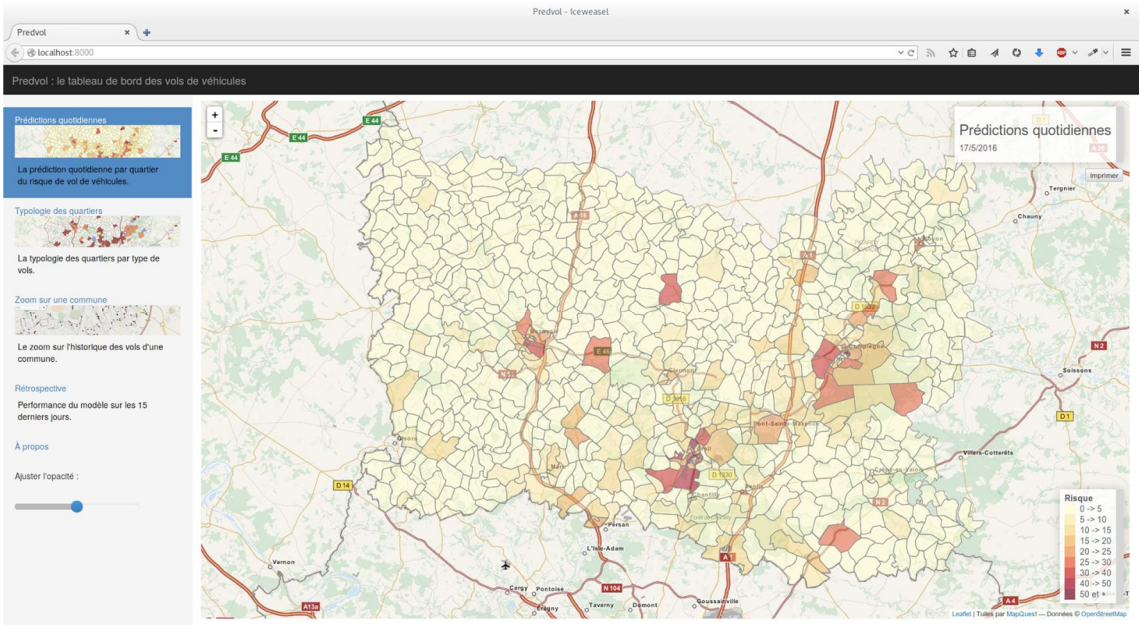
Source : administration générale des données, Secrétariat général pour la modernisation de l'action publique.

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

Enfin, trois types d'algorithmes ont été testés : Les premiers « figurent parmi les plus classiques de la littérature en matière de machine learning : régression logistique, forêts aléatoires, boosting, forêts aléatoires extrêmement randomisées, XGBoost… [43]», pour sélectionner les meilleurs prédicteurs parmi une grande quantité de variables. Le data-scientist a aussi testé l'algorithme de Predpol avec les données des vols liés aux véhicules, il constate qu'il existe bien un « risque terrain » et que les données passées concernant ce type de faits produisent des zones plus sujettes à ceux-ci. L'effet « contagion » propre à Predpol (lorsqu'il y a un crime dans une zone, la probabilité qu'il en survienne un autre dans une zone géographique proche est plus grande et décroît avec le temps) ne semble pas fonctionner avec les données de l'Oise. Finalement, le data-scientist décide de tester un troisième type d'algorithme et de produire « une carte de chaleur évolutive », soit le modèle Predpol sans l'effet de contagion. Pour cela, il retient un historique de neuf mois, « historique optimal à utiliser afin d'obtenir la carte de chaleur prédictive la plus pertinente ». L'outil, nommé Predvol, a été essayé par la compagnie de gendarmerie de Compiègne et par les agents de la brigade anti-criminalité (BAC) de la direction départementale de la sécurité publique (DDSP) de Beauvais. La carte de chaleur évolutive permettrait ainsi d'obtenir des résultats « quasiment identiques aux modèles les plus complexes », comme celui de Predpol, mais en étant beaucoup plus simple techniquement. C'est finalement, « la simple visualisation des faits passés » qui servira de prédiction au quotidien. Le data-scientist assure sa pertinence : « Le modèle prédisait 74% des faits. Et 10% des quartiers représentaient 50% du nombre de vols »[44].

[42] L'IRIS (Îlots regroupés pour l'information statistique) est un découpage territorial infra-communal créé par l'Insee.
[43] Gauthier, « Prédire les vols de voiture ? », 2017.
[44] Le-Bas C., « Sous le capot de la police prédictive », *Courrier picard*, publié le 04/02/2018.
Lien URL : http://www.courrier-picard.fr/88625/article/2018-02-04/sous-le-capot-de-la-police-predictive

Le logiciel Predvol



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

Pourtant, cette expérience est aujourd'hui très critiquée pour sa méthode. Nos interlocuteurs sont unanimes : « expérimentation ridicule », « résultats dénués de sens et de scientificité », « expérience qui fait mal », « au final, le département a été découpé en secteurs qui n'ont aucune réalité géographique, ce n'était pas parlant pour les personnels et pas précis non plus ! ».

En parallèle, à partir de 2013, la gendarmerie crée un service au sein du service central de renseignement criminel (SCRC) placé au pôle judiciaire de la gendarmerie nationale, en charge d'investir plus particulièrement le chantier du prédictif. Composé d'une dizaine de data-scientists au statut d'officiers commissionnés, il a pour mission de développer techniquement une plateforme prédictive. Un gradé, anciennement à la tête de ce service, témoigne des ambitions initiales :

> « Je me suis rendu compte que le service n'avait aucune méthode scientifique sur comment appréhender la délinquance. Et, en parallèle, à cette époque, les méthodes prédictives et l'usage de l'intelligence artificielle fleurissaient dans tous les domaines mais pas dans celui de la sécurité. Auparavant, mon expérience de terrain m'avait montré que la délinquance n'est ni déterministe, ni aléatoire, mais entre les deux. » (entretien n°6)

L'objectif qu'il se donne alors est d'essayer de cerner les facteurs explicatifs de la délinquance, les variables communes qui influent sur le passage à l'acte, pour *in fine* affiner l'analyse des phénomènes de délinquance et permettre aux gendarmes d'être plus proactifs.

2.1.2 Une plateforme « d'analyse décisionnelle »

Au sein de ce service, la gendarmerie développe une plateforme d'anticipation. Parfois nommée "PAVED" pour "plateforme d'analyse et de visualisation évolutive de la délinquance", elle est aussi appelée "plateforme d'analyse décisionnelle". Le choix des mots est important, et c'est volontairement qu'il a été décidé de ne pas faire apparaître le mot "prédictif". Ce qui n'a pas empêché les médias (et la gendarmerie) d'annoncer l'arrivée de la police prédictive en France. Officiellement, il est avancé que le terme "prédictif" renverrait à une obligation de résultat. C'est ainsi que l'explique le colonel Laurent Collorig, actuel responsable du développement de la plateforme, dans une émission diffusée sur France Culture :

> « Nous, on ne parle pas de police prédictive. C'est un outil qu'on met pour que les responsables opérationnels de la gendarmerie prennent leur décision en toute connaissance de cause, c'est un outil qu'ils ont à leur disposition, pour évaluer un petit peu l'organisation de leur service au quotidien.

> Ce n'est pas du prédictif. Le prédictif nous contraindrait, et pour le moment je ne connais pas d'outil qui va nous donner l'adresse du cambriolage qui va avoir lieu demain.» [45]

Derrière le terme « d'analyse décisionnelle », la gendarmerie annonce « un outil d'aide à la décision », qui ne vient pas se substituer à l'autorité traditionnelle. La plateforme est ainsi présentée comme un outil « supplémentaire », qui complète la connaissance opérationnelle des gendarmes de terrain : « Chaque jour, notre plateforme propose un point de vue statistique sur ce qui pourrait arriver en France », affirme son responsable technique. Actuellement, elle est accessible depuis l'intranet de toutes les gendarmeries de la métropole, et des départements et territoires d'outre-mer. Il n'y a aucune restriction d'accès, l'ensemble des gendarmes, tout grade confondu, peut s'y rendre et prendre connaissance de l'analyse du logiciel.

Les données intégrées dans la plateforme sont les chiffres informatisés des faits de délinquance produits par les services de la gendarmerie. Pour créer un modèle de prédiction, la gendarmerie se cale aussi sur les faits passés. Elle a ainsi retenu, sur les huit dernières années, l'ensemble des faits portés à sa connaissance, reposant essentiellement sur les dépôts de plainte :

> « On a fait des études statistiques pour savoir combien d'années de recul était optimal. Si on va trop loin, j'imagine que les faits de 1910 ont très peu d'influence sur ceux de l'année prochaine. Sept-huit ans, c'est l'historique où on a trouvé que l'influence du passé existe encore, et si on ajoute ou diminue le nombre d'années, on diminue la pertinence. On a assez de recul aussi pour saisir la saisonnalité et ses effets sur la délinquance. » (entretien n°2)

La plateforme présente deux onglets distincts. Le premier propose quatre types d'analyses quantitatives de la délinquance au niveau départemental, appelées aussi, « prospectives statistiques » : une première carte nationale portant sur la criminalité (par département), un graphique de l'état de la délinquance par type de faits, une courbe de tendance, et des facteurs d'influence socio-économiques. Ce premier onglet est « plutôt tourné vers la hiérarchie, la chaîne de commandement, la direction générale, le commandement de région, de groupement, de compagnie, etc. ». Ces analyses chiffrées sont destinées à alimenter la prise de décision mais aussi à enrichir les échanges entre partenaires de la sécurité :

> « Quand un commandant de groupement rencontre un préfet de police, ils peuvent discuter : ″voilà ce qu'on peut mettre en place pour lutter contre les atteintes aux biens, mais le mois prochain on attend une baisse, donc on peut peut-être mettre des agents sur un autre type de prévention″. C'est plutôt un outil pour discuter avec les élus, les préfets de police, un outil de management et de communication avant tout. » (entretien n°2)

Toutes les typologies de faits de délinquance sont analysées (ce sont les index de l'observatoire national de la délinquance et des réponses pénales qui ont été retenus). Seulement pour travailler sur l'ensemble des faits de délinquance et établir un modèle prédictif, il faut qu'il y ait assez de données (soit assez de faits au niveau local). En Isère, par exemple, le département le plus criminogène sur le territoire de la gendarmerie, les prédictions peuvent être effectuées sur les cambriolages, comme les atteintes aux biens. Mais, aucune prédiction ne peut être calculée concernant les attentats, faits heureusement trop rares pour pouvoir établir un modèle à partir des données passées.

