

# CAHIERS DE LA SÉCURITÉ ET DE LA JUSTICE

Revue de l'Institut national des hautes études de la sécurité et de la justice \_\_\_\_\_ n°47

## Sécurité totale *Le meilleur des mondes numériques ?*



### Dossier

Les usages des algorithmes. L'estimation de la récidive dans la justice pénale américaine  
Angèle CHRISTIN

Avons-nous le choix d'utiliser l'IA en temps de guerre ?  
Marie-des-Neiges RUFFO de CALABRE

L'impact de l'intelligence artificielle dans la conduite de l'enquête judiciaire  
Général Patrick TOURON

### Sécurité intérieure

La clandestinité politique : balises pour un objet d'études émergent  
Grégoire LE QUANG

### International

Côte d'Ivoire. Le phénomène des délinquants violents dits « microbes » et la réponse de la police et des acteurs informels de la sécurité (AIS)  
Henry BOAH YEBOUET

Directrice de la publication :

**Valérie MALDONADO**

Rédacteur en chef :

**Manuel PALACIO**

Comité de rédaction :

**AMADIEU Jean-Baptiste**, Agrégé de lettres, chargé de recherches au CNRS

**BERLIÈRE Jean-Marc**, Professeur émérite d'histoire contemporaine, Université de Bourgogne

**BERTHELET Pierre**, Chercheur au centre de documentation et de recherches européennes (CRDE), Université de Pau

**BOUDJAABA FABRICE**, Directeur scientifique adjoint au CNRS, Institut des Sciences Humaines et Sociales (InSHS)

**COOLS Marc**, Professeur en criminologie, Université libre de Bruxelles, Université de Gand

**DALLEST Jacques**, Procureur Général près la cour d'appel de Grenoble, professeur associé à Sciences Po Grenoble, doyen des enseignements du pôle "communication judiciaire" à l'École Nationale de la Magistrature

**DE BEAUFORT Vivianne**, Professeure à l'Essec, co-directeur du CEDE

**DE LA ROBERTIE Catherine**, Préfète de l'Aveyron, Professeure des universités, Paris I, Directrice du Master2 Stratégie Internationale & Intelligence Économique

**DE MAILLARD Jacques**, Professeur de Science politique, Université de Versailles Saint-Quentin

**DIAZ Charles**, Contrôleur Général, Inspection Générale de la Police Nationale

**DIEU François**, Professeur de sociologie, Université Toulouse 1 Capitole

**EVANS Martine**, Professeur de droit pénal et de criminologie, Université de Reims

**HERNU Patrice**, Administrateur INSEE

**LATOUREX Xavier**, Professeur de droit, Doyen de la Faculté de droit et science politique, Université Côte d'Azur

**LOUBET DEL BAYLE Jean-Louis**, Professeur émérite de Science politique, Université de Toulouse 1, Capitole

**MOCILNIKAR Antoine-Tristan**, Ingénieur général des Mines. Service de défense, de sécurité et d'intelligence économique. Ministère de la transition écologique et solidaire

**NAZAT Dominique**, Docteur en Sciences odontologiques, expert au Groupe de travail permanent pour la révision des normes d'identification du DVI d'Interpol

**PARDINI Gérard**, Sous-préfet

**PICARD Jean-Marc**, Enseignant-chercheur à l'Université de Technologie de Compiègne

**RENAUDIE Olivier**, Professeur de droit public à l'Université de Lorraine, Nancy

**ROCHE Jean-Jacques**, Directeur de la formation, des études et de la recherche de l'Institut des hautes études de la défense nationale (IHEDN)

**SAURON Jean-Luc**, Professeur de droit à l'Université Paris Dauphine

**TEYSSIER Arnaud**, Inspecteur Général de l'Administration, Professeur Associé à l'Université Paris I

**VALLAR Christian**, Avocat en droit public, professeur des universités, Université Côte d'Azur

**WARUSFEL Bertrand**, Professeur agrégé des facultés de droit, Université Paris 8

**Responsables de la communication :** Simon NATAF, Clément TENDIL

**Conception graphique :** Laetitia BÉGOT

**Vente en librairie et par correspondance** - La Direction de l'information légale et administrative (DILA),

[www.ladocumentationfrancaise.fr](http://www.ladocumentationfrancaise.fr)

**Tarifs :** Prix de vente au numéro : 23,10 € - Abonnement France (4 numéros) :

70,20 € - Abonnement Europe (4 numéros) : 75,30 €

**Abonnement DOM-TOM-CTOM :** 75,30 € (HT, avion éco) - Abonnement hors Europe (HT, avion éco) : 79,40 €

**Impression :** DILA

**Tirage :** 1 000 exemplaires



© Direction de l'information légale et administrative, Paris, 2020

**Conditions de publication :** Les Cahiers de la sécurité et de la justice publient des articles, des comptes rendus de colloques ou de séminaires et des notes bibliographiques relatifs aux différents aspects nationaux et comparés de la sécurité et de ses acteurs. Les offres de contribution sont à proposer à la rédaction pour évaluation. Les manuscrits soumis ne sont pas retournés à leurs auteurs. Toute correspondance est à adresser à l'INHESJ à la rédaction de la revue.

Tél. : +33 (0)1 76 64 89 00 - Fax : +33 (0)1 76 64 89 31

[publications@inhesj.fr](mailto:publications@inhesj.fr) - [www.cahiersdelasecuriteetdelajustice.fr](http://www.cahiersdelasecuriteetdelajustice.fr)

## Sommaire

3 Éditorial - Valérie MALDONADO

## Dossier

- 4 Protection et surveillance augmentées Le nouveau paradigme sécurité et liberté  
Manuel PALACIO
- 13 Les usages des algorithmes. L'estimation de la récidive dans la justice pénale américaine  
Angèle CHRISTIN
- 19 Avons-nous le choix d'utiliser l'IA en temps de guerre ?  
Marie-des-Neiges RUFFO de CALABRE
- 31 L'intelligence artificielle : vers une nouvelle grammaire internationale ?  
Charles THIBOUT
- 39 Quelques éléments d'une géopolitique du Net...  
Gaetan GORCE
- 43 Quel cadre juridique pour les outils d'intelligence artificielle dans le domaine du renseignement ?  
Floran VADILLO
- 53 Algorithmes prédictifs pour la police et la justice : nouveaux oracles ou simples outils de gestion du risque ?  
Léo AMSELLEM, Vincent BERTHET
- 62 L'impact de l'intelligence artificielle dans la conduite de l'enquête judiciaire  
Général Patrick TOURON
- 71 L'intelligence artificielle au service des politiques publiques de prévention  
Jérôme LAGASSE
- 80 Trois empires et un garde-manger  
Pierre BELLANGER
- 86 Intelligence artificielle et demandes de visas au Quai d'Orsay  
Olivier POUDADE
- 89 La cybersécurité dans le rétroviseur  
*L'émergence d'une politique européenne (1997-2017)*  
Pierre BERTHELET
- 100 Intelligence artificielle et Big Data : du risque cyber à l'opportunité pour les services de sécurité et de défense étatiques  
Amandine LÉVÉQUE





31

- 109** La causalité est morte : vive la corrélation !  
*Vers une criminologie du lieu augmentée par l'intelligence artificielle*  
 Jean-Luc BESSON
- 126** Risk terrain modeling and the study of the physical determinants of criminal behavior  
 Alejandro GIMÉNEZ-SANTANA,  
 Leslie W. KENNEDY, Joel M. CAPLAN

### Sécurité intérieure

- 135** La clandestinité politique : balises pour un objet d'études émergent  
 Grégoire LE QUANG
- 144** À quoi sert le terrorisme ? *Les effets du terrorisme islamiste sur les musulmans de France (2015-2019)*  
 Manuel SAN PEDRO
- 155** Approche du traitement des traces d'outils dans la problématique des cambriolages par les systèmes d'information géographiques (SIG)  
 Grégory BRICHE

### En débats

- 162** La police et les contradictions de l'individualisme post-moderne  
 Jean-Louis LOUBET DEL BAYLE

### International

- 168** Passage à l'acte. État de la recherche internationale  
 Jacques DUBUCS
- 183** Côte d'Ivoire. Le phénomène des délinquants violents dits « microbes » et la réponse de la police et des acteurs informels de la sécurité (AIS)  
 Henry BOAH YEBOUET
- 193** Relations police-population et *community policing* : le paradoxe sud-coréen  
 Éric MEYNARD



19



100



## Éditorial

L'INHESJ a pour principale mission de produire et rassembler les éléments de connaissance sur la criminalité comme sur la lutte contre la criminalité et, au-delà, sur l'ensemble des phénomènes qui constituent une menace ou un risque pour les populations. En ce sens, les recherches et les études menées ont toujours eu vocation à saisir et analyser les thématiques émergentes, les phénomènes dont l'apparition marque le point de départ de transformations significatives et durables dans les sociétés modernes.

De ce point de vue, s'il est une question porteuse des mutations les plus fortes pour les décennies à venir, c'est bien le développement des nouvelles technologies qualifiées à partir de l'adjectif « numérique ». Ce développement tant par ce qu'il produit comme nouveautés que par son ampleur et sa vitesse de propagation, peut être présenté comme le grand bouleversement du XXI<sup>e</sup> siècle. Après la révolution industrielle de la fin du XIX<sup>e</sup> siècle, la révolution scientifique et technique du XX<sup>e</sup>, nous assistons selon de nombreux penseurs à rien moins qu'une étape décisive de l'évolution de l'humanité.

Comme la société elle-même, la sécurité est une notion en perpétuelle évolution. L'Institut en a pris acte et s'est renouvelé en investissant de nouveaux domaines, au-delà de la dimension « *criminalité intérieure et ordre public* », porteurs de préoccupations « sociétales » plus larges. Il ne s'agit plus de travailler exclusivement sur la délinquance classique, mais de prendre en compte l'existence de l'ensemble des menaces qui pèsent sur les sociétés modernes et engendre une demande de protection élargie de la part de leur population. La demande de sécurité s'est en effet étendue à des domaines de la vie quotidienne comme la santé, l'éducation, le monde de l'entreprise ou encore l'environnement. La mission initiale qui était celle de l'Institut a ainsi été redéfinie de manière pluridimensionnelle autour de la notion de *sécurité globale* et, dans le même mouvement, celui-ci s'est ouvert à la dimension judiciaire des actions à mener. Cette nouvelle dimension a permis d'acter que le

cadre indispensable de toute politique de sécurité, qu'il s'agisse de la prévention ou de la répression, est celui de la Justice comme garante de l'État de droit et des libertés attachées à sa forme démocratique.

Durant les trente dernières années, s'est développée une nouvelle demande sociale généralisée de sécurité qui a rencontré de nouveaux moyens de réponse dans les évolutions technologiques et, plus largement, dans la poursuite du développement de la révolution scientifique et technique. De nouveaux outils surgissent en permanence autour du développement de l'intelligence artificielle qui renforcent les capacités de prévenir toutes les formes de risques et de menaces (robotique, algorithmes prédictifs, cyber-sécurité, etc). Mais plus la demande de sécurité se banalise et trouve de réponses efficaces grâce à la révolution numérique et plus se dessine un nouveau cadre politique et sociétal où l'accroissement de la protection des citoyens engendre un accroissement du contrôle de leur vie par des entités toujours plus puissantes. Dans le futur, cette évolution de la sécurité posera en des termes nouveaux la question des libertés.

Vouloir penser la sécurité globale, être à l'écoute de l'émergence de phénomènes qui constituent des menaces et des risques potentiels, a conduit l'Institut à ouvrir *obligatoirement* le « dossier Intelligence artificielle » et de regarder ce qui est en train de changer aujourd'hui et ce qu'il est possible de prévoir dans un avenir dont certains contours se dessinent déjà sous nos yeux.

C'est ce dossier que ce numéro des *Cahiers de la sécurité et de la justice* vous présente aujourd'hui avec des articles qui portent sur des réalisations ou des projets en cours, mais aussi en élargissant le champ de l'analyse au-delà des seules pratiques policières et judiciaires à des thèmes comme le droit, la géopolitique ou encore, plus profondément, une interrogation philosophique sur ce que pourrait être une société de protection absolue des hommes par les machines.

Valérie MALDONADO  
Directrice de l'INHESJ

# Protection et surveillance augmentées

## *Le nouveau paradigme sécurité et liberté*

Manuel PALACIO

«*Do Androids Dream of Electric Sheep ?*»  
Philip K. Dick

Le monde moderne connaît une accélération sans précédent des mutations liées aux découvertes scientifiques et aux innovations techniques. Il a fallu plus de 4 000 ans pour passer de l'invention de la roue à l'invention de la machine à vapeur, et moins d'un siècle pour passer de celle-ci à l'invention du moteur à explosion. Un millénaire et demi sépare Ptolémée de Newton et moins de trois siècles séparent celui-ci d'Einstein. Le XIX<sup>e</sup> siècle est le siècle charnière, celui des basculements. Un bouleversement majeur se produit, l'avènement de la révolution industrielle rendue possible par de nouveaux savoirs qui génèrent de nouveaux outils. Ce phénomène change radicalement les structures économiques, sociales et politiques des sociétés où il se développe ainsi que les modes de vie de leurs citoyens. Les nouveaux outils, les nouveaux modes de production, les nouveaux produits impactent tous les domaines de la vie quotidienne, santé, transports, alimentation, habitat... Siècle de transition, le XX<sup>e</sup> siècle est également un siècle d'accélération. Soixante-dix-sept années seulement séparent la création de la première voiture à essence du voyage du premier homme

sur la lune. La découverte de la pénicilline en 1928 sauve la vie de millions d'êtres humains et le développement des antibiotiques permet l'éradication d'épidémies infectieuses séculaires. Cette énumération pourrait être poursuivie avec d'innombrables dates et exemples.

## Révolutions

Le XXI<sup>e</sup> siècle est celui de la révolution numérique. Le terme est d'ailleurs problématique tant il peine (au-delà de la métaphore) à cerner une réalité d'une extrême complexité. Si les décennies précédentes sont celles des machines pensées et réalisées par les cerveaux et le travail humains, la nouvelle révolution est celle des réseaux, de la vitesse et de l'étendue des communications, de l'appréhension du réel (matériel ou virtuel) à travers les données, les fameuses *data* ! Pas un domaine de la vie quotidienne, des organisations sociales, de l'économie, de la géopolitique, qui ne soit impacté par cette révolution. Celle-ci a, dans une première étape, été définie et pensée à partir de l'essor des nouvelles technologies de communication, Internet et téléphonie mobile, qui ont mis les hommes en réseau, individus et

### Manuel PALACIO



Rédacteur en chef des Cahiers de la sécurité et de la justice, Manuel Palacio est conseiller

du directeur de l'INHESJ sur les questions de prévention de la délinquance. Issu du corps des directeurs de la Protection judiciaire de la jeunesse, il est l'auteur de *La justice des enfants perdus*, La Découverte, Paris, 2006.



populations, au sein de leurs communautés de vie et de travail, mais aussi dans des échanges à l'échelle mondiale. De ce point de vue, la révolution numérique a poursuivi le mouvement de la mondialisation initié aux siècles précédents et qui a conduit à un accroissement substantiel de la circulation des personnes, des objets, des capitaux, des informations et des connaissances. La deuxième étape qui constitue le « moment actuel » de cette révolution numérique, est celle de l'essor de l'intelligence artificielle (IA).

Le terme n'a pas encore trouvé de définition à même de cerner dans toute sa complexité le phénomène qu'elle désigne, mais il s'est répandu dans l'usage courant, bien au-delà des milieux scientifiques, pour désigner un ensemble de réalités hétérogènes et souvent mélangées dans une confusion quasi mythologique et alimentée par un marketing efficace. Il est utilisé pour parler aussi bien, parmi tant d'autres exemples, de programmes de géolocalisation, de diagnostic médical ou d'aide à la conduite automobile que d'un futur où les machines seront capables de penser comme l'être humain. Dans sa version prophétique, l'IA ne désignerait rien moins que la capacité de programmes informatiques à se substituer aux

compétences humaines en matière de création et d'action. Dans sa réalité et son actualité, elle désigne surtout l'usage de programmes permettant à des machines de réaliser de manière autonome et plus rapidement et plus efficacement que les humains des tâches bien précises qui leur étaient préalablement dévolues. L'utilisation de la terminologie de l'IA (et de ses multiples extensions et manifestations) doit être l'objet d'une rigueur extrême rendue difficile par l'étendue de ses domaines d'existence et l'ampleur des possibles qu'elle ouvre et des questions qu'elle soulève. L'IA est avant tout une métaphore qui permet à la fois la représentation d'une nouvelle étape dans la révolution scientifique et technique et la projection d'une possible révolution anthropologique aujourd'hui en gestation.

Parmi tout ce qui fait débat dans cet essor (réel et fantasmé) de l'IA, il y a, d'un côté, la promesse d'un avenir meilleur fait, au minimum, d'améliorations conséquentes de la vie quotidienne et, au maximum, de l'avènement d'un nouvel homme augmenté et, de l'autre, la peur d'une disparition de l'humanité face à sa dernière et majeure création qui l'aurait rendue définitivement obsolète. Pour rentrer sérieusement dans ce débat, il y a au préalable deux questions à poser distinctement.

## Nouveaux outils, vieux débat

La première question se pose dès lors que l'on prend en compte la réalité des usages concrets que l'IA a créés et permis, à savoir le développement substantiel d'un certain nombre d'outils qui augmentent et améliorent la capacité d'action humaine dans les domaines les plus variés. Qu'ils soient générés par des programmes informatiques n'en fait pas moins des outils et il ne s'agit alors que d'une progression quantitative et qualitative du processus d'automatisation initié au cours de la révolution industrielle. L'accroissement de la puissance de calcul à l'origine des nouveaux algorithmes augmente en proportion la capacité des nouvelles machines à assumer des tâches de plus en plus complexes et « délivrer » les humains de leur exécution. Le progrès est avéré mais la promesse de délivrance ouvre des interrogations, sinon des inquiétudes, sur l'avenir qu'un tel progrès pourrait annoncer.

Nous sommes dès lors dans le débat philosophique et politique traditionnel sur « la technique », mais posé dans un contexte nouveau et il s'agit seulement de le reprendre là où l'avaient laissé Heidegger et après lui, parmi d'autres, Jacques Ellul.

Pour le premier, la technique ne se réduit pas à sa signification première forgée avant l'avènement de la science, c'est-à-dire à la conception des moyens adéquats pour l'exécution d'une tâche qui aboutit à la production d'un objet ou service. Pour Heidegger, la science a changé la donne dès lors qu'en parvenant à mesurer le réel, elle en vient à l'objectiver totalement. La science moderne n'est pas uniquement la connaissance du réel, elle en est un formatage qui conduit à le soumettre. La nature devient un objet à maîtriser dans l'absolu et l'homme lui-même n'est plus qu'un élément calculable dans ce processus de maîtrise, voire de soumission.

Pour le deuxième, la technique est un système en soi qui s'autonomise et tend à réaliser ses propres fins au détriment de celles des hommes, ceux-ci devenant non pas les maîtres mais les objets dudit système. L'efficacité qui est la condition première de la technique dans la production des objets devient une fin en soi. Jacques Ellul s'inscrit en l'approfondissant dans un courant de pensée de critique de la technique qui dénonce le fait que le développement de celle-ci annihile toute autre finalité humaine que celle du profit incessamment renouvelé, ce qui présente le double danger de restreindre la dimension de la liberté humaine et de réduire la nature à un pur objet manufacturable, au risque de l'épuiser définitivement.

Si l'on estime que la révolution numérique ne fait qu'amener des outils nouveaux plus performants, elle relève alors de la même grille de pensée forgée précédemment dans le débat sur les rapports de l'homme à la technique. Objets connectés, programmes d'aide à la décision et au diagnostic, algorithmes de prévision améliorent significativement les conditions de vie au sein des sociétés humaines, mais s'inscrivent dans le prolongement des outils forgés dans la période précédente suscitant par conséquent le même type d'interrogations. Le saut réalisé correspond seulement à un degré supérieur dans l'efficacité des outils. Le risque qui peut être pointé est alors celui du rétrécissement de l'aire de la responsabilité humaine. Jusqu'à quel point nous défaussons-nous de notre responsabilité, de notre faculté de création parce que nous transférons une grande part de celles-ci à des programmes plus efficaces que nous ? Jusqu'à quel point acceptons-nous de limiter notre liberté en nous reposant sur des programmes parce qu'ils assurent efficacement notre protection et notre bien-être ? L'exemple de la voiture autonome est de ce point de vue tout à fait significatif. Les débats sur ce projet portent essentiellement soit sur des questions techniques (faisabilité et fiabilité), soit sur des questions morales autour de la responsabilité (qui prend la décision en cas d'accident inéluctable – question éthique – et qui est au final responsable – question juridique ?). Mais un questionnement plus global demeure au second plan qui porte sur ce que devient l'être humain dès lors qu'il se repose entièrement sur une machine sur laquelle il n'a plus, en tant qu'individu, aucune maîtrise. Il est alors le simple objet d'un service. Il n'est plus conducteur, il est transporté. Ce questionnement qui vaut ici pour le transport peut être étendu à d'autres innombrables dimensions de la vie quotidienne.

## Un au-delà de l'outil, un nouveau débat

La deuxième question se pose si l'on estime que la révolution numérique représente une étape nouvelle dans l'évolution de l'humanité et que nous nous trouvons en face d'une authentique rupture avec les périodes précédentes, une rupture anthropologique. Cette vision de la révolution numérique présuppose l'IA comme entité potentiellement substituable à l'humain. Elle n'est plus un simple outil au service de l'Homme à travers la traditionnelle automatisation des tâches humaines, mais une nouvelle réalité qui non seulement fait à la place de l'humain mais fait comme lui dans un saut qualitatif qui passe de l'exécution à la conception et la création.

Pour évaluer le degré de crédibilité de cette vision, l'enjeu de la définition de l'IA, de sa réalité dans son actualité, mais aussi de son devenir possible à l'échelle de quelques décennies, est essentiel mais difficile à tenir. Le problème réside déjà dans la multiplicité des définitions possibles de l'intelligence en tant qu'attribut humain et même de la simple connaissance du fonctionnement du cerveau humain. Siège de l'organisation de la perception, de sa traduction en représentations, de l'élaboration des décisions, bref, parmi tant d'autres fonctions, siège de la pensée, ce dernier est-il seulement un vaste système neuronal fondé sur des connexions et des combinatoires de données ? Dans cette hypothèse, l'IA serait alors un programme mathématique éminemment sophistiqué, construit sur le même modèle que le système neuronal et capable de réaliser les mêmes performances, bien au-delà de l'exécution de tâches partielles répétitives. Dans une version modeste, ce programme serait capable de reproduire des fonctions cognitives humaines. Dans une version ambitieuse, il serait capable de surpasser les performances humaines de par une plus grande puissance de calcul et donc de maniement d'un plus grand nombre de combinatoires.

Le débat n'est plus alors de savoir jusqu'à quel point l'usage de l'outil performant limite le champ de la créativité, de la responsabilité et, au final, de la liberté humaine, mais bien de savoir si le développement de l'outil est parvenu à modifier l'essence même de l'humain. Pour l'exprimer à travers les images aujourd'hui en vogue dans l'opinion commune, la question est de savoir si nous en sommes au stade de « l'homme augmenté » et, surtout, de savoir ce que ce terme recouvre. S'agit-il de l'homme aidé, de l'homme assisté par des techniques nouvelles sans cesse plus efficaces pour réaliser ce qu'il conçoit et projette ? Dans ce cas « l'homme augmenté » n'est rien d'autre qu'un homme mieux armé que ses prédécesseurs dans l'exécution de ses multiples tâches. S'agit-il plutôt d'un processus en cours annonçant l'hybridation entre l'homme et la machine ? Dans ce cas nous assistons à l'émergence d'une entité nouvelle ne marquant rien moins qu'une nouvelle ère de l'histoire de l'humanité !

Ces questions sont posées dans le cadre d'un débat dont les termes oscillent entre la parabole de *Deep Blue* battant le Grand Maître aux échecs et l'exemple du programme de reconnaissance faciale qui a besoin d'intégrer des dizaines de milliers de données (images) pour reconnaître un chat avec plus de 90 % de taux de réussite là où une ou deux images suffiront à un

Parmi les multiples définitions que l'on donne de l'IA, la plus simple est : « capacité des machines à prendre des décisions et à adopter des comportements attribués généralement à des humains ou à des animaux, mais avec un moindre niveau de performance ».

L'évolution technologique que nous connaissons depuis ces dix dernières années repose en grande partie sur le *machine learning*, à savoir, l'apprentissage automatique des machines.

Le *deep learning*, sous domaine du *machine learning*, s'est, quant à lui, révélé particulièrement efficace et gagne en notoriété depuis ces quatre dernières années, si bien que les médias y font systématiquement référence lorsqu'ils parlent d'IA. Toute une industrie s'est créée autour de cette technologie.

Pour construire une machine intelligente les principales méthodes sont les suivantes :

Il s'agit d'abord d'écrire des algorithmes qui se comportent de manière intelligente pour résoudre un problème particulier.

À ce stade les machines sont entraînées de manière totalement supervisée. Elles peuvent ainsi, par exemple, devenir un adversaire de taille dans une partie d'échecs. Nous retrouvons ces mêmes algorithmes dans les GPS ou Google Map pour planifier une trajectoire entre deux points. Mais, à ce stade, nous ne pouvons encore parler d'apprentissage.

Ensuite, le *machine learning* classique. Il nécessite une part importante de programmation directe (conception à la main) de manière à transformer le signal original (par exemple, une image) en un format traitable par le système d'apprentissage simple. Cela implique également de collecter de grandes bases de données qui sont étiquetées à la main et d'assigner à la machine une tâche bien définie (entrée/sortie). La partie apprentissage est encore relativement mineure. Le *machine learning* représente plus de 95 % des succès de l'IA. Il est utilisé pour la reconnaissance d'images, la classification de textes ou encore pour la traduction automatique, notamment par Facebook, Google, Microsoft, IBM et beaucoup de *start-up*.

Enfin, le *deep learning*, apprentissage profond ou par renforcement, repose sur l'utilisation de multiples couches d'unités de traitement de données composant un système. Il permet à ce dernier d'être entièrement entraînable (sans conception à la main) et d'apprendre de manière automatique.

Yann LECUN, Professeur à l'Université de New York, Directeur de Facebook AI Research (fair).

Défis n° 8, « L'entreprise à l'heure de l'intelligence artificielle. Entre promesses et nouveaux défis ».

<https://inhesj.fr/publications/defis/lentreprise-lheure-de-lintelligence-artificielle-entre-promesses-et-nouveaux>



enfant pour parvenir au même résultat sans le moindre pourcentage d'erreur. Sans trancher ici un tel débat (à supposer qu'il puisse être tranché), un retour au présent s'avère nécessaire qui est aussi un retour sur terre.

À strictement parler l'IA désigne aujourd'hui, d'une part, des programmes de traitement d'ensembles de données numériques dont le volume, la diversité des origines et la vitesse nécessaire à leur collecte et analyse sont au-delà de la capacité humaine de réalisation performante et, d'autre part, la possibilité pour ces programmes de tirer un certain nombre de leçons de leur propre processus d'exécution et d'intégrer une démarche d'apprentissage.

## L'IA dans le champ sécurité-justice

Quelles sont les manifestations et les conséquences de l'introduction de l'IA dans les secteurs en charge de la sécurité et de la justice ? Les domaines où les outils numériques commencent à trouver un début d'application sont aussi hétérogènes que les outils eux-mêmes. Il s'agit aujourd'hui, pour l'essentiel, de conception, d'expérimentation ou d'exécution de programmes qui facilitent l'action des institutions policières et judiciaires dans leurs missions traditionnelles comme l'enquête, le renseignement, la prévention, la détection, la police scientifique, etc. Globalement, ces outils permettent de réaliser des tâches existantes avec un taux de rapidité supérieur qui libère d'autant de l'énergie et du temps humain augmentant par là même l'efficacité et le potentiel d'action des acteurs et des services. Dans le champ judiciaire, l'IA commence à être utilisée en France comme outil de simplification du travail judiciaire par l'automatisation des procédures les plus lourdes. De manière expérimentale, la Lettonie projette d'utiliser un programme d'IA permettant de rendre

des décisions de justice en matière de délits mineurs. L'apport de l'IA réside dans sa capacité à générer des programmes à même d'affronter le volume et la complexité des dossiers à traiter comme autant de vastes systèmes de données. Elle n'est alors ni plus ni moins qu'un outil d'assistance limité au calcul et à l'analyse qui facilite l'action des services en augmentant leur potentiel de détection et d'intervention.

Toutefois, un usage de certains de ces algorithmes, basés sur une analyse de données et un calcul de probabilités appliqués à des domaines jusque-là dévolus à la conception et la décision humaines, a conduit à populariser l'idée d'une capacité à prévoir qui, très vite, s'est transformée en une capacité à prédire. C'est ainsi que l'on a pu parler, en reprenant plus que hâtivement un registre lexical importé des États-Unis, de l'avènement d'une police et d'une justice « prédictives ».

Cette expression désigne la faculté à prévoir des événements susceptibles de se produire ou de se répéter, qu'il s'agisse, par exemple, de lieux où vont se dérouler des actes de délinquance, de récidives de la part de certains sujets délinquants, ou encore des décisions de justice susceptibles d'être rendues pour certains contentieux. Le terme de police prédictive nous vient des États-Unis (*predictive policing*) où dans plusieurs grandes villes (New York, Chicago, Los Angeles...) les services de police utilisent des programmes informatiques élaborés par des entreprises privées dans le but de cerner au plus près la réalité locale de la délinquance pour pouvoir la prévenir au mieux. Ces programmes intègrent une cartographie et une analyse statistique des faits de délinquance visant à déterminer les lieux où ces faits sont susceptibles de se produire. Il s'agit donc essentiellement d'outils de prévention et le terme de prédictif désigne ici la prévision des risques.

La justice prédictive permet, par exemple, de prendre des décisions en matière de libérations conditionnelles (aux



LE RISQUE QUI PEUT ÊTRE POINTÉ EST ALORS  
CELUI DU RÉTRÉCISSEMENT DE L'AIRE  
DE LA RESPONSABILITÉ HUMAINE. JUSQU'À  
QUEL POINT NOUS DÉFAUSSONS-NOUS DE  
NOTRE RESPONSABILITÉ, DE NOTRE FACULTÉ  
DE CRÉATION PARCE QUE NOUS TRANSFÉRONS  
UNE GRANDE PART DE CELLES-CI À DES  
PROGRAMMES PLUS EFFICACES QUE NOUS ?  
JUSQU'À QUEL POINT ACCEPTONS-NOUS DE  
LIMITER NOTRE LIBERTÉ EN NOUS REPOSANT  
SUR DES PROGRAMMES PARCE QU'ILS ASSURENT  
EFFICACEMENT NOTRE PROTECTION  
ET NOTRE BIEN-ÊTRE ?



États-Unis) ou, au niveau de la justice civile en France, de prévoir la décision la plus à même d'être rendue dans un contentieux donné.

En réalité, le terme de prédictif mélange deux significations. La signification première qui est celle du verbe prédire, annoncer un événement à venir, et la deuxième qui en est l'extension abusive, annoncer un événement probable. C'est cette dernière signification, utilisée à la fois dans un usage courant, mais surtout en référence à l'analyse statistique qui extrait un certain nombre de données pour établir des tendances et des lignes d'évolution possibles, qui est la seule appropriée. Qu'il s'agisse de la police ou de la justice, leur nouvelle capacité prédictive relève du jeu de mots. Dans les différents usages, judiciaires et sécuritaires, l'algorithme est un outil de calcul de probabilités. Il permet de manipuler un très grand nombre de données en diminuant considérablement le temps de ce calcul pour parvenir à une estimation de probabilité. Pour ce qui concerne la justice civile, les outils algorithmiques permettent de traiter les données concernant les décisions rendues pour les différents types de conflits afin de produire une échelle de probabilités permettant de désigner la décision de justice qui aura le plus de « chances » d'être rendue.

Quant aux outils de police prédictive, ils consistent essentiellement à analyser des données qui concernent, sur un territoire particulier, l'organisation de l'espace et les statistiques de telle ou telle délinquance pour déterminer en fonction des moyens disponibles l'action de prévention ou de répression à mener. Il s'agit donc de mettre en lumière des tendances fortes sur les lieux où tel ou tel type de délinquance a le plus de probabilité de se produire pour avoir un temps d'avance sur les interventions.

Il n'y a donc pas de justice ni de police « prédictives » mais de nouveaux outils qui permettent un traitement d'informations aboutissant (sur la base d'une échelle de probabilités) à la production de nouveaux outils d'aide à la décision (pour la justice) et aux interventions (pour les forces de sécurité).

Exit les *Précogs* de « Minority Report », nous avons simplement affaire à des logiciels qui extraient, trient et recourent... Justice et police ne prédisent rien, mais calculent de plus en plus. Dès lors le véritable enjeu autour du prédictif n'est pas celui du libre arbitre face à un avenir définitivement établi, mais celui de la transparence et de la maîtrise. Sur quoi portent ces calculs ? Qui les manie ? Qui les contrôle ?

Même remis à sa juste place, le terme de prédictif soulève un certain nombre de questions d'ordre éthique.

– la question de l'encadrement par la loi et du contrôle démocratique en particulier dans un contexte d'émergence d'un marché privé. Dans la production des outils « prédictifs » basés sur les algorithmes, qui produit les codes et sur quelles bases ? Quel est le statut juridique de l'algorithme ? Quelle est sa place en procédure ? Comment encadre-t-on son usage ? Qui construit l'équation ? Qui agrège les données ? Qui opère des audits ?

– la question, à partir de l'existant en matière de justice civile et commerciale, d'une extension possible au champ de la justice pénale. Si la justice pénale n'est pas aujourd'hui en France directement concernée par le recours aux algorithmes, les bouleversements à l'œuvre dans le champ de la justice civile et les enseignements à tirer des expériences en cours aux États-Unis imposent d'ouvrir une réflexion prospective en identifiant un certain nombre de problèmes spécifiques qui vont se poser. Ainsi, l'effet performatif qui peut conduire à figer le présent sur la base de données du passé. Appliqué à la justice pénale, le risque est réel d'une soumission des décisions de justice (la jurisprudence), sous couvert d'efficacité managériale et d'harmonisation, à une norme médiane érigée en vérité quasi scientifique, alors qu'elle n'est que le simple résultat d'un calcul probabiliste ;

– la question pour la justice pénale de la place laissée à l'interprétation de la complexité liée à la question de la preuve lorsque le calcul du « probable » prend la place du débat judiciaire. Les données traitées par les algorithmes doivent clairement avoir le statut de simple expertise soumise au débat judiciaire comme tout élément de preuve sur lequel le juge se fonde pour condamner.

Dans le champ sécurité-justice, l'IA s'inscrit dans le prolongement du mouvement d'automatisation qui permet la simplification des tâches les plus complexes et allège le travail judiciaire et policier augmentant d'autant son efficacité. Néanmoins, ces nouveaux outils algorithmiques n'en posent pas moins des problèmes nouveaux.

Aux questions déjà soulevées dans le cas de la police et de la justice prédictives et qui concernent essentiellement les domaines de la responsabilité morale et juridique, il faut en ajouter une dernière, majeure, qui s'inscrit dans le débat traditionnel sur la technique mais le pose en des termes renouvelés. Ces nouveaux outils marquent-ils une nouvelle étape dans la réduction de l'aire de liberté humaine ? En matière de sécurité et de justice, cette question se pose plus concrètement en termes de libertés individuelles et publiques.

## Le nouveau paradigme sécurité-liberté

On ne peut dissocier les problèmes spécifiques posés par l'usage de la numérisation d'une partie du travail de la police et de la justice, la dimension technique, des tendances à l'œuvre dans les sociétés dites « développées » en matière de représentations de la sécurité, la dimension politique. Nous assistons au croisement d'un double phénomène. D'un côté, une demande croissante de sécurité de la part des populations, demande qui excède le domaine de la délinquance pour investir tous les aspects de la vie quotidienne, santé, environnement, travail, déplacements... De l'autre côté, la possibilité de répondre de plus en plus et de mieux en mieux à cette demande devenue globale grâce aux performances des nouvelles « machines » numériques. Plus cette demande se généralise et s'étend, plus elle trouve en effet de réponses dans les moyens que le développement technologique dégage mais plus ces moyens dessinent également un nouveau cadre politique et sociétal. Celui-ci se caractérise par une situation où l'accroissement de la protection des citoyens engendre simultanément un accroissement du contrôle de leurs actes et de leur vie.

Cette question est devenue symboliquement visible lors du déploiement des caméras de vidéo comme moyen de gestion de la délinquance de voie publique. Les hésitations sur la terminologie, vidéoprotection ou vidéosurveillance, étaient symptomatiques de deux visions politiques de l'usage d'une même technologie. Le débat se pose de nouveau aujourd'hui avec la reconnaissance faciale, laquelle devrait, entre autres, améliorer l'identification de personnes recherchées et faciliter la résolution de certaines enquêtes. Les deux technologies reposent sur les mêmes objectifs et le même principe de fonctionnement : améliorer la prévention et la lutte contre la délinquance à l'aide de programmes qui supposent d'extraire (au sein de la population générale) un nombre substantiel de données pour isoler un nombre limité de résultats (sur une infime partie de cette population générale). Pour protéger l'innocent du coupable, il faut recueillir un maximum d'informations sur l'innocent au risque que ces informations soient utilisées dans d'autres occasions contre l'innocent.