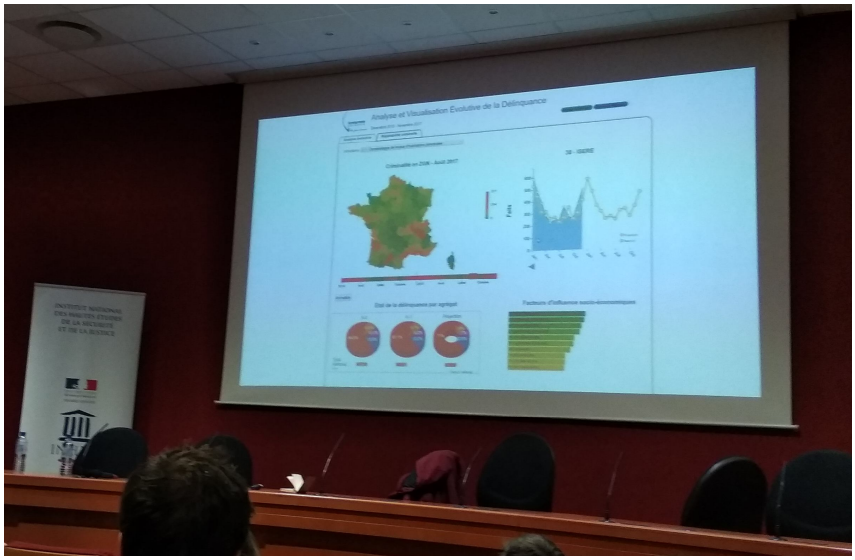
Sur ce premier onglet, figurent aussi, en bas de page, "les facteurs d'influence". Au sein de la machine ont été injectées plus de 600 variables « Insee » (données socio-économiques et certaines caractéristiques territoriales). L'objectif est de renforcer l'analyse des agents sur le terrain mais « sans pour autant produire de lien de causalité garanti à 100% ». Par exemple, le logiciel peut, pour certains territoires, montrer que les cambriolages se produisent plus souvent dans des zones résidentielles construites entre 1991 et 2008. Ces éléments ont pour objectif d'enrichir les analyses des phénomènes de délinquance et d'orienter les missions des gendarmes sur le terrain.

[45] « 22 v'là la police prédictive ! », par Antoine Beauchamp, France culture, le 05/12/2018.
Lien URL : https://www.franceculture.fr/emissions/la-methode-scientifique/la-methode-scientifique-du-mercredi-05-decembre-2018

Le service de data-scientist de la gendarmerie nationale

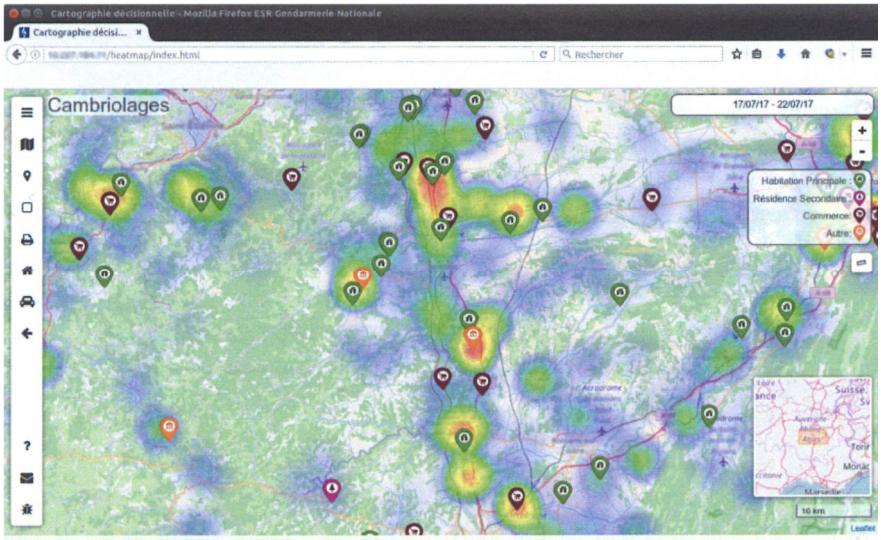
Source : gendarmerie nationale

Le premier onglet tourné vers l'analyse statistique de la délinquance



© Camille Gosselin / IAU îdF

La carte de chaleur interactive : le volet opérationnel de la plateforme



Source : gendarmerie nationale

Le deuxième onglet correspond à une carte de chaleur, à l'échelle nationale, sur laquelle il est possible de zoomer jusqu'à une adresse précise. Cette carte interactive incarne le volet « plus opérationnel » de la plateforme.

> « C'est une sorte de carte de chaleur, son ambition est d'être un outil multi-échelles, mais pour quelques faits, on se concentre ici sur certaines priorités ministérielles : les cambriolages et les vols liés à l'automobile, car ce sont aussi les faits où l'on possède le plus de données. Sur la plateforme, le gendarme peut choisir l'espace temporel qui lui va bien : il peut visualiser les tendances sous forme de carte, par journée, semaine ou mois. » (entretien n°2)

Depuis les années 1980-90, aux États-Unis comme en Europe, les cartes représentant la répartition spatiale de la criminalité sont couramment utilisées par les forces de sécurité. En cela, la carte de chaleur de la plateforme d'analyse décisionnelle ne constitue pas une grande innovation. Sa plus-value est de projeter les zones géographiques les plus sensibles à venir : en bleu, les zones les moins sensibles, en rouge, les zones les plus à risques, et un ensemble de dégradés de couleurs (vert et jaune) pour signifier de potentiels secteurs à surveiller. « L'objectif est de délimiter des zones, dans lesquelles le plus de faits possibles est probable de se produire », témoigne le responsable technique de la plateforme. Il s'agit donc de prédire certains types de faits, dans l'espace et dans le temps. Pour ce second onglet, la gendarmerie ne travaille que sur les données des cambriolages et des atteintes liées aux véhicules (agrégat formé autour des vols automobiles, vols à la roulotte, vols d'accessoires, vols de deux roues, vols de fret, etc.). Officiellement donc, la plateforme est présentée comme un outil opérationnel, venant alimenter les choix stratégiques du terrain :

> « Nous sommes des gendarmes, nous faisons du contrôle de zone, on ne va pas se mettre devant l'adresse que nous signale le point rouge, mais on va plutôt patrouiller dans la zone, on va se montrer visible pour dissuader la commission d'infractions. Le décideur opérationnel sur cette zone-là, par exemple, il va voir qu'il y a des risques de cambriolages, donc il va pouvoir décider de prendre en compte ces données-là et d'organiser son service en fonction de ces données-là. Notre métier n'est pas de laisser se commettre l'infraction, mais d'empêcher qu'elle ne se commette, donc ce n'est pas un logiciel pour faire du flagrant délit, c'est un logiciel qui est destiné à sécuriser la population et notre zone de compétence. Le flagrant délit, c'est très dangereux, on ne connaît pas la détermination de la personne qui est en face de nous, quels sont ses moyens, si elle est armée, cela peut provoquer des blessures pour les gens autour. Non, non, nous, on est là pour empêcher que les infractions ne se commettent. [46]»

Du point de vue du fonctionnement de la plateforme, les ingénieurs de la gendarmerie utilisent différentes méthodes statistiques, en fonction des territoires et des types de délits. Par exemple, la méthode retenue pour le département de l'Isère n'est pas la même que celle des Hautes-Alpes, « parce que la criminalité change, les caractéristiques du département changent, la distance moyenne entre les résidences change, la composition sociale, etc. Quand on a commencé, on ne s'attendait pas à autant de différences ». Plus d'une vingtaine de méthodes sont ainsi implémentées pour prédire. « Mais au final, ce n'est pas la solution qui est mathématiquement plus proche de la réalité qui va nous intéresser. Nos utilisateurs préfèrent avoir une bonne représentation des tendances et des évolutions futures, qu'avoir exactement le nombre de délits précis. » (entretien n°2)

L'hypothèse retenue par la gendarmerie est assez proche des modèles de prédiction décrit *supra*. Ce sont les faits passés qui détermineraient principalement les faits futurs. De par la nature des données et pour respecter la réglementation française, la gendarmerie s'intéresse aux zones de commission des faits de délinquance (et non aux individus). Elle vise donc, par l'analyse prédictive, les secteurs géographiques où se concentrent les délits. Deux composantes entrent dans cette analyse, comme la définit le SCRC : la saisonnalité (les faits passés à la même époque, les années antérieures) et la tendance (ce qui est arrivé hier, avant-hier, les événements imprévisibles, etc.). « On analyse ces deux dimensions. L'idée, c'est que la plateforme soit le plus à jour possible pour les agents de terrain. On a des prédictions mais on recalcule à chaque fois qu'on accède à d'autres données ». En théorie, les données produites par les services de la gendarmerie sur le territoire national sont centralisées au SCRC pour alimenter au quotidien la plateforme, et pour constamment recalculer les prédictions. En pratique, l'accès aux données reste une préoccupation importante, bien que les ingénieurs du SCRC aient préparé la plateforme « à capter les données chaque nuit ». « De notre côté, c'est prêt, mais il y a toujours des problèmes de transmission des données. Les versements, chaque soir, sont compliqués à mettre en œuvre ». Ces problèmes de transmission des données impactent la précision de l'outil et la production des prédictions.