Il existe un débat traditionnel et récurrent sur la relation entre sécurité et liberté comme il existe un débat sur la relation entre technique et liberté. L'extension des nouveaux outils numériques conduit à un croisement de ces deux débats qui se posent dès lors dans des termes renouvelés. Là où le débat sécurité et liberté mettait traditionnellement en jeu une tension entre les nécessités

de la répression de la délinquance et celles de la garantie des droits individuels, il est question aujourd'hui sous la pression de la demande de sécurité des populations de faire reculer toujours plus les limites au contrôle de tous au bénéfice de la capture de quelques-uns. Nous assistons ainsi à la naissance d'une « société de surveillance » qui tend à faire disparaître la notion même d'espace privé à travers l'articulation entre l'objectif de la sécurité des populations et la capacité d'intrusion permise par les nouvelles technologies. Face à l'idéal de la sécurité totale, le développement de la société de surveillance. La sécurité totale est un service, la société de surveillance le moyen et la condition de ce service. Encore ce service n'est-il plus un service public au sens antérieur du terme, c'est-à-dire exercé par l'État avec un certain nombre de garanties.

Le débat ancien sécurité et liberté opposait une vision fondée sur le conflit entre l'un et l'autre terme. Pour les uns, assurer la sécurité est une mission première de l'État qui est dès lors légitimé à employer les moyens nécessaires pour y parvenir, y compris la restriction de certaines libertés. Pour les autres, la notion de libertés individuelles est première et tout empiétement sur celles-ci au nom des impératifs de sécurité masque un autre objectif qui est celui d'assurer un ordre reposant sur les intérêts d'une fraction de la population minoritaire mais détentrice du pouvoir. Dans un État de droit la question constante concerne la position du curseur entre l'impératif de sécurité et l'idéal de liberté. Ce curseur varie selon les options politiques des pouvoirs en place et selon les évolutions de la société et de l'opinion publique en matière d'exigence de sécurité ou en fonction de l'irruption d'événements traumatiques comme les attentats terroristes. Aujourd'hui, la relation sécurité-liberté ne peut plus être appréhendée à partir du seul conflit entre ces deux termes. La révolution numérique, en ce qu'elle répond aux attentes de la société de surveillance, est venue introduire deux nouvelles dimensions et nécessite par conséquent une nouvelle grille de lecture.

Premièrement, la question de la position du curseur se pose différemment dans la mesure où la demande de sécurité devient exponentielle et s'étend à des domaines de plus en plus vastes de la vie quotidienne. Dès lors que se répand l'idée d'une possible sécurité totale, l'augmentation du prix à payer en matière de restrictions des libertés sera jugée comme inévitable, comme un moindre mal. S'il est possible d'échapper à toutes les menaces potentielles et si cette possibilité est donnée par la technique, dite neutre par essence, pourquoi en effet s'en priver. À l'origine du déplacement du curseur vers le pôle sécurité totale, il y aura une demande massive venue de la population, ce qui ne pourra être ignoré dans une société démocratique où le pouvoir est issu du vote de cette population.

Deuxièmement, la question de l'entité garante à la fois de l'obligation de sécurité et du respect des libertés se pose également d'une manière nouvelle. Dans la grille de lecture précédente, cette entité est représentée par l'État dont différentes instances d'administration et d'exécution réalisent les missions. La révolution numérique n'a pas seulement permis l'émergence de nouveaux outils qui changent les modes de vie et les relations entre les hommes, elle est également le fruit de l'autre grand événement de ce siècle tout comme elle constitue l'un des moteurs de son développement, à savoir la mondialisation. Celle-ci a bouleversé les conditions de production des objets comme des savoirs, les structures économiques comme les rapports de force géopolitiques. La « traversée des frontières » qu'elle a rendue possible a mis en cause des structures antérieures constitutives de l'organisation des peuples, comme les nations et les États. Dans le cadre de ce mouvement, la révolution numérique a introduit de nouveaux acteurs qui exercent des missions antérieurement dévolues en exclusivité aux États-nations à travers la création, la maîtrise, la propriété et la diffusion des nouveaux outils. Ces acteurs constituent des entités qui, si elles ne se sont pas substituées entièrement aux États, les concurrencent et leur contestent au minimum l'exclusivité de certaines missions, dites antérieurement « régaliennes », et au maximum la maîtrise mondiale de l'exercice de ces missions. Il s'agit des fameux « Gafam » dont le modèle économique repose sur la gratuité des services en échange de la cession d'informations sur la vie personnelle. La vision d'une révolution numérique comme simple technique neutre de mise en réseau d'individus libres s'est vite délitée devant la réalité d'organisations économiques, opaques et monopolistiques, en charge d'aspects de plus en plus nombreux de la vie humaine à travers le monde et exerçant par conséquent une fonction éminemment politique. D'évidence, un tel bouleversement change la donne en ce qui concerne la relation sécurité-justice.



LÀ OÙ LE DÉBAT SÉCURITÉ ET LIBERTÉ METTAIT TRADITIONNELLEMENT EN JEU UNE TENSION ENTRE LES NÉCESSITÉS DE LA RÉPRESSION DE LA DÉLINQUANCE ET CELLES DE LA GARANTIE DES DROITS INDIVIDUELS, IL EST QUESTION AUJOURD'HUI SOUS LA PRESSION DE LA DEMANDE DE SÉCURITÉ DES POPULATIONS DE FAIRE RECULER TOUJOURS PLUS LES LIMITES AU CONTRÔLE DE TOUS AU BÉNÉFICE DE LA CAPTURE DE QUELQUES-UNS. NOUS ASSISTONS AINSI À LA NAISSANCE D'UNE « SOCIÉTÉ DE SURVEILLANCE » QUI TEND À FAIRE DISPARAÎTRE LA NOTION MÊME D'ESPACE PRIVÉ À TRAVERS L'ARTICULATION ENTRE L'OBJECTIF DE LA SÉCURITÉ DES POPULATIONS ET LA CAPACITÉ D'INTRUSION PERMISE PAR LES NOUVELLES TECHNOLOGIES.



Là où les États de droit avaient la double mission d'assurer la sécurité et de garantir la liberté, avec selon les circonstances des variations dans l'équilibre entre l'un et l'autre, les nouveaux acteurs créateurs et diffuseurs des outils numériques au service de la sécurité, « hors sol », possèdent une réelle capacité à s'affranchir des contrôles et de la nécessité de rendre compte. Les citoyens protégés par l'État sont maintenant des utilisateurs dans le cadre d'un « contrat » où ils fournissent des informations sur eux-mêmes en échange de cette protection. Qu'en est-il du stockage et de l'utilisation de ces informations ?

La contrepartie de la protection est la dépendance à ceux qui en fournissent les moyens et la société de surveillance se met en place sous la direction de puissances hors sol, hors législations nationales.

Le nouveau paradigme sécurité *versus* liberté repose ainsi sur une nouvelle relation entre les populations et les instances en charge de leur protection différente de l'ancienne relation des citoyens avec leur État-nation ; les Gafam sont, en effet, venus changer la structure de cette relation, au risque de faire disparaître les citoyens derrière les utilisateurs. Ceux-ci ont aujourd'hui affaire à une nouvelle cartographie d'« économies-monde », telles que les définissait

Fernand Braudel, où se croisent et se confrontent des États (nations et/ou empires) classiques et des empires nouveaux (extra-territoriaux). Dès lors, le débat sur l'équilibre entre sécurité et liberté ne consiste donc plus seulement à mettre des limites (politiques, juridiques) au pouvoir d'une instance chargée de la mission de sécurité, mais aussi et surtout à maîtriser le développement d'une capacité de surveillance exponentielle au bénéfice d'intérêts de structures dont la forme et la légitimité n'ont plus rien à voir avec l'exercice du monopole de la violence légitime de Max Weber. Ce n'est plus (seulement) un État Léviathan sécuritaire qui est à redouter mais un réseau aussi étendu que complexe, dépourvu de la

moindre « volonté » centralisée et dont la sophistication même permet l'invisibilité. C'est le *Big Brother* d'Orwell sans dictateur ni parti. Si les outils nouveaux posent et poseront toujours des questions, la question première reste celle de leur finalité et de leur contrôle.

La révolution numérique reprend et prolonge les interrogations plus traditionnelles sur le contrôle démocratique et la protection des libertés, mais exige une vigilance permanente sur le risque d'installation d'une « vision du monde » fondée sur la réduction de l'humain et des relations sociales à un système mathématisé de données. La problématique « justice-police-IA » relève d'un débat global d'ordre philosophique et politique où ce qui est principalement en cause et en jeu est la nature

de l'État (démocratie ou non, existence ou absence de contrôle et de contre-pouvoirs). Hors la prophétie transhumaniste qui annonce une tout autre histoire (ou chimère), les débats à poursuivre consistent à laisser les outils à leur place, à s'entendre sur leurs fins et à se doter des moyens de contrôler leur exécution ■



## Les usages des algorithmes. L'estimation de la récidive dans la justice pénale américaine

Angèle CHRISTIN

Angèle CHRISTIN



Sociologue et ethnographe, Angèle Christin est maîtresse de conférences à l'université de Stanford au département de communication.

Son travail porte sur l'approche qualitative des *big datas* et des algorithmes.

De nombreux articles journalistiques ont récemment traité aux États-Unis la question des algorithmes prédictifs dans la justice pénale, pour la plupart de façon assez critique. Ils développent l'idée selon laquelle les programmes utilisés pour prédire les crimes futurs comportent des biais dirigés contre les populations africaines-américaines, certains demandant l'arrêt immédiat de l'utilisation de l'intelligence artificielle pour condamner des criminels. Dans l'un d'entre eux, « *When a computer program keeps you in jail*<sup>1</sup> », l'auteur s'interroge sur le fait d'être maintenu en détention contre sa volonté (ce qui est généralement le cas lorsque

l'on est en prison) par un programme informatique. Tous ces articles proviennent de médias américains très prestigieux qui se sont emparés de la question des algorithmes prédictifs dans la justice pénale. Leur lecture montre clairement le type d'inquiétudes que soulèvent les algorithmes prédictifs.

Ces inquiétudes portent tout d'abord sur la notion même de prédiction. Est-il légitime de prendre en compte, dans des décisions judiciaires présentes, le risque de crimes futurs qui n'ont pas eu lieu ? C'est l'effet *Minority Report*, le film de Steven Spielberg, qui apparaît ici autour de l'idée que l'on puisse être jugé un jour pour des crimes qui n'ont pas été encore commis.

Elles portent ensuite sur la question de la discrimination. C'est un sujet très important,

(1) Rebecca Wexler, *The New York Times*, 13 juin 2017.

dans le contexte américain où les Africains-Américains ont été discriminés de façon systématique pendant plusieurs siècles et encore plus au sein du système pénal au cours des cinquante dernières années, dans un contexte d'incarcération de masse qui touche principalement les populations de noirs pauvres.

Elles sont enfin liées à la crainte du remplacement des humains par les machines, avec l'hypothèse que l'intelligence artificielle va nous faire disparaître les humains, que la justice sera complètement automatisée et le sort de chacun déterminé par une machine. Derrière cette hypothèse se profile également la perspective d'une absence de recours contre la machine, l'idée que lorsqu'une machine décide à la place d'un humain, on ne peut plus rien y faire, selon l'exemple des programmes automatisés qui vous envoient des publicités sur Internet même si elles ne sont pas souhaitées.

Toutes ces inquiétudes sont en partie fondées. Toutefois, comme souvent, la réalité de ces outils algorithmiques et la façon dont ils sont utilisés dans les juridictions américaines se révèlent bien plus complexes que ce que les médias en disent. C'est ce que montre un état des lieux des algorithmes de prédiction de la récidive dans le cas américain dressé sur la base d'une critique raisonnée élaborée notamment à partir d'une enquête ethnographique que j'ai pu mener dans plusieurs tribunaux aux États-Unis.

Quels sont en réalité ces outils ? Il convient tout d'abord de souligner que l'usage de techniques prédictives dans le système pénal est loin d'être nouveau, notamment aux États-Unis, puisque les premières techniques remontent aux années 1930, notamment avec les travaux d'Ernest Burgess, sociologue à l'université de Chicago. Plus ou moins dans la lignée d'Émile Durkheim (bien que celui-ci ait plutôt étudié le suicide), Burgess travaillait alors sur la question de la possibilité et du moyen de savoir comment prédire le crime futur. Cette préoccupation est donc, d'une certaine manière, une question sociologique très ancienne, mais une indéniable multiplication de ces outils s'est produite au cours de ces dernières années. Cette multiplication a eu lieu en deux temps. Ce point est important, car la perception courante de ces algorithmes renvoie à la découverte d'un objet totalement nouveau, au surgissement d'une « révolution du *big data* » liée aux technologies numériques, en oubliant que ces technologies ont une histoire.

Pour ce qui concerne les algorithmes d'estimation de la récidive, cette histoire remonte aux années 1970. Ils trouvent notamment leur origine dans les travaux de criminologues et de psychologues qui ont développé, sur

la base des connaissances criminologiques de l'époque, un ensemble de *risks assessment tools*, d'« outils d'estimation du risque », fonctionnant de façon assez simple. Il s'agissait de trouver une base de données portant sur un ensemble de cas, jugés sur une période délimitée, par exemple les années 1970-1975, et comportant un certain nombre de variables. Ces variables portaient sur les prévenus, les personnes condamnées, la peine prononcée, sur la récidive en général et en particulier (prise en compte du parcours du condamné jusqu'à cinq ans après le moment de l'arrestation pour identifier s'il y a récidive). L'objectif était d'élaborer une analyse statistique construite sur la base de régressions linéaires, elles-mêmes établies à partir d'un certain nombre de variables afin de comprendre quelles étaient les variables prédictives des taux de récidive. Autrement dit, il s'agissait d'identifier quelles caractéristiques de l'individu menaient aux taux de récidive les plus élevés. Par la suite, les outils ont renversé les modèles pour les rendre prédictifs. Il s'est alors agi de dire qu'étant donné que si tel prévenu présentait telle et telle variable, par exemple s'il s'agit d'un homme de 35 ans avec un casier judiciaire portant mention de cinq condamnations dont deux pour des faits avec violences, alors le risque de récidive de cet individu sera estimé à tel ou tel pourcentage.

Les modèles ont bien entendu évolué depuis. Il existe désormais des technologies beaucoup plus complexes pour calculer et faire émerger des structures provenant de bases de données beaucoup plus importantes. Pour autant, le modèle reste le même et la plupart des outils d'estimation de la récidive continuent de fonctionner plus ou moins à partir de régressions linéaires. Quelques outils utilisent le *machine learning* (apprentissage automatique), mais peu fréquemment encore notamment parce que les bases de données ne sont pas assez étendues pour que cette utilisation apporte une véritable plus-value. C'est pourquoi le plus souvent on a recours à des techniques statistiques assez anciennes qui vont permettre d'afficher un score de risque allant de 1 à 10.

Actuellement, plus de soixante instruments d'estimation du risque sont ainsi en circulation dans les juridictions américaines, dont certains se révélant assez précis. Il existe ainsi des instruments en matière de délinquance sexuelle, comme le « Static-99 » qui est l'un des outils les plus utilisés pour prédire le risque de récidive chez les délinquants sexuels. Il existe également des instruments de mesure des risques en matière de justice des mineurs, en matière de probation, ou encore de mise en liberté conditionnelle. Certains outils sont utilisés à différents endroits de la chaîne pénale et dans différents secteurs de la justice pénale américaine. Deux de ces outils sont particulièrement significatifs.

Le premier est développé par l'État de Virginie pour la phase que l'on appelle la *Pretrial Justice*, autrement dit la phase pré-sentencielle de la justice pénale. La question à laquelle la justice souhaite répondre à ce stade est celle du placement en détention provisoire du prévenu dans l'attente de son procès. L'outil qui a été élaboré doit permettre non pas de prédire la récidive, mais de prédire ce que l'on appelle le *failure to appear in court*, autrement dit d'évaluer les chances qu'a le prévenu de ne pas comparaître devant le tribunal lorsqu'il y sera convoqué. Il s'agit d'un programme informatique installé sur les ordinateurs des officiers du *Pretrial Justice Department*, qui sont généralement des travailleurs sociaux, ainsi que sur ceux des procureurs des juridictions. Ce programme a été diffusé dans d'autres États que l'État de Virginie, car les juridictions s'empruntent et s'échangent leurs outils lorsque l'un d'eux fonctionne bien. Celui-ci regroupe un ensemble de variables assez intéressantes : « *risk factors* », les facteurs de risques ; « *history of drug use* », l'histoire de consommation de drogue ; « *employed caregivers verified* », est-ce que la personne est « aidante » ? A-t-elle des enfants ou des personnes âgées sous sa responsabilité ? A-t-elle un emploi ? Ou en a-t-elle eu un dans les deux années précédentes ? Sa résidence est-elle vérifiée ? A-t-elle un lieu de résidence vérifiable ? ... ; « *violences convictions* », poursuites pénales antérieures pour des faits de violence ; « *failure to appear in court* », est-il déjà arrivé que la personne ne se présente pas devant le tribunal ? ; « *criminal history* », « *pending charges* », « *church type* », etc. Ces variables portent donc à la fois sur l'histoire criminelle et pénale du prévenu, sur son casier judiciaire, à la fois sur des variables de nature sociodémographiques, sur l'emploi, la situation familiale, etc. Une fois que l'ensemble de ces informations est renseigné, le programme propose un bouton appelé « *calculate risk* » qui, lorsque l'on appuie dessus, affiche une estimation du risque qui va de 1, *low risk*, à 10, *high risk*. Ce sont ces estimations des risques qui sont prises en compte par les magistrats au moment de la décision de placement en détention provisoire.

Le deuxième, très commenté par la presse américaine, est dénommé COMPAS (*Correctional offender management*

*profiling for alternative sanctions*). Une analyse statistique assez importante menée par les journalistes de *ProPublica* a permis de montrer que l'outil en question était, aux États-Unis, discriminatoire vis-à-vis des noirs. Il s'agit d'un outil plus moderne, à l'interface plus esthétique, mais dont les questions sont beaucoup plus intrusives. Le questionnaire proposé, très populaire, est utilisé dans la plupart des juridictions américaines, mais également au Canada. Il est en général soumis aux prévenus et parfois aux personnes incarcérées, selon le stade de la procédure auquel il est utilisé. Parmi les questions posées existent d'abord des questions qualitatives, relatives aux réseaux de sociabilité des prévenus en général, « *Tell me about your friend* », « parlez-nous de vos amis », « avec qui passez-vous votre temps » ? « Comment sont-ils ? » « Ont-ils déjà eu des problèmes » ? « Vos parents aiment-ils vos amis » ? etc. Un second ensemble de questions, beaucoup plus détaillé, portant sur les réseaux de sociabilité et sur la sociabilité des délinquants, est ensuite soumis : « vos amis boivent-ils » ? « Oui. Non. Parfois. Je ne sais pas ». « Vos amis font-ils usage de drogues ? » « Oui. Non. Parfois. Cela dépend ». « Sont-ils affiliés à des gangs ? Oui. Non. Parfois ». « Ont-ils déjà été arrêtés ? Oui. Non. Parfois. Je ne sais pas », etc. Il s'agit en tout d'un ensemble de 110 questions soumises

aux prévenus, au terme desquelles il faudra appuyer sur le bouton de calcul de risques. Il sera alors prédit un ensemble de choses assez différentes, qui apparaîtront sous la forme d'un *assessment*, d'un résultat quantitatif, allant de 0 à 10, assorti d'un code couleur. L'outil peut prédire le *violent recidivism risk*, le *general recidivism risk*, ou encore le *pretrial bilis risk* ; il existe différents scores, différents codes couleurs donnant des indices, le rouge correspondant par exemple à une situation inquiétante. Un ensemble d'autres variables relatives à l'activité criminelle, aux relations, au mode de vie, à la personnalité et aux attitudes du prévenu est également calculé.

Pour bien saisir comment ces outils sont utilisés, il faut comprendre que la feuille de résultat est imprimée, versée au dossier et que les magistrats la consultent lorsqu'ils prennent les décisions sur les cas en question. Nous



LE FAIT QUE CES MODÈLES NE SOIENT PAS UTILISÉS DANS LE CADRE D'UNE JUSTICE TOTALEMENT AUTOMATISÉE N'EMPÊCHE PAS QUE CES ALGORITHMES D'ESTIMATION DE LA RÉCIDIVE POSENT PAR AILLEURS DES PROBLÈMES. UNE SÉRIE DE CRITIQUES PORTE AINSI SUR LES MODÈLES DE CONSTRUCTION, SUR LA FAÇON DONT CES ALGORITHMES SONT CONSTRUITS ET SUR LES PROBLÈMES QUE CELA POSE.





sommes bien loin d'une justice totalement automatisée au sein de laquelle les algorithmes prendraient les décisions. En vérité, ce sont des outils d'aide à la décision pour les magistrats, ceux-ci étant considérés dès lors comme mieux informés grâce à ces techniques quantitatives. C'est du moins comme cela qu'ils sont présentés. Les outils susmentionnés sont deux exemples parmi d'autres, puisqu'il existe plus de soixante outils, tous différents, prédisant des choses différentes et utilisant des variables différentes.

Le fait que ces modèles ne soient pas utilisés dans le cadre d'une justice totalement automatisée n'empêche pas que ces algorithmes d'estimation de la récidive posent par ailleurs des problèmes. Une série de critiques porte ainsi sur les modèles de construction, sur la façon dont ces algorithmes sont construits et sur les problèmes que cela pose.

La première critique porte sur l'opacité, laquelle se situe à plusieurs niveaux. D'abord, au niveau du code : les bases de données sur lesquelles s'appuient ces modèles ne sont jamais ni diffusées ni rendues publiques, pour la simple raison qu'ils sont en général élaborés et construits par des compagnies privées, dont l'objectif premier est, par définition, le profit. Ainsi COMPAS est construit par NorthPoint (désormais Equivant), une compagnie privée. Le code de l'algorithme est protégé par la propriété intellectuelle et les entreprises n'ont aucune envie de le partager avec qui que ce soit. Qu'il s'agisse des juridictions avec lesquelles elles travaillent, des chercheurs, des médias ou des prévenus, le code reste secret. Pour autant, lorsqu'il arrive que des codes soient rendus publics, par exemple lorsque les instruments de prédiction sont construits par les juridictions elles-mêmes et non par des compagnies privées, ils demeurent très opaques, simplement parce que la plupart des gens ne savent pas lire des codes. Combien de personnes sont formées en informatique et capables de lire le code d'un algorithme prédictif ? Assez peu.

Par ailleurs, au sein même des tribunaux, les prévenus et les avocats de la défense n'ont souvent pas accès aux résultats promus par l'algorithme. Alors que des risques et des scores allant de 1 (*low risk*) à 10 (*high risk*) circulent sur un prévenu, celui-ci ne sait pas lui-même qu'un chiffre est attaché à sa personne et le suit tout au long de son parcours pénal. Cette situation génère une forte asymétrie au sein de la chaîne judiciaire. Le problème de l'opacité réside principalement dans l'absence de mécanisme de contestation ou de recours. Qu'implique le fait d'être l'objet d'un « score » sans avoir la possibilité de le contester ? De quelle manière cela impacte-t-il l'image et le fonctionnement de la justice américaine, et tout particulièrement la notion de *due process of law*, très importante dans ce système pénal ?

La deuxième critique est relative au mode de construction des algorithmes et concerne la discrimination. Certaines analyses menées par des journalistes, des chercheurs et des informaticiens ont conduit à penser que les algorithmes d'estimation de la récidive et, notamment, COMPAS, comportent des biais dirigés envers certains groupes sociaux et ethniques et plus spécifiquement les Africains-Américains. Deux critiques quelque peu différentes l'une de l'autre ont été formulées. La première porte sur le fait que certaines variables utilisées dans les modèles utilisés servent de *proxy* et opèrent de façon très significative des corrélations à partir de la notion de race. Ainsi, les codes postaux sont-ils très utilisés aux États-Unis pour déterminer le lieu de résidence des personnes, cela dans un pays où les quartiers et leurs résidents sont fortement « ségrégués » et où l'histoire de cette ségrégation est par ailleurs très ancienne. La variable des codes postaux vient alors se corréliser assez fortement à la race, tout comme les taux d'emploi deviennent des indicateurs également reliés à la race. Si l'on crée des parallèles entre les deux types d'indicateurs, il devient alors très vite possible d'identifier si la personne est africaine-américaine ou « latino ». Ainsi, même si la variable « race » n'est jamais incluse en tant que telle dans ces modèles puisque cela serait inconstitutionnel, la plupart des variables utilisées entrent néanmoins en corrélation avec la notion de race. Un soupçon d'inconstitutionnalité plane donc sur l'ensemble de ces modèles.

Les constructeurs de ces différents modèles se défendent de la manière suivante : « *C'est très simple. Nous allons juste retirer le code postal, nous allons retirer l'emploi, et comme cela le modèle ne sera plus discriminatoire* ». Mais à cela les informaticiens et les chercheurs en sciences sociales répondent : « *C'est beaucoup plus compliqué. Vous vous servez de données historiques, de données qui datent des années 1990 en général ou du début des années 2000. Ces données historiques portant sur des cas qui ont déjà été jugés dans le cadre du système pénal américain sont marquées par un système discriminatoire. Nous savons très bien que la justice pénale américaine incarcère les noirs pauvres beaucoup plus que tout autre groupe social. En se servant de ces bases de données historiques, vous reproduisez, voire pire, vous renforcez les dynamiques raciales et sociales à l'œuvre que vous essayez d'améliorer. Or, l'argument avancé pour utiliser ces algorithmes est en général : "ils sont plus objectifs que le jugement subjectif des juges et des magistrats"* ». La réalité est que cela reproduit et renforce les discriminations.

La troisième critique porte sur le fait que les algorithmes créeraient un système à deux vitesses. La plupart de ces algorithmes prédictifs concernent en effet la petite délinquance pénale, autrement dit la justice pénale de masse, l'équivalent des procédures de comparutions immédiates en France (violences urbaines, petits délits,



LES BIG DATA SONT SOUVENT PRÉSENTÉES  
 COMME DES TECHNOLOGIES NEUTRES,  
 IMPARTIALES, OBJECTIVES, EFFICACES, OFFRANT  
 UNE FAÇON DE RÉGLER TOUT CE QUE NOUS  
 HUMAINS N'ARRIVONS PAS À FAIRE,  
 DES PROBLÈMES POLITIQUES ET SOCIAUX  
 CONNUS DE TOUS, QUI DURENT DEPUIS DES  
 SIÈCLES MAIS QUE NOUS NE PARVENONS  
 PAS À RÉSOUDRE.  
 L'ALGORITHME EST PERÇU COMME UNE SORTIE  
 DE SOLUTION TOMBÉE DU CIEL QUI NOUS  
 AIDERAIT À TOUT RÉGLER.  
 AUX ÉTATS-UNIS, C'EST CE QUE L'ON  
 APPELLE LE TECHNOLOGICAL DETERMINISM,  
 AUTREMENT DIT CETTE IDÉE QUE TOUT EST  
 POSSIBLE GRÂCE À LA TECHNOLOGIE.



usage et consommation de drogue, etc.). C'est dans ce registre que se situe la grande majorité, si ce n'est l'ensemble des algorithmes prédictifs (les exceptions concernant la justice civile). Qu'en est-il alors de la délinquance financière, de la criminalité financière ? Pourquoi existe-t-il des algorithmes permettant de prédire la récidive des petits délits urbains qui sont, on le sait, surtout commis par des minorités et des gens avec peu de revenus, et pas d'algorithmes permettant de prédire la criminalité financière ? C'est la base de la critique d'une justice à deux vitesses, l'une pour les classes supérieures gérée par des humains qui prennent le temps de la décision et l'autre, automatisée, destinée aux pauvres et aux noirs.

Il y a enfin une dernière critique qui concerne les prophéties auto-réalisatrices induites par l'usage de ces algorithmes. Ainsi un individu étiqueté comme se situant à un haut niveau de risque aura plus de probabilité d'être incarcéré. Or, sachant que les prisons sont des lieux de sociabilité criminelle assez importants et qu'il est beaucoup plus difficile de trouver un emploi si l'on a un casier judiciaire, le risque d'augmentation de la récidive augmentera encore davantage. L'algorithme crée ainsi ce qu'il cherche à décrire.

Voici en résumé, les différentes critiques de ces modèles. Toutefois, mon travail de sociologue et d'ethnologue se concentre plus sur l'étude des usages. Je passe du temps

avec les acteurs et j'essaie de comprendre comment ils font les choses.

J'ai étudié pendant de longues années la justice pénale, notamment française. En observant les audiences de comparutions immédiates, j'ai été frappée par le fait que les juges et les procureurs, qui devaient prendre un nombre très important de décisions en disposant de très peu de temps et d'assez peu d'informations, étaient conduits à adopter des raccourcis cognitifs pour distinguer quels étaient les cas normaux et les cas anormaux ainsi que pour déterminer le type d'orientation légitime à donner à tel ou tel type de cas. Dès lors, je me suis intéressée aux algorithmes prédictifs, car ceux-ci visent à donner plus d'informations aux juges et aux procureurs, des informations automatisées et quantifiées, portant sur quoi faire de ces cas, quel est le degré de risque, etc. J'ai donc décidé de mener une enquête ethnographique mais cette fois-ci dans le contexte américain. L'enquête est en cours, je la mène actuellement sur le terrain dans trois tribunaux, l'un situé sur la côte est, le deuxième sur la côte ouest et le dernier dans le sud des États-Unis, au Texas. Je conduis des entretiens avec les juges, les procureurs, les avocats, les greffiers ainsi qu'avec un ensemble d'acteurs judiciaires, afin de leur demander de quelle manière ils utilisent ces outils prédictifs. Les résultats que je vais présenter sont donc provisoires, préliminaires.

Les principaux éléments que j'ai pu établir sont les suivants. En premier lieu, je constate un important manque de confiance de la part des professionnels de la justice, envers les outils prédictifs. En général il ressort très fortement de tous mes entretiens avec les juges et les procureurs des propos tels que : « *Mais pourquoi devrait-on se servir de ces outils prédictifs, alors que moi, Madame, je suis juge ou procureur depuis trente ans, je connais mes dossiers, et ces outils regardent les mêmes variables que celles que moi je prendrais en compte. Pourquoi devrais-je faire confiance à une boîte noire que je ne connais pas ? Je ne comprends pas d'où viennent ces données. Je ne connais pas la compagnie qui les a créées. Pourquoi devrais-je reléguer mon expertise et ma légitimité à cet algorithme ?* ».

En second lieu, et c'est là le corollaire de ce manque de confiance envers les outils prédictifs, je constate que ces derniers sont assez peu utilisés. Les résultats sont imprimés et versés au dossier mais dans les faits, ils sont assez peu mentionnés et pris en compte de façon marginale au cours de la prise de décision. En réalité, ils sont surtout mentionnés et utilisés par les procureurs dans le cadre des négociations sur la peine, au cours de la procédure de *plea bargain*, qui est très répandue aux États-Unis puisqu'elle concerne 97 % des dossiers. Dans certains cas, les procureurs utilisent ces évaluations du risque dans leur argumentation, pour négocier avec les

avocats : « *Attention, votre client a un risque très fort, je vais donc demander le prononcé d'une peine d'incarcération et vous devriez l'accepter* ». Ils sont généralement utilisés en tant qu'argument de justification dans le cadre de négociations assez tendues.

En troisième lieu, je constate qu'il y a une manipulation de ces instruments. En effet, remplir les grilles et renseigner les différentes variables de ces outils prend du temps, si bien qu'en général, ce ne sont pas les magistrats mais les travailleurs sociaux qui travaillent pour le Pretrial Department qui réalisent l'entrée des données nécessaires à l'utilisation des outils. Or, ces agents savent très bien manipuler les variables, les utiliser comme ils le souhaitent, par exemple pour que l'algorithme donne un score de 10, plutôt qu'un score de 8, ou inversement un score de 1 plutôt qu'un score de 4. Ces éléments signifient que le pouvoir de juger (j'ai ainsi traduit l'utilisation du mot « *discretion* » qu'elle a, je pense, utilisé en anglais et non français, et qui se rapporte du coup au terme « *discrétionnaire* », mais ce n'est qu'une hypothèse ?) est en train de glisser des magistrats vers ces travailleurs sociaux : ce sont eux qui décident comment remplir les variables, de même que ce sont eux qui savent quelles sont les variables qui ont le plus de poids dans un algorithme.

Enfin, et c'est un peu le bilan de cette enquête, je constate qu'il existe un écart assez marqué entre les usages souhaités et les usages réels des algorithmes. Les usages souhaités renvoient à l'idée selon laquelle les algorithmes doivent permettre de rendre la prise de décision judiciaire plus objective, plus informée, plus efficace, plus rapide. Mais, comme je viens de le montrer, ce qui se passe au sein des juridictions est plus compliqué et plus éloigné de ces projections un peu idéalisées.

Dans cette présentation, j'ai introduit les algorithmes prédictifs utilisés dans la justice pénale américaine et après avoir présenté un état des lieux des outils, j'ai discuté d'un certain nombre de critiques et de problèmes qui émergent, du fait de cette multiplication des technologies prédictives dans le secteur pénal.

Certaines de ces critiques portent plutôt sur les modèles, et il s'agit de critiques très importantes qu'il est nécessaire de prendre en compte, notamment afin d'essayer d'améliorer ces modèles, ou de se débarrasser de certains d'entre eux. Il n'est pas certain qu'une solution permettant de rendre ces

algorithmes parfaitement justes existe. Il y aura toujours des problèmes de discrimination, notamment parce que ces algorithmes s'appuient sur des données historiques et que ces données historiques sont elles-mêmes le véhicule de discriminations.

J'ai également abordé le fait que l'observation de l'usage fait de ces outils montre qu'ils s'imbriquent dans des pratiques judiciaires et des pratiques pénales de façon beaucoup plus complexe. On peut observer tout un ensemble d'effets inattendus, dont on discute peu alors qu'ils sont déterminants, surtout dans la perspective de réformer la justice pénale américaine.

En conclusion, je souhaite insister sur la nature proprement politique des technologies du *Big data*. Les *Big data* sont souvent présentées comme des technologies neutres, impartiales, objectives, efficaces, offrant une façon de régler tout ce que nous, humains, n'arrivons pas à faire, des problèmes politiques et sociaux connus de tous, qui durent depuis des siècles mais que nous ne parvenons pas à résoudre.

L'algorithme est perçu comme une sorte de solution tombée du ciel qui nous aiderait à tout régler. Aux États-Unis, c'est ce que l'on appelle le *technological determinism*, autrement dit cette idée que tout est possible grâce à la technologie. J'aimerais à l'inverse insister sur la nature proprement politique de ces technologies de prédiction. Dans le secteur pénal comme dans d'autres, le déploiement de ces instruments, de même que la façon dont ils s'installent dans des réseaux de pratiques et d'acteurs, pose des questions complexes. Nous devons nous demander quel modèle de justice nous voulons pour le futur, comment cela impactera ces algorithmes, mais aussi comment cela impactera tout le reste de la chaîne pénale ■



## Avons-nous le choix d'utiliser l'IA en temps de guerre ?

Marie-des-Neiges RUFFO de CALABRE

Marie-des-Neiges  
RUFFO DE CALABRE



Marie-des-Neiges Ruffo de Calabre est docteur en philosophie (Université Paris-Sorbonne,

Université de Namur), chercheur post-doc à l'université catholique de Lille au sein d'ETHICS (EA 7446), chercheur associé au Centre de recherche des écoles de St Cyr Coëtquidan (CREC), chargée d'enseignement à l'Institut catholique de Paris, chargée de cours à l'université de Namur (Belgique), membre d'ESPHIN (Espace philosophique de Namur), membre du Centre de recherche en information, droit et société (CRIDS), membre de la Complaints commission d'Euro-ISME (European Chapter of the International Society for Military Ethics), Prix de thèse IHEDN (Institut des hautes études de défense nationale), auteur d'*Itinéraire d'un robot tueur*, Éditions le Pommier, 2018.

Les possibilités d'emploi de l'IA dans le domaine militaire sont vastes, devons-nous l'utiliser à tout prix, sans analyse éthique préalable ? Si des enjeux stratégiques et légaux sont en jeu, il demeure nécessaire de respecter les deux piliers de l'éthique militaire ; la discrimination et la proportionnalité, ainsi que la tradition de la guerre juste. En outre, l'utilisation de l'IA pourrait accroître de nombreuses difficultés préexistantes : la course à l'armement, la prolifération, la dissuasion, le risque d'à nouveau user de l'arme nucléaire, de la guerre totale, des attaques préventives, et des armes de destruction massive notamment. L'IA n'est pas une technologie *mala in se*, pour autant qu'elle ne serve pas l'autonomie du tir, à travers la construction de SALA. L'humain doit conserver non seulement un contrôle efficace sur la machine, mais aussi une supervision éclairée par des connaissances techniques et des convictions éthiques démocratiques.

On attribue souvent à Machiavel cette sentence : « *la fin justifie les moyens* ». Les Anglais quant à eux utilisent le proverbe « *All is fair in love and war* », pour exprimer qu'à la guerre comme en amour, tout serait permis. Parfois, l'éthique semble oubliée ou considérée comme un accessoire luxueux, un artifice de bon ton pour le public, mais sans réel impact dans les pratiques. Ainsi, il n'est pas rare de constater une volonté ferme de développer et d'user de tous les moyens possibles pour porter la victoire.