[46] *Ibid*.

2.2 Usages et acceptabilité de l'outil

La plateforme d'analyse décisionnelle a récemment fait l'objet d'une expérimentation dans plusieurs départements. Les témoignages recueillis auprès de quelques gendarmes nous renseignent sur les usages concrets et opérationnels de la plateforme, et les perspectives d'évolution souhaitées.

2.2.1 Des prédictions qui alimentent l'opérationnel ?

La plateforme d'analyse décisionnelle de la gendarmerie nationale a, officiellement, fait l'objet d'une expérimentation lancée dans onze départements français. La fin de l'expérimentation a coïncidé avec le début du terrain de cette étude. Il a donc été possible de recueillir quelques éléments de bilan. Nous avons échangé avec quatre responsables de groupements de gendarmerie qui ont expérimenté (et expérimentent toujours) la plateforme d'analyse décisionnelle. N'ayant pas eu accès à la liste complète des onze départements participants, nous avons eu des retours épars. Cependant, le recueil de ces quelques témoignages donne à voir diverses postures et usages de la plateforme d'analyse décisionnelle et soulève bien des questions. La gendarmerie n'a, d'ailleurs, pas donné de consignes particulières concernant l'utilisation de la plateforme pendant cette expérimentation, l'objectif étant d'insister sur l'aide que fournit l'outil dans la prise de décision. Récemment, par la voix du colonel Laurent Collorig, quelques résultats et retours opérationnels ont été publiquement formulés :

> « Il y a un retour positif [sur l'utilisation du logiciel] d'abord en termes d'acceptabilité, à partir du moment où ce logiciel ne s'impose pas à la décision mais aide à la décision. C'est-à-dire, que le responsable de la gendarmerie sur le terrain garde la main sur son pouvoir décisionnaire, on ne va pas le contrôler par rapport au logiciel, ça c'est important, par rapport à ce qui se passe dans d'autres pays. Du moment qu'on a une bonne acceptabilité, on a une bonne utilisation du logiciel. […] Ce que je peux vous donner, c'est qu'en moyenne, dans ces onze départements [où le logiciel a été expérimenté], sur les premiers mois de l'année, la baisse de la délinquance a été supérieure, pour ce qui concerne les cambriolages et les atteintes liées aux véhicules, par rapport à la baisse de la délinquance observée en zone gendarmerie sur la même période […]. Le logiciel avait anticipé 87% des faits. Je vais quand même modérer mon propos, nous avions anticipé 87% des zones où ce sont produits les cambriolages, nous n'avons pas les adresses des cambriolages.»[47]

En janvier dernier, lors d'une présentation de la plateforme à l'INHESJ, le colonel a indiqué que la délinquance aurait baissé dans les compagnies utilisant le logiciel, et que son usage aurait eu des incidences positives sur les politiques de sécurité au quotidien, favorisant notamment les échanges avec les élus locaux. Des éléments de résultats qu'il pondère directement : « même si on n'attribue pas clairement cette réussite qu'au logiciel. »

Nos interlocuteurs semblent, dans l'ensemble, intéressés par le développement de l'intelligence artificielle dans leur domaine (ce qui ne veut pas dire que ce sujet fasse consensus au sein de la gendarmerie). Ils considèrent le prédictif comme « une grande opportunité pour demain », permettant plus largement, « de prendre conscience des chantiers d'avenir qui se posent au sein de la gendarmerie ». Pour autant, la plateforme d'analyse décisionnelle apparaît comme un sujet clivant. Bien qu'elle soit régulièrement caractérisée comme « le début de quelque chose » ou « une première brique », elle semble avoir créé des adeptes comme des plus sceptiques. Son développement apparaît, pour certains, comme « une véritable opportunité », « un atout » pour renforcer les moyens d'action de la gendarmerie. C'est surtout la carte de chaleur, le volet plus opérationnel de l'outil, qui est utilisée et commentée, car « elle donne à voir une représentation cartographique qui s'imprime sur la rétine ». Elle est appréciée pour son résultat « très visuel », qui permettrait *in fine* de faciliter l'appropriation du territoire. Voués à changer régulièrement de postes, les gendarmes s'accordent à dire que la plateforme est un moyen utile pour appréhender les territoires et les phénomènes de délinquance plus rapidement, notamment lors de leur prise de fonction. La carte de chaleur permet de repérer « en un clin d'œil » les zones sensibles à l'échelle d'un département. Une manière de valoriser aussi les connaissances produites par les services de la gendarmerie, en les rendant accessibles à tous. En revanche, la plateforme est peu évoquée comme un moyen d'alimenter les échanges et les communications avec les partenaires locaux. Un commandant de groupement indique que les prédictions en tendance (issues du volet prospectives statistiques) ont été utilisées par l'un de ses commandants de brigade pour alerter les habitants :

[47] *Ibid.*

> « Quand on remarque que pour le mois suivant, on attend une hausse des cambriolages, c'est intéressant d'en informer un dispositif comme voisins vigilants. On leur demande de porter une attention particulière sur certains secteurs. Par contre, on ne transmet pas de carte, et on ne parle pas de la source et de la plateforme prédictive. » (entretien n°3)

La démarche lui paraît intéressante et plus généralement, il précise que les éléments quantitatifs produits par la plateforme enrichissent ses échanges avec les partenaires locaux (sans pour autant citer sa source).

À l'inverse, certaines critiques sont émises concernant les prédictions du logiciel. Les analyses qu'il proposerait ne seraient pas si complémentaires à celles effectuées au quotidien par les gendarmes. Il indiquerait essentiellement des périmètres déjà sous surveillance des forces de sécurité ou connus des services. Cet argument remet en question l'acceptabilité de l'outil au sein de la gendarmerie, et plus particulièrement auprès des gendarmes de la base :

> « Ils [les gendarmes de la base] considèrent que ce n'est pas assez pointu. En gros, l'outil ne leur apporte pas assez, pour un gendarme au niveau local. Ce qui est assez différent pour un commandant de groupement ou de compagnie. Pour un gendarme au niveau local qui connaît normalement bien sa délinquance, la plateforme présente peu de plus-value. S'il est là depuis quatre ou cinq ans, de manière empirique, il aura déjà identifié les zones à contrôler, il va se constituer sa propre analyse prédictive, parce qu'il voit passer les messages d'informations judiciaires, parce qu'il a identifié les vulnérabilités de certains secteurs, etc. Mais cela peut être utile pour le jeune gendarme qui arrive qui, sur six mois ou durant sa première année, doit appréhender son territoire. Ici, il y a beaucoup de *turn-over*, donc cela peut aider. Mais au bout d'un an, avec l'appui des anciens, il aura fait le tour. » (entretien n°4)

La difficulté repose sur la nature même de la plateforme et sur la manière dont elle est définie et présentée. La communication officielle entourant le dispositif oscille entre l'annonce d'un outil prédictif et la prise de distance par rapport aux velléités de prédictions. Pour les concepteurs, la plateforme a d'ailleurs pour principale priorité de donner un avis, et de ne pas figer l'analyse et la prise de décision (ce qui est notamment reproché au logiciel Predpol, qui recommande aux patrouilles de police de circuler dans des zones très précises de 200 mètres sur 200 mètres) :

> « Pour les onze départements en expérimentation, nous avons fait une présentation de l'outil, pour leur montrer le fonctionnement et pour les rassurer : "Ce n'est pas Madame Irma", il y a une analyse mathématique derrière, on n'essaie pas de "voler vos boulots", et ce n'est pas non plus un outil qui est en train de dire "fais ceci, fais cela", c'est une opinion qu'il faut confronter à vos propres connaissances. C'est comme un autre gendarme, qui aurait un peu plus d'expérience, un peu de plus de connaissances. » (entretien n°2)

Malgré ce souci de pédagogie, sur le terrain, certains agents se montrent perplexes et remettent en question les choix qui orientent le développement de la plateforme.

> « Le problème de cet outil, c'est que ce n'est pas un outil algorithmique. Il ne prend pas en compte la météo, le taux de chômage, il ne prend pas assez de variables, c'est seulement un outil statistique. Il va vous sortir la délinquance sur les six dernières années, et à partir de là, il va construire des cartes de chaleur, qui sont très précises, car on peut descendre jusqu'à la rue. […] Mais pour ceux qui ont regardé, les zones chaudes, on les connaît déjà. » (entretien n°4)

Au niveau local, les gendarmes ont largement intégré les éléments de langages associés à l'analyse décisionnelle : un outil d'aide à la décision qui ne vient pas se substituer à leur autorité. Mais leurs attentes opérationnelles concernent surtout la précision des prédictions effectuées par la machine. Plusieurs demandes ont été, notamment, rapportées lors d'une audition clôturant la fin de l'expérimentation de la plateforme d'analyse décisionnelle. Certains de nos interlocuteurs ont fait part de ces remarques que nous synthétisons ci-dessous :

- La précision horaire des prédictions, la machine effectuant pour le moment des prédictions à la journée.

> « C'est pareil pour toute la journée, donc là c'est un peu compliqué. Nous, ce qui nous intéresse, c'est par demi-journée, la distinction entre le jour et la nuit, etc. Le top serait par demi-journée. Il faudrait au moins des plages horaires de huit heures, par exemple : le matin, l'après midi, et la nuit. Cela pourrait présenter une utilité. Nous, ça nous permettrait d'orienter les patrouilles sur le terrain. […] Une analyse sur une journée n'est pas assez fine pour orienter le service […]. » (entretien n°3)

- La distinction entre faits au sein d'une même typologie.

  « Dans les pistes d'évolution qu'on a soulevées, on a aussi demandé à ce qu'une distinction entre types de faits puisse exister. Aujourd'hui, on a tous les cambriolages dans le même *item*. Mais entre un cambriolage dans une résidence principale, secondaire, des locaux commerciaux, des cabanons de jardins, des locaux de la mairie, etc. ce n'est pas du tout la même chose. Or, dans l'outil, tout est mélangé. » (entretien n°3)

- L'intégration du facteur météorologique pour affiner l'analyse prédictive de la délinquance et l'orientation des patrouilles.

  « Si, en plus l'année dernière, il n'y a pas eu de neige au mois de février et que cette année, il y en a, ce facteur météo va avoir beaucoup plus d'incidence sur la délinquance. La météo n'est pas prise en compte par la machine, et, par exemple, pour les cambriolages, c'est un élément primordial. » (entretien n°4)

- La création d'axes routiers de chaleur qui correspondraient davantage au mode d'action des gendarmes sur le terrain.

  « Plus que des zones, c'est des axes routiers de chaleurs qu'il serait intéressant de déterminer. Des axes qui sont susceptibles de favoriser le déplacement des délinquants car ils permettent d'accéder à des zones qui se font taper. Car sur l'outil, on voit les zones d'impact, mais on ne voit pas les zones qui permettent d'y arriver. Or si on veut contrôler, ce n'est pas dans la zone d'impact. Je ne mets pas mes points de contrôle dans les zones de chaleur, je mets mes points de contrôle sur les axes d'accès à ces zones de chaleur. Notre métier, c'est de procéder principalement par contrôles routiers. » (entretien n°4)

L'ensemble de ces remarques (qui sont par ailleurs, pour certaines, travaillées par les data-scientist du SCRC) donnent surtout à voir la manière dont est investi l'outil par les commandants de groupement. Leurs attentes traduisent une envie d'accéder à des prédictions précises pour qu'elles alimentent leurs usages opérationnels. D'ailleurs, le manque de portabilité de la plateforme est aussi soulevé. Actuellement, le logiciel n'est disponible que *via* l'intranet de la gendarmerie sur l'ensemble des smartphones et tablettes, mais son application n'a pas encore été développée, ce qui rend sa portabilité limitée sur le terrain (sans parler de l'accès au réseau 4G qui s'avère difficile sur les territoires ruraux de la gendarmerie).

De plus, certains gendarmes se montrent très attachés au prédictif et se disent parfois déçus par la plateforme, à l'image de ce qui peut être développé à l'étranger :

> « Il faudrait rapidement passer à la seconde version de l'outil, sinon les gens vont complètement s'en désintéresser […]. En fait ce qui serait intéressant, c'est quand le gendarme part en patrouille, on lui suggère les missions qu'il a à réaliser. Il pourrait rentrer dans un quadrilatère de 1km sur 1km et la machine devrait lui proposer des missions, par exemple : risque de cambriolages à tel endroit, aller voir le référent voisin vigilant, etc. C'est un peu ce que fait Predpol et c'est l'avenir ! » (entretien n°4)

Malgré cet intérêt pour le prédictif, des interrogations subsistent aussi quant aux risques de surévaluer les prédictions de la plateforme en leur donnant parfois trop d'importance dans l'analyse des phénomènes que les gendarmes ont à appréhender : « quelle valeur donner à l'information produite par l'algorithme ? », s'interroge un colonel. En cela, les gendarmes interviewés insistent sur la nécessaire prudence quant aux baisses ou hausses de la délinquance attribuées à l'usage du logiciel.

En termes de fréquentation, le nombre de fois où les agents se connectent pour prendre connaissance des analyses et prédictions, est très variable d'un gendarme à l'autre. Néanmoins, aucun n'affirme se rendre sur le logiciel tous les jours. Un interlocuteur a affirmé se connecter une fois par semaine, « car c'est le plus significatif », un autre y aller « deux fois par mois, et mes commandants de compagnie un peu plus je pense », et un autre a déclaré que durant les deux premiers mois de l'expérimentation, il se connectait très fréquemment « par curiosité surtout. Mais d'une semaine à l'autre, les cartes n'évoluaient pas vraiment », alors il explique s'être à la longue lassé, et ne s'y rend désormais que de façon occasionnelle.

Le dispositif actuel d'analyse décisionnelle figure comme une première étape dans le chantier qu'ouvre l'intelligence artificielle dans le domaine de la sécurité publique. Car, derrière la prédiction des zones de commission de faits de délinquance, c'est aussi toute une réflexion qui s'engage au sein de la gendarmerie sur la gestion et l'optimisation des services de sécurité à l'heure des *big data*.

2.2.2 Entre prédiction et gestion

La quantité de données produites par les services policiers interroge à la fois leur stockage, leur gestion et leur exploitation. Les données doivent aussi répondre aux besoins informationnels et analytiques des agents et de l'administration policière. Ce besoin informationnel concerne la délinquance, mais également la gestion de l'administration. La plateforme d'analyse décisionnelle développée par la gendarmerie se pose déjà comme un moyen de répondre à des enjeux d'optimisation du service de sécurité publique sur l'ensemble du territoire national.

> « En France, on ne parle pas de diminuer les effectifs de police et de gendarmerie. On est plutôt dans une perspective de recrutements. Donc l'algorithme va nous apporter un plus, sur le volet ressources humaines, pour mieux gérer, mieux attribuer les effectifs sur tels ou tels coins du territoire. C'est un objectif de deuxième plan pour la gendarmerie qui se dote d'un outil opérationnel pour aider le décideur à établir son plan d'action, mais aussi au regard des résultats de chaque département, on peut décider de l'allocation des ressources, ça fait aussi partie des politiques publiques, pour toujours mieux allouer, mieux dispatcher […]. Cela ne veut pas dire non plus qu'on va fermer une brigade de gendarmerie. Pour la gendarmerie mobile, hors contexte du maintien de l'ordre, ce sont des effectifs qui peuvent être projetés sur l'ensemble du territoire, c'est là qu'il peut y avoir des arbitrages et identifier les zones où du renfort est nécessaire et notamment des escadrons de gendarmerie mobile. Pour le préfet de zone de défense, cela peut être un outil […]. » (entretien n°1)

Au niveau local, la plateforme est aussi investie comme un moyen de comparer les territoires entre eux. Un gendarme précise qu'il utilise la plateforme pour situer les résultats de son département sur le plan national :

> « L'outil permet aussi de voir ce qui se passe ailleurs, pour un commandant de groupement et de compagnie, c'est intéressant. Moi, ça me permet de me comparer, avec les territoires qui rencontrent des problématiques équivalentes. Cela me permet de me situer, de savoir où je me situe dans le top dix des départements, plus je perds de place, mieux c'est ! » (entretien n°4)

Au niveau du commandement de groupement, l'outil est aussi identifié comme « une aide à la gestion managériale, c'est pour cela que c'est une aide à la décision, il permet d'effectuer des choix ». Un colonel surenchérit :

> « Ce n'est pas tant la géographie de la délinquance qui est importante, c'est plutôt quelle stratégie je vais mettre en place, quel choix je vais devoir faire dans l'analyse opérationnelle, pour allouer les moyens humains suffisants, sur le créneau horaire et l'espace géographique qui va bien, pour obtenir le meilleur résultat possible. On recherche le meilleur rendement opérationnel, est-ce que je vais allouer mes effectifs sur telle commune ou sur telle autre. » (entretien n°5)

Récemment, la gendarmerie a d'ailleurs mis en avant, à plusieurs reprises, des démarches locales pilotées par des commandants de groupement, dans l'objectif d'accroître l'efficacité des gendarmes. C'est le cas en Lot-et-Garonne, par exemple, où un projet de réorganisation et de redéploiement des effectifs a été mis en place dans un but simple : l'optimisation des ressources sur le terrain, pour assurer à la fois les patrouilles de surveillance et les interventions, et en limitant le temps des déplacements (pas plus de 30 minutes). Ce projet semble faire des émules, puisque des initiatives similaires se développent sur d'autres territoires, en réponses aux besoins opérationnels.