Si l'objectif visé, la victoire, ressemble à une bonne intention, pouvons-nous, en tant que nation démocratique, nous contenter de balayer les principes juridiques et éthiques, au seul motif qu'ils pourraient constituer des contraintes à l'action ? Ne devrions-nous pas plutôt étudier préventivement les conséquences éthiques et juridiques des moyens que nous développons ? Si les moyens technologiques sont majoritairement éthiquement « neutres » indépendamment de leur contexte d'emploi, qu'en est-il des capacités nouvelles liées à l'automatisation, à l'autonomie, à l'emploi du *Big Data*, de l'IA, dans le contexte si

particulier des engagements militaires ? L'ampleur de ces révolutions numériques nous laisse-t-elle encore le choix de les utiliser ? Serions-nous forcés d'en faire usage au mépris de l'éthique ?

## De la possible existence de restrictions applicables à la guerre

Si, depuis le propulseur paléolithique jusqu'aux missiles balistiques intercontinentaux, l'histoire de l'armement a connu une sophistication croissante, et que selon Grossman, la guerre n'est rien d'autre que « *l'histoire de mécanismes de plus en plus efficaces pour conditionner les hommes à surmonter leur résistance innée à tuer leurs semblables*<sup>1</sup> », l'évolution juridique n'est heureusement pas en reste ; en témoignent les principes juridiques qui ont encadré progressivement les conflits, jusqu'aux derniers développements du droit international humanitaire (DIH), des conventions de Genève<sup>2</sup> et les interdictions de la CCW<sup>3</sup>. Le Moyen-Âge connaissait la « Trêve de Dieu », notre époque suspend théoriquement le déclenchement d'hostilités à une résolution de l'ONU. Certes, tout comme la trêve de Dieu ne fut pas toujours scrupuleusement respectée, ainsi en est-il parfois des décisions de l'ONU, comme ce fut le cas de la guerre en Irak en 2003. Cependant, loin de signifier leur inutilité, ces tentatives d'encadrer la violence pour favoriser la paix sont à considérer comme autant de pas dirigés vers davantage d'humanité, qui nous éloignent toujours un peu plus de la barbarie. Le chemin est certes encore long, certains ont parfois fait marche arrière, comme lors des nombreux génocides du XX<sup>e</sup> siècle, mais cela ne doit pas décourager les consciences.

Cet appel aux consciences trouve sa source dans l'éthique. L'éthique n'est pas une discipline qui idéalise les réalités pratiques au point d'en être déconnectée, sa vocation est plutôt de les inspirer. Ainsi en va-t-il du droit, comme l'illustre la clause de Martens du préambule des conventions de la Haye de 1899 et 1907. Cette dernière mentionne qu'en temps de guerre les belligérants doivent respecter notamment « *les exigences de la conscience publique* ». Le droit, inspiré par de fortes convictions éthiques préalables, régule ainsi concrètement la conduite dans la guerre. Les tribunaux seront ainsi « armés » pour rendre justice<sup>4</sup> après

les hostilités. Inspiré par ces convictions, le droit viendra sanctionner ce que l'éthique ne pouvait que défendre.

Si le non-respect ponctuel des principes éthiques et juridiques ne doit pas ébranler la conviction qu'il est possible d'humaniser la guerre, c'est aussi en raison de la finalité même de celle-ci. En effet, la guerre n'a pas vocation de durer, au contraire de la paix qu'elle est censée assurer. La tradition éthique dite « de la Guerre Juste » complète aujourd'hui utilement le *Jus in Bello*, c'est-à-dire le droit durant la guerre, d'un *Jus post Bellum*, c'est-à-dire le droit après la guerre. Le discours prononcé à l'ONU le 14 février 2003 par le ministre des Affaires étrangères français, Dominique de Villepin, pour s'opposer au déclenchement de la guerre en Irak, illustre notamment ce lien : « *N'oublions pas qu'après avoir gagné la guerre, il faut construire la paix*<sup>5</sup> ». S'il est nécessaire de prendre garde à la conformité éthique des moyens que l'on déploie même en temps de guerre, et à la manière dont on usera de ces moyens, c'est bien en raison de l'exigence d'assurer une paix durable par la suite.

Pour gagner une guerre, il ne suffit pas d'une victoire militaire, fût-elle écrasante, mais aussi un traité de paix équitable. Les conditions du traité de Versailles conjuguées à la crise économique de 1929 entre autres ont déclenché en Allemagne une volonté de revanche qui suscitera la Seconde Guerre mondiale. Cet exemple de non-considération du *Jus Post Bellum* ayant pour conséquence un échec pour la paix 20 ans plus tard à peine est à comparer avec les résultats du plan Marshall de 1947, qui fut préféré au plan Morgenthau, car il favorisait la reprise économique. Pourtant, ce plan supposait que même les perdants, les ennemis, le camp des combattants injustes en somme, bénéficient de ces aides économiques à la reconstruction. L'exigence éthique d'assurer la paix a surpassé la justice purement rétributive de la loi du talion, « œil pour œil, dent pour dent », pour un résultat bien supérieur. Le plan Morgenthau proposait lui que l'Allemagne soit privée de ses industries et paye des réparations aux vainqueurs. Pour comprendre ce que cela aurait représenté et pour l'anecdote historique, il est bon de savoir que cela fera bientôt neuf ans seulement que l'Allemagne a officiellement terminé de payer les réparations liées au traité de Versailles<sup>6</sup>.

Si donc comme le disait Clausewitz « *la guerre est la continuité de la politique par d'autres moyens*<sup>7</sup> », la politique

(1) Royal (B.), 2008, *La conviction d'humanité, l'éthique du soldat français*, Economica, p. 24.

(2) Voir notamment l'article 36 du premier protocole additionnel aux conventions de Genève sur les armes nouvelles.

(3) Convention on Conventional Weapon, qui a notamment interdit le recours aux lasers aveuglants.

(4) Autant que possible, même si parfois des décennies après.

(5) Extrait du discours prononcé le 14 février 2003.

(6) An. « Dimanche, l'Allemagne aura fini de payer les réparations de la Première Guerre mondiale », in *Libération*, 29 septembre 2010.

doit continuer pendant et après la guerre et cette dernière ne doit pas être considérée isolément. Un des réquisits éthiques est donc de chercher à sortir du conflit, alors même qu'il est en cours. Par ailleurs, la fin des hostilités est un désir partagé par les dirigeants, les civils, et même souvent les combattants eux-mêmes. L'opinion de chacun ne diffère que sur la manière dont l'on pourrait obtenir ce résultat. N'importe quelle technologie, même la plus innovante, ne changerait pas grand-chose à ce constat.

## Comment les nouvelles technologies pourraient-elles menacer l'éthique ?

Étant à présent entendu que l'éthique militaire et ses exigences ne se limitent pas au temps de guerre proprement dit, ni aux seuls militaires, et qu'il est à la fois possible, nécessaire et judicieux de respecter ses contraintes pour une paix plus stable, la meilleure guerre étant celle que l'on ne doit pas mener, que dire de l'automatisation, de l'autonomie, de l'emploi de l'IA, et du *Big Data*, lorsqu'ils sont déployés en contexte militaire ? Rappelons que les principes éthiques eux-mêmes ne seront jamais modifiés par les nouvelles technologies, mais ces innovations peuvent les menacer d'une façon potentiellement différente qu'autrefois. Ce seront donc aux doctrines d'usages des nouvelles technologies à se conformer à l'éthique, non l'inverse. Autrement, cela constituerait un recul du progrès des droits humains.

Quelles seraient donc les grandes menaces que font peser l'automatisation, l'autonomie, le *Big Data* et l'IA sur le respect de l'éthique ? Pour les quatre, la menace serait d'autant plus grave

qu'elles seraient utilisées pour déclencher des capacités létales. D'une manière générale, le premier point, commun au *Jus in Bello* et au droit, pour déterminer la correspondance d'une technologie avec les contraintes de la théorie de la guerre juste et du DIH, consistera à vérifier le respect de deux critères traditionnels : la discrimination<sup>8</sup> et la proportionnalité<sup>9</sup>. En tous les cas, si ces systèmes commettaient des erreurs de ciblage et tuaient non pas des combattants mais des civils, il serait certain que le principe de discrimination serait violé. Quant au deuxième critère, si ces systèmes tuaient des civils non pas en raison d'une erreur de ciblage, mais d'une force de frappe trop importante, et que les dommages collatéraux s'accumulaient, on pourrait se demander si le système ne contreviendrait pas à l'exigence de proportionnalité. Ce ne sont à ce stade que des hypothèses. Le respect de ces critères seuls ne sera néanmoins pas libérateur du respect d'autres enjeux éthiques.

### L'automatisation et l'autonomie

L'automatisation, comme le déclenchement d'une mine par exemple, pose déjà un problème éthique, car la réaction de l'engin ne fait pas la distinction entre un civil ou un ennemi. Pour tenter de préserver le respect du principe éthique de distinction entre combattants et non-combattants (protégés par le DIH<sup>10</sup>), on peut ainsi délimiter clairement la zone pour prévenir les civils de ne pas s'approcher, instaurer un barrage, etc. La limite géographique peut être posée pour protéger le civil des mines. Rappelons que seules les mines anti-véhicules sont aujourd'hui autorisées, les mines anti-personnel étant prohibées par la convention d'Ottawa de 1997. L'autonomie d'un engin se distingue de l'automatique en ce qu'elle nécessite

SI DONC COMME LE DISAIT  
CLAUSEWITZ « LA GUERRE EST LA  
CONTINUITÉ DE LA POLITIQUE PAR  
D'AUTRES MOYENS », LA POLITIQUE  
DOIT CONTINUER PENDANT  
ET APRÈS LA GUERRE ET CETTE  
DERNIÈRE NE DOIT PAS ÊTRE  
CONSIDÉRÉE ISOLÉMENT. UN DES  
RÉQUISITS ÉTHIQUES EST DONC DE  
CHERCHER À SORTIR DU CONFLIT,  
ALORS MÊME QU'IL EST EN COURS.

(7) Clausewitz (C.), 1999, *De la Guerre* (1832), trad. L.Murawiec, édition Librairie Académique Perrin, p. 46.

(8) Distinguer un combattant d'un civil.

(9) Faire usage d'une force proportionnée à l'objectif à atteindre, afin de ne pas causer de torts excessifs. Cela suppose de respecter les civils, mais aussi autant que possible leurs biens, donc de ne cibler que des objectifs militaires, etc.

(10) Droit international humanitaire. Voir l'article 48 du premier protocole additionnel aux conventions de Genève relatif à la discrimination entre civils et combattants, et l'article 50 qui suit, définissant le civil comme n'étant pas un combattant.

un traitement informatique des données reçues par son ou ses capteurs avant de déclencher une réponse, qui peut être variable. Ce traitement informatique, s'il ne fait pas intervenir un opérateur pour s'effectuer, peut mériter l'appellation « autonome » pour réaliser une tâche bien précise. Si les tâches dont il est chargé incluent l'usage d'une arme, le danger, pour l'éthique, inclut le risque précédent de non-discrimination, si le programme n'est pas capable de vérifier s'il a affaire à un combattant ou non.

Quel serait le risque d'un tir de riposte automatique ? « *Si une riposte automatique était installée, le temps de son efficacité tactique serait limité. La contre-mesure probablement adoptée par l'adversaire ne sera pas l'abandon de la lutte armée, mais l'adoption de dispositifs moins dangereux pour le sniper, et plus meurtriers pour la patrouille : poses de mines, jets de grenades, etc. À terme, le résultat du tir automatique serait un accroissement de la violence, sans gain positif en faveur du rétablissement de la paix.*<sup>11</sup> »

## Les SALA et les drones

Si les armes dont est équipé le robot ont la capacité de tuer, ce type de système peut porter l'acronyme de SALA, pour « systèmes d'armes létales autonomes ». Dans leur acronyme, le système n'est pas forcément un UAV, *Unmanned aerial Vehicle*, autrement dit un drone. C'est la capacité d'autonomie pour déclencher le tir qui qualifie le SALA, pas sa capacité à voler ou non. Le débat fait rage pour déterminer si ces systèmes existent déjà, pour la bonne raison qu'en l'absence de consensus juridique sur leur définition, la question demeure ouverte. Plusieurs modèles actuellement existants pourraient être concernés par la future définition des LAWS, *Letal Autonomous Weapons Systems*, la version anglaise de l'acronyme SALA : le système sous tourelle Phalanx, le Harpy, ou encore le robot de Samsung déployé à la frontière entre les deux Corées, SGR-A1, pour ne citer qu'eux. La CCW étudie la conformité de ces systèmes aux principes du DIH, notamment avec la clause de Martens, tandis que certains *lobbys* et ONG comme Human Right Watch, Stop Killer Robot ou encore PAX appellent à un moratoire préventif sur ce type de systèmes. En effet, si d'aucuns affirment qu'à ce jour il n'existe pas de système actuellement utilisé sur un champ de bataille qui pourrait à la fois cibler et tirer sans l'intervention d'un humain, d'autres travaillent sur des solutions techniques qui pourraient le permettre. Ainsi par exemple, ALX Système, une société belge qui a notamment emporté le dernier NATO innovation

challenge pour une solution d'interception de drones<sup>12</sup>, a doté ses appareils d'un système de reconnaissance de formes qui identifie les humains en temps réel sur la vidéo du moniteur. Avec deux autres firmes belges, ils travaillent aujourd'hui avec General Atomics<sup>13</sup>, le constructeur du drone Predator.

Pourtant, nous l'avons dit, le SALA n'est pas forcément un drone. Mais la capacité d'autonomie du tir pourrait s'ajouter aux autres dangers éthiques du drone. Car les risques spécifiques à l'emploi de capacités létales par des drones, même téléopérés, existent, le philosophe Grégoire Chamayou en a abondamment traité dans *Théorie du Drone*. Nous ne prétendons pas être exhaustifs, mais citons notamment la non-proportionnalité des missiles utilisés compte tenu de la cible à atteindre, la juste comparaison devant être faite entre l'usage d'un drone ou une action au sol, plutôt qu'avec le recours à un bombardier B-17. Citons aussi l'inégalité des chances entre les combattants, qui remet en question l'affirmation de Puffendorf selon laquelle le droit de tuer à la guerre n'existe que sur le fondement de la réciprocité de ce droit. Un autre risque est de tirer en dehors d'un engagement préalable, l'usage de la force militaire ressemblant alors plus pour certains à une exécution sans procès. En effet, et cette difficulté sera partagée par les SALA, il faudra rassembler des indices en amont pour déterminer qui peut être une cible légitime ou non, sans que la future victime puisse se défendre de l'accusation d'être un terroriste. Des problèmes légaux supplémentaires peuvent être liés à la manière dont sont utilisés les drones et non pas à leur technologie, songeons notamment à des tirs de drones réalisés sur le territoire de pays avec lesquels les USA ne sont pas en guerre, comme le Pakistan ou le Yémen. Ce problème juridique n'est pas spécifique à la technologie utilisée par les drones mais s'y additionne. Ceci tend à montrer qu'une fois la possibilité technique à disposition, les contraintes juridiques sont parfois « oubliées » par le détenteur de leur pouvoir. Tel l'anneau qui rend invisible, son porteur<sup>14</sup> pousse ce dernier à croire son impunité certaine. Pour éviter cet écueil, il peut être bon de réfléchir en amont aux risques éthiques avant de donner un outil « trop tentant » à disposition.

## L'autonomie et l'IA

L'autonomie, qui consiste pour le système à réagir à son environnement en se basant sur son traitement informatique sans intervention de l'utilisateur, peut

(11) In Ruffo, 2019, *Robotisation militaire : enjeux militaires, éthiques, légaux*, Economica (à paraître).

(12) <https://www.lecho.be/dossier/pme-wallonie/le-liegeois-alx-systems-seduit-l-otan-avec-ses-drones-autonomes/10095330.html>

(13) <https://www.lecho.be/actualite/archive/le-liegeois-alx-systems-retenu-par-general-atomics/10137972.html>

(14) Voir le mythe de Gygès dans *La République* de Platon.

être soit déterminée à l'avance par une programmation définie, un algorithme – qui laissera néanmoins une part d'incertitude proportionnelle à sa complexité – soit ne préciser que l'objectif à atteindre, laissant le soin à la machine de fixer elle-même les moyens d'y arriver. Cette seconde option fait appel à l'apprentissage machine. Ce type de programmation a connu des progrès spectaculaires ces dernières années, au point que certaines techniques d'apprentissage machine (supervisées ou non, par renforcement ou par *deep learning*, etc.) sont parfois confondues dans le vocable courant sous le terme générique d'IA<sup>15</sup>, d'autant plus que l'apprentissage peut combiner plusieurs de ces approches, plusieurs types d'algorithmes. Enfin, même si certains algorithmes peuvent servir de base à des applications différentes, chaque IA est destinée à une tâche précise. L'IA n'est pas toute-puissante ou omnisciente, certains confondant les pouvoirs de l'informatique avec de la magie ou l'action d'une divinité. Il n'existe donc pas une mais des IA, construites avec plus ou moins de biais cognitifs, et selon des buts socio-politiques variables. Une IA construite pour la Chine aurait ainsi tendance à moins protéger la vie privée que ne devrait le faire une IA destinée au marché européen. La conformité éthique du système dépendra de la manière dont elle aura été programmée, et de ce qu'on lui demande de faire. Au regard de l'éthique militaire, une IA en tant que telle n'est donc pas une technologie *mala in se*. Par exemple, la reconnaissance de formes, telles que les humains, pour secourir plus rapidement des survivants dans une zone sinistrée, peut être une bonne chose. Mais la situation est tout autre si l'on envisage un usage à finalité létale.

L'apprentissage machine nécessite à la fois une forte capacité de calcul, et beaucoup de données sur le problème à résoudre. Toutes les IA n'ont pas besoin d'être « nourries » par des données « externes », qu'elles soient réelles ou simulées, certaines peuvent « produire » les données dont elles auront besoin pour apprendre, par exemple par *Self Learning*. Ainsi pour le jeu de Go, la différence entre l'IA AlphaGo et la version AlphaGo zero, est que la seconde a seulement reçu les règles du jeu, et a appris en jouant contre elle-même, tandis que la première avait reçu des données de parties jouées entre des humains. Si, comme c'est probable dans le domaine militaire, les données nécessaires à l'apprentissage machine n'étaient pas disponibles et qu'il devenait nécessaire de se rabattre sur l'option des données simulées, la fiabilité du résultat

ne serait pas garantie. Si, à l'inverse, les données sont collectées sur le terrain, il faudra en réalité beaucoup de travail d'analyse de la part des humains pour « nettoyer » ces données avant que la machine ne devienne capable de les traiter seule, une fois qu'elle aura été entraînée avec ces données « propres ». C'est en effet une évidence que la qualité d'un système informatique soit tributaire des données sur base à partir desquelles il fonctionne.