L'usage de la plateforme d'analyse décisionnelle amène également à discuter l'un des principaux objectifs de la police prédictive : la proactivité des forces de sécurité. Les retours d'expérience concernant l'utilisation de l'outil ne semble pas remettre en question les modes opérationnels, ni même le registre d'action des gendarmes. Les adeptes comme les sceptiques envisagent la plateforme comme un moyen qui conforte leurs modes d'intervention. « L'utilisation actuelle de l'algorithme prédictif sur des données géographiques fait écho à la logique d'intervention des patrouilles : sécurisation, prévention, dissuasion », affirme un colonel. L'outil permet, notamment, d'accompagner la hiérarchie dans le montage d'opérations complexes de contrôle, nécessitant une forte présence des gendarmes sur le long terme :

> « Cet outil, les commandants de groupement et de compagnie l'utilisent car c'est à ce niveau que se décident les opérations coordonnées. Moi, je l'utilise car je fonctionne beaucoup par opérations coordonnées. Je mets trente-cinq points de contrôles, avec hélicoptères, etc. sur le département, j'ai six compagnies, qui comptent entre 110 à 180 hommes et qui, pareil, organisent des opérations coordonnées de manière régulière. Avec les opérations coordonnées, on est sur la phase prévention, on est là pour empêcher la commission des délits. Quand il y a une enquête, c'est déjà trop tard. Notre cœur de métier, c'est bien la prévention et empêcher que les délits ne se produisent. On vit

> dans un monde concurrentiel, donc tous ceux qui ne viennent pas taper ici, iront ailleurs, donc le principe, c'est bien la tenue du terrain ! L'algorithme, il est censé nous aider dans nos missions de prévention-dissuasion. Avant de projeter 200-250 gendarmes H24 sur le terrain, le but, c'est de produire de l'insécurité pour les délinquants. Donc pour produire de l'insécurité, l'une des clés, c'est de produire des opérations coordonnées, et pour faire cela, je me base sur les cartes prédictives. » (entretien n°4)

Le registre de la prévention se confond parfois avec celui de la dissuasion, donnant lieu à une réflexion sur l'adéquation entre les faits de délinquance et la répartition des moyens humains envisagés pour éviter la commission des délits. La mise en place d'une plateforme prédictive doit répondre à des logiques d'action : « L'idée [en utilisant la plateforme], c'est de limiter les patrouilles itinérantes, car elles sont complètement inefficaces », explique un gendarme. Patrick Perrot, fût à la tête du SCRC et a initialement contribué au développement de la plateforme d'analyse décisionnelle, dans un article publié dans la revue « Sécurité globale », il explique les contraintes à positionner une administration, telle que la gendarmerie sur le registre de la proactivité : « Toute la difficulté se situe entre l'objectivité d'une analyse *a posteriori* et la nécessaire célérité d'une décision. Conjuguer l'*a posteriori*, le temps réel et l'*a priori* nécessite de développer une capacité de réflexion, d'analyse approfondie mais aussi d'action. En d'autres termes, il s'agit d'adopter une vision de rupture pour être capable d'envisager des forces de l'ordre proactives, adaptatives et réactives. » [48]

La recherche de proactivité, dans le contexte des *big data*, s'oriente ainsi dans l'exploitation de l'information collectée et produite par les forces de sécurité. Le développement des technologies de l'information et l'interprétation des données sont identifiés comme des leviers pour rendre la gendarmerie plus efficace aussi bien en termes d'actions que de coûts. Un colonel conclut lors de notre entretien : « On est conditionné à travailler en mode réactif, je le vois bien sur le terrain ». Le modèle prédictif actuel ne remettrait pas en question le prisme professionnel, ni même le paradigme de la prévention de la délinquance, comme il lui est souvent attribué. Néanmoins, au sein de la gendarmerie nationale, il ouvre d'autres chantiers, comme celui des ressources humaines ou encore de la donnée. Les retours sont mitigés sur les données produites par les gendarmes eux-mêmes : « La plateforme d'analyse décisionnelle participe à une prise de conscience, pour des sujets moins attractifs, comme la nécessité d'avoir un puits de données propres. Il faut nettoyer nos données, et faisons déjà de l'analytique! », déclare un gendarme.

Enfin, la plateforme d'analyse décisionnelle pose plus largement le sujet de l'efficacité d'une politique publique. Nos interlocuteurs la considère comme une première étape, qu'ils souhaiteraient voir évoluer pour « pouvoir calculer l'impact des patrouilles de gendarmes sur la délinquance elle-même » ; « ce qui serait intéressant de savoir, ce serait de connaître l'impact de notre activité sur la délinquance ». Certains gendarmes se sont en effet dits intéressés par la possibilité de visualiser l'impact de leurs activités sur la délinquance constatée. Pour le SCRC, cela pourrait être envisagé comme une piste à creuser, en s'appuyant notamment sur les données géo-localisées des véhicules de patrouilles.

***

Depuis 2017, la plateforme d'analyse décisionnelle de la gendarmerie fonctionne sur l'ensemble du territoire national, et a fait l'objet d'une expérimentation sur onze départements. Alimentée par les données informatisées des faits portés à la connaissance de l'administration sur les huit dernières années, elle présente une analyse statistique de la délinquance par département, et une carte de chaleur des zones sensibles futures pour les cambriolages et les atteintes liées aux véhicules. Pour les plus critiques, les velléités prédictives de l'outil sont limitées (en comparaison de certains logiciels utilisés par les polices américaines) car il se base essentiellement sur les données du passé et ne prend pas assez en compte d'autres variables. Son analyse reposerait alors sur des calculs de probabilité. Principalement utilisée par la hiérarchie, la plateforme s'adresse surtout à la chaîne de commandement. Cependant, si dans l'ensemble elle n'est pas considérée comme un outil achevé, elle a su créer des attentes, notamment au niveau opérationnel. La plateforme ne vise pas tant à comprendre et à analyser les phénomènes de délinquance, qu'à répondre aux enjeux d'optimisation des ressources et d'adéquation entre la délinquance et la répartition territoriale des effectifs de gendarmes. À ce stade, il serait prématuré de considérer cette démarche comme un véritable changement de paradigme. Tout en posant un certain nombre de questions, elle tend plutôt à conforter les dynamiques observées depuis plusieurs décennies au sein des forces de sécurité (orientations professionnelles, management, politique du chiffre, etc.).

[48] Perrot P., « Disruption et révolution numérique : une nouvelle ère pour la sécurité », 2017.

2.3 Vers une police algorithmique ?

Au sein des forces de sécurité, l'avenir de l'analyse de la délinquance reposerait-elle principalement sur l'usage d'algorithmes ? Après la police de l'information tournée vers la gestion, la circulation des données et l'usage des technologies de l'information[49], la police algorithmique serait-elle l'aboutissement « d'une police intelligente », qui aurait su tirer profit des *big data* pour optimiser ses services face à l'insécurité ?

2.3.1 La donnée au cœur de l'action policière

La production, la gestion et l'exploitation des données sont au cœur du *policing* territorial et soulèvent de multiples interrogations. Nos interlocuteurs ont à maintes reprises, signifié que le nettoyage des données (aussi bien au sein de la gendarmerie qu'au sein de la police) est un véritable enjeu, qui renvoie plus largement au sens et à l'interprétation de l'analyse produite. Actuellement, les données créées par les services de sécurité sont qualifiées de « données administratives », ne répondant pas, initialement, à un besoin analytique. Elles visent, principalement, à « objectiver » l'insécurité et à quantifier l'ampleur de la délinquance. En découle la manière dont elles sont renseignées par les agents de la base. Du côté de la police comme de la gendarmerie, on regrette le manque de précision avec lesquelles elles sont enregistrées (concernant aussi bien les faits que leur localisation). Une autre question porte sur l'accès à ces données. Il n'existe pas de puits de données propre et cohérent du côté de la gendarmerie (ni probablement du côté de la police). Dans ce cadre, la transmission quotidienne des données et leur nettoyage restent une préoccupation majeure pour alimenter les calculs de prédiction.

Au sein de la gendarmerie, les données qui alimentent la plateforme d'analyse décisionnelle proviennent des faits constatés et portés à la connaissance des services. Comme toujours, ces statistiques soulèvent l'épineuse question des biais ; elles reflètent l'activité policière avant tout et ne prennent pas en compte les victimes qui ne portent pas plainte. Or, ce chiffre noir, autrement dit l'ensemble des faits non portés à la connaissance des services de police représente une part non négligeable de la délinquance effective. L'enquête "Victimation et sentiment d'insécurité" de l'IAU îdF l'illustre bien[50]. D'après les résultats de l'enquête de 2017, 24% des victimes d'atteintes aux biens (incluant les atteintes liées aux véhicules, les cambriolages et les vols sans violence) déclarent ne pas avoir porté plainte estimant que « cela n'aurait servi à rien ». Elles sont 18% à répondre que « cela n'en valait pas la peine ». En Île-de-France, tous types d'atteintes confondues, environ une victime sur trois seulement porte plainte (34%). Ces chiffres (ré)interrogent la nécessité de diversifier les mesures de la délinquance, y compris dans les calculs de prédictions. À terme, le risque n'est-il pas d'isoler des territoires et d'écarter une partie de la population de l'offre publique de sécurité ? C'est un enjeu que pose l'utilisation de ce type de logiciel, en réaffirmant les risques d'accentuation d'une offre de sécurité à deux vitesses : numérique et automatique pour les désordres et violences urbaines, humaine et renseignée pour les autres types de faits. Une répartition sociale et territoriale de la sécurité qui pourrait recouvrir une dimension discriminante (qui par ailleurs, existe déjà pour certains).

En outre, d'aucuns s'interrogent quant à la nature des données portant sur la sécurité publique. En France, à la différence des États-Unis, elles ne sont pas considérées comme des "données d'intérêt public". Les données produites par les services de sécurité restent internes aux administrations policières. Et c'est un sujet auquel les organisations sont attachées, notamment la gendarmerie. C'est d'ailleurs pour cette raison que le développement de la plateforme d'analyse décisionnelle à été développée par des agents recrutés pour cette mission spécifique au sein de la gendarmerie.

> « La police et la gendarmerie partent du principe que les données qu'elles produisent, ce sont leurs données. Mais on pourrait partir du principe que non, et que ce sont des données publiques, d'intérêt public. Débarrassées de leurs identifiants personnels, pourquoi elles ne seraient pas publiques ? » (entretien n°8)

C'est, en effet, au regard de ce qui est pratiqué aux États-Unis que certaines remarques sur le positionnement des institutions françaises se font entendre :

> « Aux États-Unis, on peut faire des programmes discriminants, mais il y a une évaluation derrière, car la police publie ses données, et qu'il y a des associations qui alertent sur des cas de

[49] Jobard F., De Maillard J., *Sociologie de la police, politiques, organisations, réformes*, 2015.

[50] L'enquête « Victimation et sentiment d'insécurité en Île-de-France » est menée tous les deux ans, depuis 2001, auprès d'un échantillon de 10 500 Franciliens âgés de 15 ans et plus. Lien des résultats de l'enquête 2017 : http://www.iau-idf.fr/nos-travaux/publications/victimation-et-sentiment-dinsecurite-en-ile-de-france-1.html

> discrimination, et d'abus de pouvoir. En France, l'évaluation des ZSP, de la vidéosurveillance, il n'y en a jamais eu et pourtant on dit que ça marche ! Donc on ne va pas sur l'expérimentation, mais quand on expérimente, on n'évalue pas, donc c'est un problème pour que tous ces outils innovants puissent se développer. On regarde beaucoup les États-Unis et on pointe les problèmes, mais on ne fait rien. » (entretien n°8)

En France, le sujet des données est intimement lié à celui des libertés individuelles et soulève des questions d'ordre politique. Dans le débat public, des craintes s'expriment régulièrement quant au recueil et à l'utilisation de données à caractère personnel par les agents de l'État (quand bien même, ils œuvrent à assurer la sécurité publique). Cette tendance illustre une perte de confiance en l'État et en ses services. En comparaison, c'est plus récemment, notamment au moment de la mise en place du RGPD, que des inquiétudes similaires se sont exprimées à l'égard des « géants du web ». Un colonel donne son point de vue sur ce sujet :

> « Quand on a un délinquant à rechercher, on va regarder sur son Facebook, parfois on a son adresse par je ne sais quelle opération du saint esprit, car certains fichiers des services de l'État ne sont pas toujours à jour, alors que sur les réseaux sociaux, les sources ouvertes, on dispose d'informations parfois plus pertinentes. C'est là qu'il faut mettre un contrôle "béton" *a posteriori*, pour que cette donnée soit bien récupérée dans un but d'utilité publique et pas à des fins personnelles. Mais c'est culturel, tant qu'on n'aura pas un système basé sur la confiance dans les agents de l'État, qui sont chargés d'assurer la sécurité, et bien ça ne pourra pas fonctionner. Mais il faut aussi un système transparent : on est allé chercher telles données, à tel endroit, pour tel type de finalité. Il faut pouvoir expliquer que c'est pour un but d'utilité publique […]. On donne bien des données personnelles à des sociétés privées, comme Google, Facebook, etc. alors pourquoi on ne les donnerait pas aux services de l'État qui assurent la sécurité ? » (entretien n°4)

Enfin, certains de nos interlocuteurs estiment que les données produites par les administrations policières ne sont plus indispensables au développement d'outils prédictifs. L'expérimentation menée par l'ONDRP (cf. *supra*) montre d'ailleurs que certaines analyses prédictives tendent, en se focalisant sur les données contextuelles, à prédire les lieux favorables à la commission de certains faits de délinquance. Ce projet vise à se détacher des données passées de la criminalité, pour établir une prédiction en s'appuyant sur les données environnementales (entre autres, les caractéristiques du bâti, l'état de l'éclairage public, les horaires d'ouverture et de fermeture des commerces, l'emplacement des distributeurs automatiques de billets, etc.). Ce serait « la constitution d'un véritable système d'information géographique » qui permettrait de mieux orienter les patrouilles sur le terrain, et d'analyser aux préalables les vulnérabilités d'un site face à la délinquance. Ce cadre de réflexion renvoie directement au développement de la prévention situationnelle qui, depuis les années 1970, prend de plus en plus d'ampleur dans les politiques de prévention de la délinquance.

Dans le contexte actuel, la production massive de données laisse envisager d'autres types d'analyses en matière de sécurité. Certains gendarmes ont montré beaucoup d'intérêt à prendre en compte les échanges et contenus générés sur les médias sociaux, qui révèlent, parfois en temps réel, si une situation liée notamment à une manifestation ou un regroupement, peut dégénérer ou pas. Par exemple, en 2017, aux États-Unis, des manifestations de suprémacistes blancs organisées à Charlottesville ont donné lieux à des affrontements et à la mort d'une militante anti-raciste. Suite à ces violences, une plus grande vigilance a été portée aux publications sur les réseaux sociaux, pour éviter que ce type de débordements ne se produisent à nouveau. Certains gendarmes évoquent également les possibilités que pourrait recouvrir l'exploitation des données émises et produites par les smartphones eux-mêmes. Ces données permettraient d'identifier rapidement l'importance des flux, de visualiser l'encombrement de certains espaces pouvant engendrer d'éventuelles tensions. Elles intéresseraient, en premier lieu, les forces de l'ordre et les services en charge de la gestion et du maintien de l'ordre public.

2.3.2 L'algorithme, entre sciences et politiques managériales

L'intégration des sciences « dites dures » dans l'analyse des phénomènes de délinquance ne date pas de l'intérêt croissant pour la police prédictive. En outre, l'usage des technologies de l'information et de la communication viennent résolument ancrer les forces de sécurité dans des stratégies managériales. Au sein de la gendarmerie, la mise en œuvre d'un outil prédictif s'accompagne de réflexions plus larges portant sur l'optimisation territoriale des effectifs, rapportée à l'intensité des phénomènes de délinquance « objectivée » par la machine. Un ensemble de démarches qui vise à rationaliser la gestion des patrouilles pour garantir une meilleure efficacité. Pourtant, pour le moment,

il est difficile de prétendre que l'expérimentation menée à la gendarmerie puisse à elle seule, impacter la délinquance au niveau local.

Dans ce cadre, les postures professionnelles semblent (ré)affirmées par l'arrivée du prédictif. L'outil tel qu'il est développé aujourd'hui s'adresse à la hiérarchie, et semble peu concerner les agents de la base. De ce fait, les postures et l'ensemble des stratégies opérationnelles ne font pas l'objet d'une doctrine renouvelée. Les gendarmes s'appuient, notamment, sur la carte prédictive pour mettre en place des opérations de contrôles routiers. L'outil est utilisé pour servir l'ensemble des stratégies dissuasives constitutives du corps des gendarmes pour « tenir le terrain ».

Cependant, certains de nos interlocuteurs se saisissent du lancement de la plateforme prédictive pour soulever des interrogations et des enjeux d'articulation avec, notamment, la mise en place de la police de sécurité du quotidien (PSQ). Serait-elle un moyen de rapprocher autrement les forces de sécurité et le territoire ? Serait-elle propice au développement d'une police prédictive plus locale et davantage tournée vers l'appréhension des causes qui mènent à la déviance ?

> « Il faudrait que cela passe par un changement de doctrine policière. Le changement de doctrine, c'est la PSQ, elle pourrait être un cadre quasi-idéal pour mieux renseigner, mieux produire des données, pour mieux les exploiter pour de l'analyse. Car la PSQ, c'est une police locale, avec des décisions locales, on autorise un chef de service à prendre des décisions seul. C'est de laisser les échelons locaux prendre des décisions pour le local, d'identifier les problèmes, de les analyser et de mettre en place un certain nombre de techniques pour les prévenir ou y trouver des solutions […]. » (entretien n°8)

La police de sécurité du quotidien a aussi été investie comme un moyen pour renforcer les effectifs sur les zones les plus sensibles. Derrière cette réforme, c'est aussi « une politique RH », affirme un colonel, « mais est-ce la bonne méthode ? ». Pour le moment et à notre connaissance, la police prédictive et la mise en œuvre de la PSQ n'ont pas fait l'objet d'une réflexion portant plus spécifiquement sur leurs apports mutuels.