Enfin, l'emploi de l'apprentissage machine peut potentiellement laisser dans la « black box », autrement dit dans l'opacité, la manière dont la machine a procédé à sa décision. Une telle contrainte technique est en soi une porte ouverte à toutes les déviations éthiques. Certains pourraient être tentés d'arguer que ce qui ne peut être expliqué ne doit pas être justifié, et passer ainsi sous silence des actions illégales. Cependant, certaines solutions techniques existent pour tenter d'augmenter la confiance que l'on peut accorder aux décisions de la machine. Ainsi, pour la reconnaissance d'image, certaines IA peuvent indiquer les zones de l'image qui ont été prises en compte pour déterminer son étiquetage. Loin d'évacuer l'humain, ce dernier est réintégré pour valider la décision de la machine. Ceci peut s'avérer utile pour des raisons de sécurité, et plus encore pour lutter contre le piratage. En effet, dans une *adversarial attack*<sup>16</sup> par exemple, une image peut contenir des pixels destinés à tromper le système de reconnaissance, même si à l'œil nu l'image semble normale. Si l'IA devait être utilisée pour prendre des décisions en matière militaire et plus encore pour cibler et déclencher des tirs, elle ne devrait pas être séparée d'une supervision humaine non seulement pour des raisons éthiques que nous allons approfondir, mais aussi pour des questions de sécurité, de résistance du système aux attaques informatiques qui ne manqueront pas d'arriver.

Cela peut s'avérer utile de développer des IA pour des capacités de cyberdéfense, d'empêcher des attaques, de créer des moyens de rendre des IA hostiles inutilisables. Autrement dit, l'IA ne doit pas être pensée comme une technologie destinée à l'attaque, mais aussi comme une capacité de défense contre des attaques informatiques, que ce soit à l'aide de virus, ou d'autres IA. En effet, se reposer sur l'informatique et sur l'apprentissage en évacuant la « sentinelle » humaine, ce serait ouvrir une vulnérabilité forte à l'intox de la machine, à son piratage, voire pire, à son détournement. Apprendre à déstabiliser

(15) Différentes définitions de l'IA existent et font débat. La définition historique donnée par le Dartmouth College est celle-ci: «to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it». Dans cet article, nous nous bornerons à considérer l'IA de la manière la plus large possible comme un ensemble de techniques de programmations, sans nous référer explicitement à sa recherche de similitude avec le raisonnement humain.

(16) Attaque contradictoire.



des IA peut, en outre, être un moyen d'en développer de plus sûres, ce qui constituerait une approche moins dangereuse pour l'éthique.

## Le Big Data et l'IA

Les données « externes » pour entraîner la machine sont aujourd'hui accessibles le plus souvent grâce au *Big Data*. Le croisement des différentes bases de données existantes donne naissance à cet ensemble massif de mégadonnées qu'il devient impossible de traiter et d'exploiter par les seules capacités humaines. La seule possibilité de stocker ces données, notamment en utilisant le *Cloud*, pose des questions techniques, voire écologiques puisque les fermes de serveurs doivent être réfrigérées, etc., partant de l'idée que le tout est plus que la somme des parties, l'espoir du *Big Data*, complémentaire de l'IA, est que de nouvelles connaissances puissent apparaître. La vision globale de l'ensemble des données connues et produites permettrait peut-être de mettre à jour des corrélations inédites, ou encore la connaissance d'une masse de données gigantesque permettrait de prendre de meilleures décisions parce que fondées sur plus d'informations, etc. Si aujourd'hui Amazon ou Microsoft, des compagnies privées qui ne vendent aucun armement, intéressent les militaires, c'est notamment pour stocker des données sur des serveurs accessibles via le *Cloud*, qui seront exploitées, traitées et utilisées pour entraîner des IA.

Ainsi, l'une des premières modifications les plus radicales provoquées par l'usage de l'IA en contexte militaire paraîtra inattendue à qui ne connaît pas le droit de la guerre : dès lors que ces entreprises privées vendent des solutions technologiques aux militaires, pour en équiper des armes ou comme simple support de leur fonctionnement, elles pourraient se voir attribuer le qualificatif de cible militaire légitime, au même titre que les usines d'armements traditionnels. Si des employés peuvent avoir conscience qu'ils deviennent des cibles militaires lorsqu'ils assemblent une bombe, en est-il de même des employés qui codent derrière un ordinateur ou veillent au bon fonctionnement d'un serveur ? L'une des exigences éthiques minimale serait donc de s'assurer du plein consentement de ces employés.

Précisons que la démission de plusieurs employés de Google pour refuser que leur entreprise développe ces technologies, en particulier le projet «Maven», n'était certes pas motivée par ce risque de devenir une cible légitime,



CELA PEUT S'AVÉRER UTILE DE DÉVELOPPER DES IA POUR DES CAPACITÉS DE CYBERDÉFENSE, D'EMPÊCHER DES ATTAQUES, DE CRÉER DES MOYENS DE RENDRE DES IA HOSTILES INUTILISABLES. AUTREMENT DIT, L'IA NE DOIT PAS ÊTRE PENSÉE COMME UNE TECHNOLOGIE DESTINÉE À L'ATTAQUE, MAIS AUSSI COMME UNE CAPACITÉ DE DÉFENSE CONTRE DES ATTAQUES INFORMATIQUES, QUE CE SOIT À L'AIDE DE VIRUS, OU D'AUTRES IA. EN EFFET, SE REPOSER SUR L'INFORMATIQUE ET SUR L'APPRENTISSAGE EN ÉVACUANT LA « SENTINELLE » HUMAINE, CE SERAIT OUVRIR UNE VULNÉRABILITÉ FORTE À L'INTOX DE LA MACHINE, À SON PIRATAGE, VOIRE PIRE, À SON DÉTOURNEMENT.



mais avant tout parce qu'ils ne désiraient pas participer à la construction d'une technologie destinée à causer des dommages à des êtres humains. Les informaticiens sont aujourd'hui de plus en plus conscients que l'usage de l'IA dans le domaine militaire, en écartant le soldat du champ de bataille au profit d'engins technologiques, a fait reculer d'autant en amont le moment de la décision humaine éthique. Pour beaucoup, la seule conscience, outre l'autorité étatique, pouvant faire barrage avant le lancement d'un système autonome létal risque d'être son concepteur.

Si en revanche les entreprises privées et leurs employés acceptent consciemment de travailler pour la Défense sur des systèmes d'armes sur lesquels les militaires n'auront pas une « supervision humaine efficace », nous nous retrouvons peut-être dans une situation similaire au déploiement de milices privées. Autrement dit, l'État se déposséderait de sa puissance de coercition au profit d'acteurs non étatiques. Est-il acceptable éthiquement de déléguer le pouvoir de tuer à des individus qui ne sont pas des soldats, mais des mercenaires, avec les conséquences que cela représente au niveau du DIH<sup>17</sup>? Nous pourrions nous demander dans quelle mesure les programmeurs

(17) Selon les conventions de Genève, les mercenaires ne bénéficient pas des protections juridiques des prisonniers de guerre par exemple. Voir la convention de Genève relative au traitement des prisonniers de guerre (Convention III du 12 août 1949), Protocole additionnel I, Titre III, [P. I, 46, 47].

d'entreprises civiles ne rencontrent pas certains aspects de la définition du mercenaire<sup>18</sup> à savoir une participation pour des motifs financiers, pour prendre part à un combat, et ne pas avoir de lien statutaire avec les parties en conflit (à déterminer selon les individus). La question est ouverte, mais permet de percevoir qu'en déléguant à la seule machine, produite par des entreprises privées, le pouvoir à la fois de sélectionner ses cibles et de tirer seule, l'État se dessaisit de son monopole de coercition légitime au profit donc des GAFAs. Devrions-nous en conclure que ces derniers, battant bientôt cryptomonnaie<sup>19</sup>, créant des solutions informatiques pour décider qui doit mourir ou non, s'arrogeant ainsi progressivement des prérogatives régaliennes, sont en passe de devenir les égaux des acteurs étatiques ? Avec quel impact pour les démocraties et les individus qui pensaient y vivre selon leurs lois ?

L'autre danger éthique de l'usage du *Big Data* et de l'IA à des fins militaires est de ne pas respecter l'un des deux principes éthiques de base, la discrimination. Si les bases de données issues de la société civile sont exploitées pour une visée militaire, on peut se demander si les civils et leurs biens, donc par extension leurs données privées, qui doivent être protégées en temps de guerre le sont encore dans la cyberguerre. En résumé, est-ce que l'utilisation des données civiles dans une IA militaire respecte le principe de discrimination ? Enfin, un autre enjeu éthique relatif au *Big Data* est le respect de la vie privée des individus, mais ceci n'est pas spécifique aux actions militaires et se poserait dans les mêmes termes pour le domaine civil.

Ainsi définis, les termes IA et *Big Data* recouvrent des techniques et des moyens divers qui pourraient donner la méta-capacité d'autonomie, différente de l'automatique, à des systèmes conçus pour accomplir certaines tâches prédéterminées. Si ces tâches incluent le ciblage et le déclenchement du tir sans intervention humaine, une ligne rouge éthique serait franchie, car il s'agirait alors de SALA. Conserver un humain dans la boucle de commandement, non seulement comme force de réaction rapide en cas d'erreur systèmes pendant son fonctionnement, mais aussi comme certification de la cible en amont, est une solution à privilégier pour continuer à développer et utiliser l'IA en minimisant les risques à la fois éthiques et sécuritaires.

## De quelques dangers éthiques supplémentaires relatifs à l'emploi de l'IA en contexte militaire

### La notion de responsabilité

Pourquoi les SALA constituent-ils une ligne rouge éthique à ne pas franchir ? Que ce soit grâce à une programmation prévue d'avance, par apprentissage machine, ou par d'autres techniques d'IA, la capacité d'autonomie, autrement dit la possibilité même que ce puisse être une « machine » plutôt qu'un homme qui puisse à la fois sélectionner une cible et déclencher un tir, engendre des difficultés, notamment l'apparente disparition d'un responsable humain puisqu'il n'y a personne derrière la gâchette. Mais cette disparition n'est qu'apparente. Dans les faits, la responsabilité se retrouve dès lors comme « diluée » dans la chaîne de commandement qui va de l'ingénieur informatique jusqu'à l'opérateur qui active le mode autonome en passant par le responsable politique qui a commandé ces armes et par les officiers qui en ont ordonné l'usage.

Des propositions pour fixer une limite à la responsabilité légale ont certes été proposées. Il en existe de trois sortes ; la première consiste pour le fabricant à se dégager de toute responsabilité dès que la livraison aura été effectuée. Ce dispositif n'est pas nouveau si on se fie à un document du ministère de la Défense anglais de 2011 relatif aux drones téléopérés : « *si la logique du processus actuel des [vols] pilotés est maintenue, les responsabilités des concepteurs auront été déchargées une fois que le système d'aéronef non habité (UAS) aura été certifié par les autorités aériennes militaires ou civiles nationales compétentes*.<sup>20</sup> ». On peut supposer que cette possibilité serait envisagée pour des systèmes d'armes létales autonomes. La deuxième consiste à tenir pour responsable celui qui active le mode autonome de la machine. C'est la solution technique proposée par le roboticien Ronald Arkin avec le quatrième module de son « gouverneur éthique », permettant d'identifier celui qui a allumé le robot. La troisième propose que la responsabilité juridique appartienne au robot lui-même. Cette approche nécessite de créer une fiction juridique, la « personnalité électronique ». Le rapport de l'eurodéputée Mady Delvaux allait dans ce sens en 2017, même si la proposition fut

(18) Voir Tercinet (J.), 1977, « Les mercenaires et le Droit international », *Annuaire français de droit international*, volume 23, p. 269-293.

(19) Facebook lancera bientôt sa monnaie, la Libra. Précisons que certains auteurs libéraux n'assimilent pas la monnaie à une prérogative régalienn.

(20) Ministry of Defense, «The UK approach to unmanned aircraft system», *Joint doctrine Note 2/11*, 30 mars 2011, p 5-6.

critiquée notamment par Nathalie Nevejans<sup>21</sup>. Cependant, quelles que soient les critiques que l'on puisse adresser à chacune de ces trois approches, elles ne sont relatives qu'à l'aspect légal de la responsabilité, laissant de côté l'existence de la responsabilité morale.

Cette apparente dilution de la responsabilité morale le long de la chaîne de commandement ne doit pas être perçue comme une « évaporation » de celle-ci, mais bien plutôt comme une teinture tenace, qui se répandrait sur tout ce qui entre en contact avec elle. En cas de morts involontaires provoquées par la machine, est-ce que les solutions légales énoncées plus haut satisfèraient les familles de victimes ? Peut-être leur verserait-on des indemnités, mais la demande de justice ne serait-elle qu'une question d'argent ? Sans humain pour endosser la responsabilité, quelle place y aurait-il pour que les familles entendent des remords, des excuses, souvent psychologiquement plus cruciales à entendre que la condamnation ? Quelle place pour le pardon ou l'oubli, si nécessaires dans le *Jus Post Bellum* ? Sans humain pour combattre, il n'y aura pas d'homme pour faire la paix.

## Le Targetting killing

L'emploi des drones présentait un second inconvénient qui risque d'être partagé avec l'usage de l'IA, le *targetting killing*. S'il s'agit d'une guerre asymétrique, déterminer si une personne appartient à un réseau terroriste ou non semble plus complexe que d'observer la couleur des uniformes ennemis avant de tirer, comme au temps des guerres napoléoniennes. Il y a fort à parier que l'IA sera utilisée pour traiter des informations afin de se renseigner *a priori* sur la future cible. On peut être dès lors inquiet de la sélection des futurs critères qui qualifieront une cible. Le cas de l'algorithme *Skynet* de la NSA pose question à ce sujet<sup>22</sup>. Edward Snowden a révélé que la NSA utilisait cet algorithme d'apprentissage au Pakistan. Utilisant les données téléphoniques et le *Big Data*, il est destiné à repérer des terroristes à partir d'un *pattern* de comportements. S'il est difficile de ne pas se voir accorder un crédit par un algorithme parce qu'une variable de notre dossier fait chuter notre « cotation », que dire de la fixation d'une « note » et d'un seuil critique, équivalent pour l'individu à un arrêt de mort, décrété par une machine, sur base de lois statistiques ? Encore faut-il avoir confiance dans

la programmation de l'algorithme. En ce qui concerne *Skynet*, le directeur de Human Right Data Analysis Group, Patrick Ball, a pour sa part, «*described the NSA's methods as "ridiculously optimistic" and "completely bullshit"*»<sup>23</sup>. Outre les biais cognitifs que l'on peut craindre dans n'importe quel algorithme, il existera aussi toujours des cas particuliers. Ainsi, un journaliste d'Al Jazeera a été étiqueté par erreur par le programme de la NSA comme étant un terroriste.

Ce cas ne sera sans doute pas unique, en effet les algorithmes sont confrontés à un écueil mathématique, soit ils seront programmés pour sélectionner un ensemble ne contenant que des terroristes potentiels, et certains passeront inévitablement hors du filet, soit ils seront programmés pour n'en manquer aucun, et dans ce cas ils engloberont inévitablement des innocents, ce que l'on appelle autrement des « faux positifs ». Face à un tel dilemme, il serait bon que l'humain demeure l'expert qui vérifiera les critères de « tri », et fera la distinction finale pour épargner les innocents, à la fois *a priori* dans l'établissement d'une *black list*, mais aussi au moment de presser la gâchette s'il s'agit de reconnaissance de forme. Cependant, même cette garantie n'est pas certaine si l'humain fait trop confiance à la machine – en raison peut-être d'un complexe d'infériorité vis-à-vis de ces capacités de calcul. L'exemple réel du journaliste d'Al Jazeera nous enseigne une chose ; laissé seul, un algorithme proposera certainement des faux positifs, mais le danger le plus inquiétant est que l'humain ayant rapporté ce cas l'ait présenté comme un succès de la machine. Nous trouvons donc deux dangers : laisser la machine décider seule, ou oublier que notre rôle n'est pas de la croire mais de vérifier ce qu'elle nous dit, au risque sinon de revenir au premier cas de figure. La supervision humaine efficace nécessite que nous fassions usage de notre capacité critique, plus que jamais.

## La décision stratégique

Quel pourrait être un très mauvais usage de l'IA ? Laisser une intelligence artificielle décider du futur déclenchement des conflits. Certains auteurs ont étudié l'histoire pour tenter de déterminer la probabilité d'une guerre. Ainsi, Graham Allison, inspiré par ce qu'il appelle le « piège de Thucydide<sup>24</sup> », étudie la probabilité d'une guerre entre la Chine et les USA. Son étude portait sur seize cas historiques similaires antérieurs où la montée d'une

(21) Nevejans (N.), 2016, *Traité de droit et d'éthique de la robotique civile*, LEH édition, Bordeaux, Coll. « Science, éthique et société », préfaces J. Hauser et J.-G. Ganascia, décembre.

(22) Cet algorithme ne semble pas non plus unique en son genre, on cite également le cas de « MonsterMind ».

(23) Grothoff (C.), Porup (J.M.), 2016, « The NSA's SKYNET program may be killing thousands of innocent people », *Arstechnica*, 16 février.

(24) Graham (A.), 2019, *Vers la guerre, la chine et l'Amérique dans le piège de Thucydide ?*, Paris, éditions Odile Jacob.

nouvelle puissance faisait peur à la puissance établie au point de rendre la guerre inévitable. Mais Graham n'a pas l'intention d'utiliser ces connaissances pour programmer une IA. Le faible nombre de données, seize cas, serait insuffisant pour entraîner l'apprentissage d'une IA. Ceux qui possèdent un minimum de connaissances statistiques savent qu'il s'agit d'un échantillon trop petit pour être représentatif. Le risque serait de décider de se fonder malgré tout sur ces seuls cas pour programmer un algorithme, voire les compléter par des données simulées, dont la fiabilité peut être interrogée. L'opacité en outre des procédés soit pour des raisons de fonctionnement mathématiques, soit pour des raisons de secret-défense, qui auront mené à ces résultats, pose de graves questions éthiques et démocratiques. Treize des seize cas ayant résulté en une guerre entre les deux puissances, un algorithme programmé sur ces données déciderait inévitablement de déclencher une guerre lui aussi. Ceci contreviendrait à deux autres principes issus du *Jus ad Bellum*, à savoir ne déclencher une guerre qu'en dernier recours et seulement par une autorité compétente. Imaginer un jour qu'un algorithme puisse décider seul de déclencher une guerre serait une absurdité éthique, politique, démocratique et diplomatique.

Et pourtant, il existe déjà des logiciels destinés à aider à la décision stratégique en situation d'incertitude. Si l'on compare certaines actions à la guerre comme des « coups de poker », l'expression risquerait bien de décrire le futur de la réflexion stratégique. En effet, il existe différentes IA capables de jouer au poker<sup>25</sup>, donc de bluffer les humains, et les plus avancées comme *Pluribus* gagnent même dans des parties à 6 joueurs. « L'ancêtre » de *Pluribus*, l'IA *Libratus*, a été vendue à l'armée américaine pour 10 millions de dollars<sup>26</sup>. L'objectif déclaré étant bien d'aider à la décision stratégique. Même en conservant une supervision humaine, de tels systèmes ne devraient être manipulés qu'avec précaution si l'on veut laisser une chance à la paix et aux manœuvres diplomatiques.