Aux États-Unis, la police prédictive a, aussi, dû affronter les critiques. En outre, dans le contexte actuel, les méthodes des polices américaines ont vivement agité le débat public suite aux décès de plusieurs personnes, désarmées et principalement afro-américaines, tuées par des policiers dans l'exercice de leur fonction. Dans ce contexte, les données policières ont été utilisées pour évaluer l'action discriminante de la police, et notamment en matière de prédiction. L'exemple le plus connu est celui de la Rand Corporation, think thank qui s'est emparé des données d'un logiciel de la police de Chicago utilisé pour prévenir la criminalité en orientant les personnes les plus vulnérables vers des programmes sociaux. En 2013, la publication de ces travaux conclut notamment que le logiciel renforcerait les pratiques et les stratégies d'intervention des policiers sur le terrain, en ciblant en priorité les plus pauvres et les minorités[51]. Dans le monde académique, il y a un consensus critique sur les biais discriminants des données et des algorithmes de la police prédictive : « En assimilant les lieux à la criminalité, on amplifie les problèmes de maintien de l'ordre. […] De nombreuses polices ont essayé de cibler les quartiers à forte criminalité. Mais cela implique souvent, des contrôles, des arrestations et des interrogations injustifiées (et inconstitutionnelles) des membres de la communauté ».[52]

Bilel Benbouzid remarque ainsi que pour les développeurs et les fournisseurs de logiciels de police prédictive, ces critiques sont l'occasion de faire évoluer leurs machines et d'intégrer cette problématique des biais dans la conception des programmes. C'est le cas, notamment, de Predpol qui se saisit du sujet dans l'optique de corriger son algorithme, partant du principe, comme le souligne le chercheur que « la police prédictive produit une activité ni plus ni moins plus discriminante que les pratiques courantes des patrouilles »[53]. Néanmoins, la firme semble ne pas renoncer à l'idée de pouvoir « mesurer, gérer et corriger les biais » par le calcul et dans son algorithme. En d'autres termes, elle cherche à répondre à un enjeu de justice sociale en rationalisant, par des techniques mathématiques, les préjudices sociaux que peuvent entraîner les contrôles de police. « Prédire le crime, c'est intégrer des règles d'action dans le paramétrage des machines, plaçant dans le calcul la clé de l'harmonie sociale » [54].

---

[51] Perry W.L., McInnis B., Price C C., Smith S C., Hollywood J S., *Predictive policing, the role of crime forecasting in law enforcement operations*, 2013.

[52] Shapiro A., « Reform predictive policing », 2017 : « Equating locations with ciminality amplifies problematic policing patterns. […] Many forces have tried 'hot-spot policing' - targeting patrols at high-crime neighbourhoods. But this often involves unwarranted (and unconstitutional) stopping, searching and questioning of community members ».

[53] Benbouzid B., « Quand prédire, c'est gérer. La police prédictive aux États-Unis », 2018.

[54] *Ibid*.

2.3.3 La gouvernance de la police algorithmique

La révolution numérique est aussi présentée comme « une révolution des pouvoirs » et non seulement une révolution technique. « À mesure de l'explosion du nombre de données généré par la numérisation de nos sociétés et du développement de procédés algorithmiques permettant de les trier, de les agréger et de les représenter […], les outils statistiques deviennent une technique de gouvernement ».[55]

En outre, depuis plusieurs décennies les acteurs privés accompagnent les politiques de sécurité et de prévention de la délinquance (diagnostics et conseils en sûreté, vidéosurveillance, agents de sécurité privés, etc.), et les technologies de sécurité et de contrôle constituent d'ailleurs un filon lucratif pour ce secteur. La police prédictive est une nouvelle opportunité pour eux. En France, les acteurs publics semblent partagés quant à la place à accorder aux entreprises privées. Culturellement, les forces de l'ordre (gendarmerie et police nationales) tendent à considérer que la sensibilité de leurs données implique de développer des outils internes, assurant des garanties tant pour l'institution que pour les citoyens. Les acteurs privés se tournent alors du côté des acteurs locaux (et notamment des collectivités territoriales), pour qui la police prédictive et, plus largement, l'ensemble des dispositifs dits « intelligents » (sous-couverts d'être innovants) représentent une réponse à la demande sociale de sécurité. Certains élus sont particulièrement soucieux de mettre en avant l'ensemble des actions qu'ils entreprennent en la matière (Cf. les villes de Marseille et de Nice développées *supra*).

Pourtant, le recours à des algorithmes produit par des entreprises privées soulève un certain nombre d'enjeux, déterminants dans la forme que prendront les services et les politiques publiques de sécurité :

• La compréhension des algorithmes, les choix opérés au moment de leur conception, ne sont pas à la portée de tous. Il s'agit donc de les rendre plus transparents pour qu'une lecture sociale de l'algorithme soit possible, et pour assurer l'évaluation des politiques publiques qui en découle.

• Quand un service public est gouverné par des algorithmes privés, est-ce toujours un service public ? Actuellement, les services publics de sécurité sont régulièrement concurrencés par des acteurs privés, qui les menacent parfois d'obsolescence. Pour garantir son unicité, la police prédictive doit (ré)affirmer la nécessité de bâtir des services publics de sécurité garants de l'égalité entre les citoyens et les territoires.

[55] Thieulin B., « Gouverner à l'heure de la révolution des pouvoirs », 2018.

Conclusion

En France, la police prédictive telle qu'elle se développe est assez éloignée des images fantasmées qui lui sont souvent associées. D'ailleurs, la référence à *Minority report*, perd tout son sens lorsqu'on s'intéresse concrètement à ce qui est élaboré. La police prédictive apparaît dans un contexte où le cadre juridique autour des données à caractère personnel se voit renforcé. Elle ne peut donc pas concerner les individus, il ne s'agit pas de savoir qui va commettre le prochain délit. Elle cible les zones géographiques sensibles, où certains types de faits sont plus susceptibles de se produire à l'avenir. En parallèle, les forces de sécurité doivent répondre à un double enjeu, l'exploitation informationnelle des données et l'optimisation des ressources humaines rapportée à la mesure de la délinquance. Les *big data* et les technologies de l'information sont mobilisés en ce sens. Mais pour l'heure, loin des représentations dominantes, ces outils émergents ne semblent pas aboutir à un réel changement de paradigme des forces de sécurité.

À ce stade, nombreux sont les acteurs (publics et privés) à montrer un intérêt croissant pour l'usage de l'intelligence artificielle dans la gestion des enjeux de sécurité publique. Les démarches se multiplient et font l'objet d'annonce, sans pour autant que les dispositifs soient à ce jour complètement aboutis. La gendarmerie nationale figure comme pionnière, en lançant une plateforme d'analyse décisionnelle officiellement développée pour prédire certains faits de délinquance. Pour produire ses prédictions dans l'espace et dans le temps, la plateforme s'appuie principalement sur les données informatisées des faits de délinquance sur les huit dernières années. Elle est, cependant, éloignée des applications prédictives embarquées par les agents sur le terrain, permettant d'orienter les patrouilles en temps réel. Elle est surtout employée par la hiérarchie et donne « un point de vue statistique » sur la délinquance par types de faits et par département. Elle propose une projection statistique concernant certains délits, et une carte de chaleur interactive correspondant au « volet plus opérationnel » de l'outil. C'est cet onglet qui semble d'ailleurs le plus apprécié par les gendarmes. Le bilan qu'ils en tirent est assez contrasté et varie d'un agent à l'autre. Ce n'est pas tant l'ergonomie de la plateforme qui est critiquée, mais plutôt les prédictions qui manqueraient de précisions (distinction horaire, caractéristiques du bâti, facteur météorologique, etc.). Le recueil de ces quelques éléments de bilan permet de constater que les gendarmes vont y puiser occasionnellement les informations qu'ils jugent intéressantes. La plateforme n'a, à ce stade, que peu d'incidence sur le positionnement des gendarmes et leurs stratégies spatiales de contrôle des populations. Néanmoins, elle revêt davantage un aspect managérial. Elle les alimente dans leur réflexion concernant notamment l'adéquation des ressources humaines par rapport à l'ampleur de la délinquance « objectivée » par la machine. Et en cela, elle participe à des enjeux d'optimisation des patrouilles de gendarmes, qui doivent régulièrement répondre de leur efficacité.

Cependant, la plateforme a aussi su créer des attentes. Les gendarmes rencontrés pour cette étude se disent, dans l'ensemble, séduits à l'idée d'utiliser dorénavant ce type d'outils. Bien que les logiciels prédictifs américains soient régulièrement décriés (par la presse comme par les institutions policières en France), les aspirations des gendarmes se rapprochent de ce qui est développé outre-atlantique. Mieux gérer les patrouilles et les interventions, calibrer la réponse face à un phénomène de délinquance, optimiser le temps passé sur un secteur, sont autant de préoccupations sur lesquelles les outils prédictifs sont attendus.

Sur le marché de la sécurité et du numérique, le secteur privé propose des innovations qui bousculent les limites du cadre légal, moins soucieux d'afficher des réserves ou des craintes à l'égard de ces outils innovants. La start-up « Two-i » qui propose un logiciel de détection des émotions pour prédire et anticiper les comportements déviants des passagers du tramway à Nice en est une illustration. Au-delà des enjeux juridiques, c'est une question éthique que pose le développement de l'intelligence artificielle dans le domaine de la sécurité publique. Plus largement, la police prédictive soulève un ensemble de questions qui aurait tout intérêt à être débattu publiquement :

- La nécessité de mener une réflexion collective. Au-delà du seul effet d'annonce, que peut-on attendre de la police prédictive ? Quels sont ses principaux apports ? Quel renseignement doit-elle fournir ? Pour quel type d'usages ? Il faut pouvoir définir son intérêt pour les administrations policières et pour le service public auquel elle doit contribuer. La police prédictive doit-elle transformer l'exercice du maintien de l'ordre, doit-elle redéfinir les missions des agents sur le terrain ? Dans ce cadre, police et gendarmerie ne peuvent fonctionner en silo et doivent participer ensemble à cette réflexion incluant les autres acteurs de la prévention et de la sécurité et notamment les collectivités territoriales qui, comme on l'a vu, s'intéressent au sujet.

- La police prédictive ne peut se réduire à un instrument de gestion des institutions policières. Le volet managérial se résume souvent à l'examen, au niveau local, des ressources humaines face à la mesure de la délinquance. La police prédictive répond à une volonté de rationalisation des services publics de sécurité. Cependant, elle ne saurait être qu'une évaluation comptable de l'action de la police. Elle doit aussi permettre une réflexion plus « qualitative » du service public de sécurité rendu. Le chantier de la donnée doit permettre de mettre en perspective ce qui est développé au nom du prédictif. Les données ne peuvent servir qu'à « objectiver » les phénomènes de délinquance, elles sont à considérer dans toute leur complexité, prenant en compte l'ensemble des biais liés aux représentations et aux pratiques des acteurs impliqués dans leur production.

- La multiplication des dispositifs intelligents et prédictifs dans la surveillance et le contrôle des espaces urbains nécessite une réflexion quant à la concordance entre le besoin de sécurité publique et l'offre de surveillance. De plus en plus de collectivités territoriales sont séduites par des plateformes numériques permettant d'optimiser l'ensemble de la gestion des espaces publics (éclairage public, stationnement, manifestation, travaux, etc.), y compris sur le plan de la tranquillité et de la sécurité. Le risque, tel que l'identifie les associations de défenses des libertés individuelles, est celui d'une surenchère de dispositifs de contrôle et un renforcement des logiques de surveillance massive. En outre, l'usager et l'habitant sont les grands absents du développement de ces dispositifs technologiques, quelle place leur accorder dans l'essor de la *safe city* ?

BIBLIOGRAPHIE

ABITEBOUL S., DOWEK G., *Le temps des algorithmes*, Paris, Le Pommier, 2017.

ALLIX G., « Comment des villes "hyper connectées" contrôlent l'espace public », *Le Monde*, publié le 19.12.2018

BENBOUZID B., « De la prévention situationnelle au *predictive policing*. Sociologie d'une controverse ignorée », *Champ pénal/Penal field* [En ligne], Vol. XII/2015, mis en ligne le 23 mars 2015, consulté le 10 juin 2015.
URL: http://champpenal.revues.org/9050

BENBOUZID B., « À qui profite le crime ? Le marché de la prédiction du crime aux États-Unis », *La Vie des idées*, 13 septembre 2016.
URL: http://www.laviedesidees.fr/A-qui-prodite-le-crime.html

BENBOUZID B., « Des crimes et des séismes. La police prédictive entre science, technique et divination », *Réseaux,* 2017/6 (n°206), p.95-123.

BENBOUZID B., « À quoi les humains tiennent-ils lorsqu'ils délèguent du pouvoir aux machines ? La police prédictive aux États-Unis dans la science, l'administration et le droit », *Séminaire de Recherche du LaDHUL, La délégation cognitive aux machines,* 21/03/2018.

BENBOUZID B., « Quand prédire, c'est gérer. La police prédictive aux États-Unis », *Réseaux*, 2018/5 (n°211), p.221-256.

BESSON J-L., *Les cartes du crime*, Paris, Presses universitaires de France, 2004.

BON D., ROBERT P., ZAUBERMAN R., « La délinquance : entre statistiques de police et enquêtes de victimation », *Note Rapide,* n°538, IAU îdF, mars 2011.

CNIL, *La plateforme d'une ville, les données personnelles au cœur de la fabrique de la smart city*, Cahiers Innovation et prospective n°5, 2017.

CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une république numérique, décembre 2017.

DE MAILLARD J., *Polices comparées*, Issy-les-Moulineaux, Clefs politique, LGDJ, 2017.

GAUTHIER F., « Prédire les vols de voitures ? », *Revue de la gendarmerie nationale*, n°206, décembre 2017.
Ou sur le site d'Etalab, URL : https://agd.data.gouv.fr/2018/01/12/predire-les-vols-de-voitures/

GOSSELIN C., *Données numériques et gestion locale de la sécurité, production et usages de bases de données chez les acteurs locaux*, IAU îdF, février 2018.

HÉRARD P., « Surveillance : le réseau français "intelligent" d'identification par caméras arrive », *TV5 Monde*, mis en ligne le 09.06.2018.

JOBARD F., DE MAILLARD J., *Sociologie de la police, politiques, organisations, réformes*, Paris, Armand Colin, Collection U, 2015.

LA QUADRATURE DU NET, « La surveillance policière dopée aux *big data* arrive près de chez vous ! », 20 mars 2018 ; « La *smart city* policière se répand comme une traînée de poudre », 06 juillet 2018.

LE-BAS C., « Sous le capot de la police prédictive », *Courrier picard*, publié le 04.02.2018.

LEGROS C., « À Marseille, le *big data* au service de la sécurité dans la ville », *Le Monde*, publié le 08.12.2017.

NAKACHE D., « "Two-i", la biopolitique au pouvoir à Nice », *Médiapart*, publié le 09.01.2019.

PERROT P., « L'algorithme prédictif », in *Observatoire FIC.com, carrefour des réflexions sur la cybersécurité*, publié le 07/01/2016.
URL: https://observatoire-fic.com/lalgorithme-predictif/

PERROT P., « Disruption et révolution numérique : une nouvelle ère pour la sécurité », *Sécurité globale* 2017/3 (N°11), p. 81-88.

PERRY W L., MCINNIS B., PRICE C C., SMITH S C., HOLLYWOOD J S., *Predictive policing, the role of crime forecasting in law enforcement operations*, Rand Corporation, 2013.
Lien URL: https://www.rand.org/pubs/research_reports/RR233.html

PIQUARD A., TUAL M., « L'éthique dans l'intelligence artificielle, année zéro », *Le Monde*, 05/10/2018.

ROUVROY A., BERNS T., « Le nouveau pouvoir statistique ou quand le contrôle s'exerce sur un réel normé, docile et sans évènement car constitué de corps "numériques" …», *Multitudes*, 2010/1 n°40, p.88-103.

SHAPIRO A., « Reform predictive policing », *Nature News*, vol. 541, p.458-460.

THIEULIN B., « Gouverner à l'heure de la révolution des pouvoirs », *Pouvoirs*, n°164, 2018.

VILLANI C., *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*. Mission confiée par le Premier Ministre Edouard Philippe, mars 2018.

ANNEXES

Annexe 1 : Liste des entretiens

N°	Organisme	Fonction	Date
1	**Gendarmerie nationale**	Chef d'escadron, Chargé de projets / chef du département études, École des officiers de la gendarmerie nationale	28/05/2018
2		Chef de département, Service Central de Renseignement Criminel, Division du Renseignement, Département des Sciences de la Donnée	14/06/2018
3		Colonel, Commandant de groupement (Nord de la France)	18/06/2018
4		Colonel, Commandant de groupement (Nord de la France)	19/06/2018
5		Colonel, Commandant de groupement (Sud de la France)	03/08/2018
6		Colonel, Commandant de groupement (Est de la France)	14/09/2018
7		Sous-directeur, service des technologies et des systèmes d'information de la sécurité intérieure, ST(SI)^2	20/09/2018
8	**ONDRP** Observatoire national de la délinquance et des réponses pénales	Chargé d'études géostatistiques	29/05/2018
9	**Mission Etalab**	Data Scientist	01/06/2018
10	**CNIL** Commission nationale de l'informatique et des libertés	Juriste Services des affaires régaliennes et des collectivités territoriales	22/06/2018
		Chargé d'études prospectives Pôle innovation, études et prospectives	22/06/2018
11	**Université Marne-la-Vallée**	Maître de conférences, chercheur au laboratoire interdisciplinaire sciences innovations sociétés (LISIS).	03/07/2018

LEXIQUE

***Algorithme**
Description d'une suite finie et non ambigüe d'étapes ou d'instructions permettant d'obtenir un résultat à partir d'éléments fournis en entrée.

Apprentissage automatique ou *Machine learning
Branche de l'intelligence artificielle, fondée sur des méthodes d'apprentissage et d'acquisition automatique de nouvelles connaissances par les ordinateurs, qui permet de les faire agir sans qu'ils aient à être explicitement programmés.

****Big data***
Désigne la conjonction entre d'une part, d'immenses volumes de données devenus difficilement traitables à l'heure du numérique et, d'autre part, les nouvelles techniques permettant de traiter ces données, voire d'en tirer par le repérage de corrélations des informations inattendues.

****Biométrie**
Regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.).

***Intelligence artificielle**
Théories et techniques « consistant à faire faire à des machines ce que l'homme ferait moyennant une certaine intelligence » (Marvin Minsky). On distingue IA faible (IA capable de simuler l'intelligence humaine pour une tâche bien déterminée) et IA forte (IA générique et autonome qui pourrait appliquer ses capacités à n'importe quel problème, répliquant en cela une caractéristique forte de l'intelligence humaine, soit une forme de « conscience » de la machine).

****Reconnaissance faciale**
Une technique qui permet à partir des traits de visage :
- d'authentifier une personne : c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès), ou
- d'identifier une personne : c'est-à-dire, de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données.

*Cf. définitions in CNIL, *Comment permettre à l'homme de garder la main ?, les enjeux éthiques des algorithmes et de l'intelligence artificielle*, décembre 2017.

**Cf. définitions tirées sur site internet de la CNIL : https://www.cnil.fr/fr

L'INSTITUT D'AMÉNAGEMENT ET D'URBANISME DE LA RÉGION D'ÎLE-DE-FRANCE
EST UNE ASSOCIATION LOI DE 1901.

15, RUE FALGUIÈRE - 75740 PARIS CEDEX 15 - TÉL. : 01 77 49 77 49