Si le risque de laisser un logiciel décider seul de tirer et de cibler posait des questions éthiques, le type d'arme qui pourrait être lancé n'avait pas été spécifiquement abordé. Or, depuis la création de missiles hypersoniques dotés de capacités nucléaires, il semble que l'emploi d'une IA

autonome pour décider du tir nucléaire soit sérieusement envisagé par les USA. « *Sur le terrain, elle devrait essentiellement tourner autour de l'arrimage à l'intelligence artificielle du macro-système NC3. [...] on imagine que l'entrée en scène de l'intelligence artificielle devrait mettre de côté les intervenants du centre de contrôle commande que sont le président des États-Unis et l'Autorité de commandement national*<sup>27</sup> ». Selon ce scénario, on confierait donc les codes nucléaires à une IA.

Certains affirmeront que la sécurité en serait augmentée, car cela minimiserait les risques de perte des codes par la distraction tout humaine des présidents<sup>28</sup>. D'autres affirmeront qu'il s'agit d'une nécessité pour répondre plus vite encore aux attaques, car le temps de réponse est réduit, et d'assurer ainsi la possibilité de la « seconde frappe ». Quelques autres rappelleront un précédent historique qui aurait pu rester inconnu de tous, à savoir la décision du lieutenant-colonel Stanislav Petrov d'aller à l'encontre du système d'alerte Oko. « *“J'ai eu une drôle de sensation dans le ventre.” C'est par ces mots que Stanislav Petrov explique au Washington Post, en 1999, comment il a décidé de ne rien faire ce 26 septembre 1983, alors que les écrans de contrôle d'un bunker secret près de Moscou, indiquent que cinq missiles américains foncent sur l'URSS*<sup>29</sup> ». Ignorant l'alarme déclenchée par Oko, Stanislav Petrov a douté de son exactitude et s'est ainsi abstenu de déclencher la Troisième Guerre mondiale. L'alarme n'était due qu'à une erreur technique : « *Le système de surveillance a mal interprété la réflexion des rayons du soleil sur les nuages, confondue avec le dégagement d'énergie des missiles au décollage*<sup>30</sup> ». Bien entendu, le faible nombre de missiles a fait douter Petrov, mais ce qu'il faut pointer, ce sont les raisons pour lesquelles il a pu douter. « *C'est une chance que ce soit lui, qui a étudié l'ingénierie à Kïev, à l'École supérieure de radiotechnique des forces armées soviétiques, de service ce soir-là. “Mes collègues étaient des soldats professionnels, on leur a appris à obéir et appliquer les ordres.” Ils n'auraient peut-être pas soupçonné comme lui, une erreur technique.*<sup>31</sup> ».

Ce que nous enseignent ces différents exemples, c'est que la machine peut faire des erreurs, pour des raisons techniques ou autres. L'humain ne doit pas la croire ou lui faire confiance, mais il doit la superviser, ce qui ne sera possible que si l'humain en question est capable de douter du bon fonctionnement de la machine et des résultats qu'elle lui propose, mais ne doit jamais lui imposer. Ceci

(25) DeepStack, *Libratus* et *Pluribus* notamment.

(26) <https://www.androidpit.fr/libratus-le-joueur-de-poker-recrutement-armee-americaine>

(27) <https://intelligence-artificielle.developpez.com/actu/275940/Des-experts-US-proposent-de-placer-l-arsenal-nucleaire-du-pays-sous-le-contrôle-d-une-IA-pour-pouvoir-contrer-carrer-d-éventuelles-attaques-de-la-Russie-ou-de-la-Chine/>

(28) <http://www.lefigaro.fr/international/2010/10/22/01003-20101022ARTFIG00397-comment-bill-clinton-a-egare-les-codes-nucleaires.php>

(29) <https://www.ouest-france.fr/leditiondusoir/data/8962/reader/reader.html#!preferred/1/package/8962/pub/12486/page/5>

(30) *Idem*.

(31) *Idem*.

n'est possible qu'en joignant à une solide formation éthique du soldat et de l'officier une compréhension fine du fonctionnement et des capacités des logiciels qui doivent le guider. La capacité de douter n'est pas naturelle, elle doit s'apprendre et s'appuyer sur une connaissance technique et éthique. La supervision humaine, pour être efficace, nécessite plus que jamais un esprit critique. L'IA ne saurait être la canne blanche d'un aveugle dans le brouillard de la guerre, ou bien si précisément, l'outil ne pourra jamais donner la vue ni la direction à suivre, et celui qui s'accrocherait à la canne blanche, pensant ainsi voir, risque de le découvrir à ses dépens.

L'IA ne devrait pas être utilisée pour écarter la réflexion de l'humain, comme si après avoir été écarté le soldat du champ de bataille on écartait désormais l'analyste du renseignement et le général de la réflexion stratégique. Outre qu'ils doivent être ceux qui devront répondre, ce qui est à l'origine du mot responsabilité, leurs capacités propres de perception, d'imagination, de résistance à l'inattendu, de créativité, de surprise seront d'autant plus des atouts dans des guerres futures qu'elles seraient menées par des machines qui apprendraient de nos mouvements prévisibles.

### **Dystopie : Si les IA équipaient les SALA**

Ironiquement, si l'IA équipait demain des SALA, l'argumentaire de vente pourrait se résumer ainsi : « Il s'agit d'une arme écologique puisqu'elle est dotée d'un système de reconnaissance des humains, ce qui protège la nature. Elle est proportionnée, car vous pourrez vous emparer d'une ville en laissant les infrastructures intactes, seule la population est touchée. Vous ne trouverez ni résistance ni risque. Le système détermine lui-même la ville dotée de la plus haute importance stratégique et il ne vous faudra attendre que le temps nécessaire pour que les munitions de l'essai de SALA se vident. ». Certes personne n'est assez cynique, mais le risque que l'efficacité des SALA en fasse des armes de destructions massives est réel.

Cette efficacité potentielle de l'IA incite aujourd'hui les états à opérer une course à l'IA qui n'est pas sans rappeler la course à l'armement. Quand nous nous demandons si nous avons le choix de faire usage de l'IA, c'est bien parce que certains craignent que ne pas en disposer nous placerait en position de faiblesse. C'est la stratégie de la dissuasion qui refait surface. Mais les programmes informatiques se piratent, se copient, la prolifération des IA permettant d'équiper des SALA sera beaucoup plus rapide que celle des bombes nucléaires. Sous la menace de ces acteurs imprévisibles qui se dotent d'IA, qui dit que la tentation de mener des attaques préventives ne se



CETTE EFFICACITÉ POTENTIELLE DE L'IA INCITE AUJOURD'HUI LES ÉTATS À OPÉRER UNE COURSE À L'IA QUI N'EST PAS SANS RAPPELER LA COURSE À L'ARMEMENT. QUAND NOUS NOUS DEMANDONS SI NOUS AVONS LE CHOIX DE FAIRE USAGE DE L'IA, C'EST BIEN PARCE QUE CERTAINS CRAIGNENT QUE NE PAS EN DISPOSER NOUS PLACERAIT EN POSITION DE FAIBLESSE. C'EST LA STRATÉGIE DE LA DISSUASION QUI REFAIT SURFACE.



fera pas plus forte ? Et si une nation décide de lancer une de ces attaques, est-ce que le concept de guerre totale ne surgirait pas à son tour, parce que la machine ne connaît pas de repos et qu'elle aura la capacité de tirer jusqu'à l'extermination totale de l'espèce humaine ? Même si l'IA n'était pas reliée aux bombes nucléaires, son emploi pour déclencher des capacités létales en ferait une arme de destruction massive.

### **Conclusion**

Si le drone était une technologie qui semblait donner un avantage dans les guerres asymétriques, l'IA est développée en prévision du retour d'une guerre plus traditionnelle, entre deux nations. L'IA n'est pas une technologie *mala in se*, pour autant qu'elle ne serve pas l'autonomie du tir, autrement dit qu'elle ne décide pas seule de cibler et de tirer, afin qu'elle ne serve pas la construction des SALA. Les possibilités d'emploi de l'IA dans le domaine militaire sont si vastes que nous y retrouvons dans un cocktail détonnant tous les problèmes de la course à l'armement, de la prolifération, de la dissuasion (donc le risque d'à nouveau user de l'arme nucléaire), de la guerre totale, des attaques préventives, des armes de destruction massive, mais aussi, on l'a vu, des milices privées. Nous nous retrouvons dans une situation dans laquelle l'IA en semblant concentrer le savoir grâce aux *Big Data* et à ses capacités de calcul impressionnantes semble concentrer en même temps la résurgence d'une bonne part des dangers des guerres modernes. Enfin, si l'on tire les leçons du développement des drones, on peut constater que des technologies produites par l'armée deviennent par la suite disponibles dans le monde civil. Elles peuvent

ensuite être détournées, à bas coût tout d'abord, puis avec une sophistication croissante. Le raid de drones des Yéménites sur les réserves de pétrole en Arabie saoudite en est un exemple<sup>32</sup>. N'oublions donc jamais que tout ce que nous développons, d'autres s'en empareront. Assurons-nous auparavant de ne développer que des systèmes en adéquation avec les règles avec lesquelles nous souhaiterions être combattus.

S'il est nécessaire d'assurer politiquement, éthiquement, que la paix viendra et durera, que dire à ceux qui ont à lutter concrètement ? Ceux-ci ne ressentent parfois pas l'utilité à long terme de se priver de moyens plus expéditifs – pour employer un euphémisme – au motif qu'ils sont in-éthiques. Si l'envie de se battre avec la même férocité que le camp d'en face fait rage dans le cœur de certains combattants, ce qui se comprend aisément, c'est précisément parce que ce manque de respect des règles semble crier vengeance, peut-être davantage encore dans des âmes pétries d'idéaux de justice que d'autres. Si ce mécanisme psychologique est connu, il masque une conséquence logique : ne pas respecter les règles éthico-juridiques existantes revient en somme à ne pas avoir de standard éthique plus élevé que ceux des terroristes, autrement dit à se conduire comme eux et à vouloir provoquer à son tour les actes qui sont précisément à l'origine de cette révolte de l'être. Le philosophe Nietzsche résumait ainsi ce risque : « *Celui qui combat des monstres doit prendre garde à ne pas devenir monstre lui-même*<sup>33</sup> ». Si dans la fiction certains personnages semblent assumer qu'il faille « être un monstre pour combattre des monstres », conduisant à une surenchère de violence dans les films d'action, telle n'est pas la voie de l'éthique militaire, dont le principe général pourrait être résumé par une volonté de « diminuer la violence », au sens étymologique du terme latin *violare*, ou « dépasser les limites ». Le soldat n'a

ainsi pas vocation à être cruel, mais à maîtriser sa force pour respecter ces limites. Le droit français<sup>34</sup> fait appel à la responsabilité du militaire, tant dans son obéissance aux ordres que dans l'exercice du commandement. Tout militaire devrait désobéir à l'ordre qu'il aurait reçu de perpétrer ce qui serait un crime contre l'humanité, et aucun ne devrait jamais en donner un de la sorte. Nous l'avons rappelé, il existe dans le droit certaines restrictions à l'usage de la force, même par des militaires en temps de guerre. Elles sont issues de convictions éthiques préalables à l'établissement de cette norme. Le soldat démocratique se doit de combattre non seulement en se contentant de ne pas violer le droit, mais en adéquation avec le respect des convictions éthiques. Cette injonction exigeante n'en est pas moins réaliste, en témoigne ce militaire engagé en Somalie : « [...] *il nous restera surtout la légitime fierté d'avoir combattu en homme et non en bête, avec discernement et sans haine, contre des gens qui pourtant ne nous aimaient guère* [...] »<sup>35</sup>. L'enjeu éthique du soldat se pose donc à lui-même, l'engage à la première personne, pour lui seul, dans la solitude de sa conscience. La question éthique ne se résume donc pas au respect du droit, du permis ou du défendu, mais englobe la totalité de l'individu. Quels que soient les moyens mis à sa disposition, dans l'usage qu'il en fait ou qui lui est demandé, respecte-t-il son humanité, ses convictions démocratiques, le sens de son engagement ? Tôt ou tard, il devra répondre de l'usage de la force qui lui a été confiée, car au contraire de l'IA, lui n'est heureusement pas une machine. Alors, avons-nous le choix d'utiliser l'IA en temps de guerre ? Nous devons toujours préserver qu'il puisse y avoir un choix, pour préserver l'humanité avant, pendant, et après la guerre ■

## Bibliographie

### Ouvrages

ROYAL (B.), 2008, *La conviction d'humanité, l'éthique du soldat français*, Paris, Economica, 2008..

Coll., CEULEMANS (C.), DEWYN (D.), LAMBERT (D.), RUFFO (M.d.N.), WARNOTTE (P), *Robotisation militaire : enjeux militaires, éthiques, légaux*, Paris, Economica, 2019. (à paraître).

CICR, 1907, *Convention (IV) concernant les lois et coutumes de la guerre sur terre et son Annexe : règlement concernant les lois et coutumes de la guerre sur terre*, 18 octobre 1907.

CICR, 1977, *Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux, Protocole I*, 8 juin 1977.

(32) <https://www.lesoir.be/247832/article/2019-09-16/attaque-de-drones-contre-larabie-saoudite-le-prix-du-petrole-senvole-les-etats>

(33) Nietzsche (F.), 1971, *Par-delà Bien et Mal*, trad. C. Heim, aphorisme 146, Paris, Gallimard,.

(34) Article 8 du statut général des militaires.

(35) Royal (B.), *op. cit.*, p 33

CICR, 2006, *Guide de l'examen de la licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre.*, Mise en œuvre des dispositions de l'article 36 du protocole additionnel 1 de 1977, Comité international de la Croix Rouge, 2006.

CLAUSEWITZ (C.), 1999, *De la Guerre* (1832), trad. L.Murawiec, édition Librairie Académique Perrin., 1999

GRAHAM (A.), 2019, *Vers la guerre, la chine et l'Amérique dans le piège de Thucydide ?*, Paris, éditions Odile Jacob, 2019.

GROTHOFF (C.), PORUP (J.M.), 2016, «The NSA's SKYNET program may be killing thousands of innocent people», *Arstechnica*, 16 février 2016.

MINISTRY OF DEFENSE, 2011, «The UK approach to unmanned aircraft system», *Joint doctrine Note 2/11*, 30 mars. 2011

NEVEJEANS (N.), 2016, *Traité de droit et d'éthique de la robotique civile*, LEH édition, Bordeaux, Coll. « Science, éthique et société », préfaces J. Hauser et J.-G. Ganascia, décembre 2016.

NIETZSCHE (F.), 1971, *Par-delà Bien et Mal*, trad. HEIM (C.), Paris, Gallimard, 1971.

TERCINET (J.), 1977, « Les mercenaires et le Droit international », *Annuaire français de droit international*, volume 23, 1977.

## Articles

An., 2019, « Attaque de drones contre l'Arabie Saoudite, le prix du pétrole s'envole », *Le Soir*, 16 septembre.

An., 2010, « Dimanche, l'Allemagne aura fini de payer les réparations de la Première Guerre mondiale », *Libération*, 29 septembre.

An., 2019, « Le liégeois ALX Systems retenu par General Atomics », In *L'ÉchoÉcho*, 19 juin.

An., 2019, « Le liégeois ALX Systems séduit l'OTAN avec ses drones autonomes », *L'Écho* 11 février

MCCOURT (D.), 2019, « Libratus, l'intelligence artificielle championne de poker recrutée par le Pentagone », *Android*, 17 janvier.

RUIZ (P.), 2019, « Des experts US proposent de placer l'arsenal nucléaire du pays sous le contrôle d'une IA », *Developez.com*, 5 septembre.

VEY (I.) 2010, « Comment Bill Clinton a égaré les codes nucléaires », *Le Figaro*, 22 octobre.

MERDIGNAC (M.), 2017, « Le Russe qui a évité une guerre nucléaire est mort », *Ouest France*, 19 septembre.



# L'intelligence artificielle : vers une nouvelle grammaire internationale ?

Charles THIBOUT

Charles THIBOUT



Charles Thibout est chercheur doctorant au Centre européen de sociologie et

de science politique (Panthéon-Sorbonne, CNRS, EHESS) et chercheur associé à l'Institut de relations internationales et stratégiques (IRIS). Il collabore régulièrement avec *France Culture*, en tant que rédacteur en chef de la matinale.

Un consensus plane à la tête des principales puissances : l'intelligence artificielle serait la nouvelle « arme absolue », susceptible d'établir la suprématie de quiconque en maîtriserait les techniques les plus avancées. Les promesses portées par ce répertoire technologique en termes de productivité industrielle, de supériorité militaire, tactique et stratégique, et de régulation sociale, attisent la convoitise de la plupart des États économiquement développés. Les plans nationaux de développement de l'IA se multiplient : les

politiques de formation, de recherche-développement ou de recrutement des meilleurs ingénieurs et mathématiciens de ce domaine dessinent une nouvelle économie politique du système international, dans laquelle un ensemble de techniques fait fonction de critère discriminant, d'unité métrologique dans la hiérarchie des États – non sans quelque analogie avec les capacités nucléaires et spatiales de l'ère bipolaire.

Issu du mouvement cybernétique des années 1940 et 1950, ce répertoire de techniques fut d'abord le privilège des États-Unis, avant qu'une première forme (éphémère) de compétition n'advînt dans les années 1980, portée par les ambitions émancipatrices du vassal nippon et les derniers feux de



la puissance industrielle et technologique européenne. Porteur d'espoirs souvent déçus, l'intelligence artificielle fut des décennies durant reléguée, faute de résultats tangibles, aux abîmes de la science et de la technologie. L'IA ne réapparaîtrait sur le devant de la scène qu'au début des années 2010, revigorée par les succès d'un domaine longtemps marginalisé, l'apprentissage automatique (*machine learning*) et, à l'intérieur de celui-ci, l'« apprentissage profond » (*deep learning*). Largement médiatisés, ces progrès technologiques rencontrèrent concomitamment les ambitions éclectiques de quelques États qui, sans tarder, les placèrent au centre de leur agenda public. Pour lors, seuls la Chine et les États-Unis font figure de prétendants crédibles à l'hégémonie en IA, quoique, désormais, cette compétition technologique tend à offrir à des acteurs privés, les firmes numériques transnationales qui concentrent les innovations, les financements et les « talents » dans ce domaine, une fonction (géo) politique majeure : la fourniture de ces technologies et l'élaboration des stratégies nationales y afférentes.

## La domination historique des États-Unis

L'intérêt stratégique de l'intelligence artificielle naît précisément à New York, dans les années 1940, au sein d'un mouvement scientifique dont l'objectif était d'édifier une science générale du fonctionnement de l'esprit humain, devant permettre *in fine* la reproduction dudit esprit dans une machine. Ce mouvement, la cybernétique (*kubernètikè* = science du gouvernement), réunissait des scientifiques d'horizons divers (physiciens, mathématiciens, neurologues, économistes, psychologues...) partageant une idéologie commune, le libéralisme<sup>1</sup>, qui posèrent les fondements théoriques de ce que nous appelons aujourd'hui l'intelligence artificielle. D'ailleurs, John McCarthy, qui formula pour la première fois cette notion en 1955, fut l'une des figures de proue du mouvement cybernétique. Or, ces scientifiques eurent partie liée, dès l'origine, avec l'armée américaine. Parmi les vingt-quatre principaux membres de ce collectif, dix furent recrutés par le département de la Guerre pour mener différents travaux de recherche, dont le projet Manhattan. L'intérêt de l'armée américaine se porta notamment sur les dispositifs prédictifs développés par

ces chercheurs, comme le projet « AA Predictor » (*Anti-Aircraft Predictor*), conçu par deux cybernéticiens, Norbert Wiener et Julian Bigelow, également ingénieur d'IBM, dont l'idée était de mesurer le mouvement des aéronefs ennemis et d'en déduire par un calcul probabiliste la trajectoire prévisible, afin d'améliorer la précision de tir de la défense antiaérienne. L'organisateur de ce projet n'était autre que le National Defense Research Committee (NDRC), l'ancêtre de la DARPA<sup>2</sup>.

C'est précisément le successeur du NDRC, l'Advanced Research Projects Agency (ARPA, qui deviendrait quelque temps plus tard la DARPA), qui conduisit les premiers programmes de financement destinés à la recherche en intelligence artificielle. Le premier laboratoire concerné fut le Lincoln Laboratory du MIT, en 1962, dirigé par Marvin Minsky, lequel participa à l'érection de l'IA en champ de recherche à part entière avec John McCarthy, six ans auparavant, lors de la conférence de Dartmouth. Dès 1963, le contrat d'une valeur de 2,2 millions de dollars fut étendu aux programmes de recherche de la Carnegie-Mellon et de Stanford, où John McCarthy venait de fonder le premier laboratoire dédié à l'intelligence artificielle. Pendant plus d'une décennie, l'ARPA maintint ses financements avant que le Pentagone ne fit machine arrière, faute de résultats probants. À ce premier hiver de l'IA succédèrent d'autres périodes d'euphorie et de désillusions, suivant un schéma analogue. Et, malgré la tentative des Japonais et des Européens de rivaliser avec les progrès scientifiques américains, durant les années 1980, les États-Unis préservèrent leur avance, sans toutefois en faire bénéficier efficacement leur appareil de défense. Il faudrait attendre le début des années 2010, marqué par l'assomption d'une technique d'apprentissage jusqu'alors marginale, le *deep learning*, conjuguée aux progrès fulgurants des dispositifs de calcul et l'explosion du nombre de données numériques, pour que l'intelligence artificielle attirât de nouveau l'attention des pouvoirs publics.

Si l'intelligence artificielle est redevenue un enjeu stratégique pour les États-Unis, c'est non seulement en raison de progrès techniques, mais aussi du renouvellement du paysage géopolitique. Le deuxième mandat de Barack Obama marqua un changement de priorité pour la défense américaine : après la mort d'Oussama ben Laden, la Russie et la Chine furent de nouveau présentées comme les principales menaces à la sécurité nationale et au *leadership* américains. Ce sentiment fut conforté par la crise ukrainienne de 2014, qui mit en lumière la maîtrise des

(1) Voir Thibout (C.), 2019 (à paraître), « Politique de l'intelligence artificielle », in Barraud (B.) (dir.), *L'intelligence artificielle. Dans toutes ses dimensions*, Paris, L'Harmattan.

(2) Segal (J.), 2004, « Du comportement des avions ennemis aux modélisations de la connaissance : la notion scientifique et technique d'information », *Intellectica*, 2, 39, p. 55-77.

nouvelles technologies par la Russie dans la conduite de la guerre hybride<sup>3</sup>. Un an auparavant, la Chine avait en outre dévoilé son initiative des Nouvelles routes de la soie, dotée d'un budget colossal (1 000 milliards de dollars), qui déjà s'apparentait à la constitution d'un vaste réseau de dépendances en direction de l'Europe et de l'Afrique. C'est dans ce contexte qu'à l'automne 2014, le secrétaire à la Défense, Chuck Hagel, dévoila la Third Offset Strategy, une stratégie de « compensation » héritée de la guerre froide, visant à identifier, encourager et conduire des ruptures technologiques en réaction « à l'érosion [du] confortable avantage technologique dont jouissent les États-Unis depuis la Seconde Guerre mondiale<sup>4</sup> », selon les termes du secrétaire-adjoint, Robert O. Work. Parmi les technologies mises en exergue par le Pentagone, l'intelligence artificielle tient la première place. L'on peut estimer aujourd'hui le budget dédié à l'IA par l'État à quatre milliards de dollars, dont la moitié est à disposition du département de la Défense.



SI L'INTELLIGENCE ARTIFICIELLE EST REDEVENUE UN ENJEU STRATÉGIQUE POUR LES ÉTATS-UNIS, C'EST NON SEULEMENT EN RAISON DE PROGRÈS TECHNIQUES, MAIS AUSSI DU RENOUVELLEMENT DU PAYSAGE GÉOPOLITIQUE. LE DEUXIÈME MANDAT DE BARACK OBAMA MARQUA UN CHANGEMENT DE PRIORITÉ POUR LA DÉFENSE AMÉRICAINE : APRÈS LA MORT D'OUSSAMA BEN LADEN, LA RUSSIE ET LA CHINE FURENT DE NOUVEAU PRÉSENTÉES COMME LES PRINCIPALES MENACES À LA SÉCURITÉ NATIONALE ET AU LEADERSHIP AMÉRICAINS.



transnationales numériques, communément regroupées sous l'acronyme GAFAM. D'abord, Google, Amazon, Facebook, Apple, Microsoft (mais aussi IBM, Oracle, Cisco, Intel et d'autres encore) se caractérisent par leur primatie financière : ils constituent les principales capitalisations boursières au monde, tous secteurs confondus ; Amazon et Alphabet (maison-mère de Google) sont les deux entreprises qui investissent le plus de capitaux dans la R & D (respectivement 22,6 et 16,2 milliards de dollars en 2018). Mais leur place dans la course à l'intelligence artificielle se manifeste plus nettement encore par leur politique systématique de rachat d'entreprises spécialisées en IA. Entre 1998 et 2018, les GAFAM *stricto sensu* se sont portés acquéreurs d'une cinquantaine d'entreprises du secteur, dont la moitié depuis 2016 ; ils font partie des dix entreprises qui ont mené le plus de rachats dans ce domaine (1<sup>er</sup> Alphabet ; 2<sup>e</sup> Apple ; 3<sup>e</sup> Microsoft ; 5<sup>e</sup> Amazon ; 8<sup>e</sup> Facebook<sup>5</sup>).

Deux entreprises américaines, IBM et Microsoft, occupent également les deux premières places du classement en termes de brevets déposés dans le secteur de l'IA (respectivement 8 920 et 5 930 brevets).

## La montée en puissance du secteur privé

Sans le concours principal de l'État, les technologies d'intelligence artificielle n'eussent sans doute pas atteint leur niveau de sophistication actuel. Néanmoins, le secteur public ne tient plus le premier rôle dans le développement de l'IA aux États-Unis ; ce sont les grandes firmes

L'essor du secteur privé aux États-Unis est directement lié à la mue néolibérale de l'action publique américaine, entamée dans les années 1980. D'abord, l'État a permis au Nasdaq de se transformer en marché boursier de l'innovation ; les entreprises sans assise financière solide mais reconnues pour leur potentiel de croissance (cas typique des startups) pourraient désormais accéder à des capitaux financiers hors de la sphère bancaire<sup>6</sup>.

(3) Les pirates et « proxies » (mercenaires informatiques) russes se sont alors particulièrement illustrés par leurs compétences en matière de sabotage, d'espionnage et de subversion informatiques. Voir notamment Rukomeda (Roman), «Russia's Hybrid War against Ukraine: the latest Developments and Trends», Centre for Integrity in the Defence Sector, 28 septembre 2018. Disponible sur : <https://cids.no/2018/09/28/russias-hybrid-war-against-ukraine-the-latest-developments-and-trends/>

(4) Discours de Robert Work, «The Third Offset Strategy and its Implications for Partners and Allies», Département de la Défense, Washington DC, 28 janvier 2015.

(5) World Intellectual Property Organization, *WIPO Technology Trends 2019, Artificial Intelligence*, Genève, WIPO, 2019. Verizon, Cisco, Salesforce, IBM et Intel se partagent le reste du classement.

Puis le Bayh-Dol Act de 1980 a permis aux universités américaines de vendre aux entreprises des licences exclusives sur des brevets, quand bien même ces brevets seraient le résultat de recherches financées sur fonds publics fédéraux<sup>7</sup>. Puis, l'USPTO (Bureau des brevets et des marques commerciales) a facilité l'extension de la brevetabilité à différents domaines, dont les logiciels, ce qui a eu pour effet de lancer définitivement la création d'un véritable marché des produits de la recherche<sup>8</sup>. Autrement dit, l'État a réuni les conditions de sa propre dépossession en matière scientifique et technologique, en offrant un cadre légal particulièrement favorable aux firmes technologiques sans réelle contrepartie. De surcroît, il a maintenu une politique active de soutien à la création et au développement d'entreprises numériques. Ainsi, le fonds d'investissement de la CIA, In-Q-Tel, créé en 1999, a financé la société Keyhole, créateur du logiciel de visualisation satellitaire Earth Viewer ; la société a été rachetée par Google en 2004 et son logiciel phare fut rebaptisé Google Earth. La même année, Facebook a reçu sa première injection de capital, d'une valeur de 500 000 dollars, de la part de Peter Thiel, dont la société Palantir était elle-même financée par In-Q-Tel. Les deux investissements suivants ont été conduits en 2005 par Peter Thiel et Accel Partners (12,7 millions de dollars), puis Peter Thiel, Accel Partners et Greylock Partners (27,5 millions de dollars), dont le président, Howard Hox, fut membre du comité exécutif d'In-Q-Tel.

Plus fondamentale encore est la place qu'occupent ces firmes technologiques dans le procès d'action publique aux États-Unis. Car, en effet, en régime néolibéral, l'État n'est plus seulement dépossédé de ses moyens d'agir, il tend également à confier la définition de son agenda à des acteurs privés, extérieurs à la sphère politico-administrative ; et ce, pour plusieurs raisons, la principale étant leur plus grande efficacité présumée, car ils auraient été préservés des modes de pensée et de gestion bureaucratiques de l'appareil d'État et seraient donc capables de leur substituer une agilité, une capacité d'innovation et une audace étrangères aux élites administratives. Dans le cas de l'intelligence artificielle, comme les acteurs privés (en l'occurrence les GAFAM) sont reconnus pour leur supériorité technoscientifique, l'État fédéral recourt à un certain nombre de procédés

(subventions directes, dégrèvements, contrats lucratifs), par quoi il entend les inciter à lui transférer une partie de leurs innovations en IA, dans des domaines où il peut encore faire valoir une prérogative régaliennne (défense du territoire, maintien de l'ordre et renseignement, principalement). C'est ainsi qu'en 2017, Google a pris part au projet Maven.

Élaboré et mis en œuvre par le département de la Défense, le projet Maven vise à permettre au Pentagone de mieux tirer avantage des technologies d'analyse de données et d'apprentissage automatique (*machine learning*), une technique d'apprentissage particulièrement en vogue dans le secteur de l'intelligence artificielle. Dans ce cadre, la participation de Google consistait à transférer certaines de ses technologies de vision par ordinateur (reconnaissance d'images), afin qu'elles fussent intégrées aux drones de l'armée américaine pour détecter et prédire la trajectoire des individus et des véhicules filmés par leurs caméras. S'il est fort probable que d'autres entreprises aient participé à ce projet ou à des programmes similaires, l'implication de Google est éloquentes à plusieurs titres. Les liens qu'entretiennent Google et le Pentagone sont particulièrement étroits, d'abord en termes de parcours professionnels : de 1998, date de naissance de Google, à début 2016, 28 personnes (30 en comptant les départs vers la CIA) ont navigué d'une structure à l'autre, dont une écrasante majorité de départs vers le département de la Défense<sup>9</sup>. Plus largement, au moins 251 personnes ont travaillé pour Google et le gouvernement fédéral, les équipes de campagnes nationales (Sénat, Chambre, Présidence) ou le Congrès, durant les deux mandats de Barack Obama<sup>10</sup>.

Cette coalescence des trajectoires professionnelles entre Google et le département de la Défense a ceci d'intéressant qu'elle a aussi concerné des personnalités de premier ordre, à l'instar d'Eric Schmidt. Ce dernier a véritablement mené deux carrières imbriquées l'une dans l'autre : d'une part, en tant qu'homme d'affaires (PDG de Google entre 2001 et 2011, *executive chairman* de Google entre 2011 et 2015, puis d'Alphabet entre 2015 et 2018) et, d'autre part, comme personnalité proche du milieu politico-administratif, souvent dans un rôle hybride de *go-between*, d'intermédiaire entre ces deux espaces. Il a notamment conseillé et soutenu financièrement Barack Obama pendant la campagne présidentielle de 2008,

(6) Coriat (B.), 2003, «Does Biotech Reflect a New Science-Based Innovation Regime?», *Industry and Innovation*, vol. 10, n°3, p. 231-253.

(7) Voir notamment Mowery (D. C.), 2004, *Ivory Tower and Industrial Innovation. University-Industry Technology Transfer before and after the Bayh-Dol Act in the United States*, Palo Alto (CA), Stanford University Press.

(8) Voir notamment Kevles (D.), 2002, *A History of Patenting Life in the United States with Comparative Attention to Europe and Canada*, Report to European Group on Ethics, Science and New Technology, Bruxelles, Commission européenne.

(9) Ici ne sont pas pris en compte les allers-retours entre Google et d'autres entités gouvernementales, dont la Maison-Blanche, ni les individus cumulant des fonctions dans chaque structure.

(10) Campaign for Accountability, *Google Transparency Project*, «Google's Revolving Door (US)», avril 2016. Disponible sur : <https://googletransparencyproject.org/articles/googles-revolving-door-us>

auprès duquel il occupa plusieurs fonctions par la suite à la Maison-Blanche, notamment au sein du President's Council of Advisors on Science and Technology. En mars 2016, le secrétaire à la Défense, Ash Carter, l'a nommé président du Defense Innovation Advisory Board, un comité chargé de faciliter le transfert d'innovations technologiques et organisationnelles de la Silicon Valley vers le Pentagone. Un an plus tard, Google fut invité à rejoindre le projet Maven, dirigé par le secrétaire-adjoint à la Défense, Robert Work.

En janvier 2019, Robert Work a été nommé vice-président de la National Security Commission on Artificial Intelligence, une commission créée par le Congrès mais dont trois des quinze membres ont été désignés par les secrétaires à la Défense et au Commerce<sup>11</sup>. L'objectif de cette commission n'est pas anodin, puisqu'elle est chargée de définir une stratégie en matière d'intelligence artificielle qui garantisse la sécurité nationale et anticipe le risque d'« utilisation de l'intelligence artificielle par des États étrangers en avance dans l'emploi militaire » de ces technologies, en donnant d'emblée la priorité aux « partenariats publics-privés<sup>12</sup> ». Or, c'est Eric Schmidt qui fut choisi pour présider cette commission et en désigner les membres, avec l'accord du secrétaire à la Défense<sup>13</sup>. Parmi eux, six travaillent ou ont travaillé dans de grandes firmes technologiques américaines (Apple, Amazon, Google, IBM, Intel, Microsoft, Oracle...), la plupart à des postes de direction<sup>14</sup>. Il faut rappeler que si Eric Schmidt a quitté ses fonctions de président d'Alphabet au début de l'année 2018, il demeure conseiller technique et membre du conseil d'administration du conglomerat.

L'immixtion des GAFAM dans le processus d'action publique bénéficie fortement de l'attention que le personnel politique et administratif américain accorde à l'intelligence artificielle. Elle s'appuie tout autant sur la crainte de voir la Chine ravir la place de première puissance, notamment grâce aux prouesses techniques que multiplie le pays. Or, dans le même temps, les tentatives de ces entreprises pour pénétrer ce marché de 800 millions d'internautes et attirer les ingénieurs et les mathématiciens chinois risquent de contrevenir aux intérêts des États-Unis. En décembre 2017, sur fond de

guerre commerciale sino-américaine, Google a annoncé l'ouverture d'un centre de recherche et de formation en IA à Pékin ; un an plus tard, Amazon et Microsoft firent de même à Shanghai, alors que le développement des entreprises étrangères en Chine est synonyme de transfert de technologies. Certaines voix se sont élevées pour critiquer ces agissements, tel Peter Thiel, cofondateur de PayPal et de Palantir, et ancien conseiller de Donald Trump, qui a accusé Google de partager le résultat de ses recherches en IA avec l'armée chinoise<sup>15</sup>. Quoi qu'il en soit, le fait est que ces entreprises, qui concentrent les technologies les plus avancées et les principaux financements dans le domaine de l'intelligence artificielle, ont su placer les autorités dans leur dépendance, jusqu'à élaborer une stratégie autonome et, le cas échéant, opposée aux intérêts du gouvernement américain.

## Les ambitions chinoises

À l'échelle interétatique, la prééminence historique des États-Unis dans le champ de l'intelligence artificielle a commencé d'être ébranlée en 2016 lorsque, paradoxalement, un programme développé par Deepmind, la filiale britannique de Google, triompha de l'un des tout meilleurs joueurs de go au monde. Ce programme, baptisé AlphaGo, fut le détonateur d'un vaste plan de réorientation des ressources en direction du développement de l'intelligence artificielle à des fins stratégiques, coordonné par le Parti communiste chinois (PCC). Aussi trivial puisse-t-il paraître, cet événement eut un effet dont on ne mesure pas encore complètement la portée, à la fois parce que ce jeu millénaire tient une place à part dans la culture chinoise et la politique de rayonnement nationaliste de la République populaire depuis son avènement, en 1949 ; mais aussi parce que la victoire d'une machine marquait sans nuance l'ascendant technologique d'un Occident pourtant ignorant des subtilités d'un jeu aux orientations essentiellement martiales d'une difficulté extrême. Les prouesses techniques de l'entreprise furent alors perçues comme une menace, à laquelle il fallait répondre fermement<sup>16</sup>.

(11) House of Representatives, H.R.5515 - 115<sup>th</sup> Congress (2017-2018), *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Washington, U.S. Government Publishing Office, 13 août 2018 ; section 1051, « National Security Commission on Artificial Intelligence ».

(12) Voir Thibout (C.), 2019, « Quid de la domination technologique et scientifique ? », in Badie (B.), Vidal (D.), *Fin du leadership américain ?*, Paris, La Découverte, p. 132-139.

(13) National Security Commission on Artificial Intelligence, *Initial Report. NSCAI Update to Congress*, juillet 2019.

(14) Parmi eux, mentionnons Safran Catz (PDG d'Oracle), Eric Horowitz (directeur de Microsoft Research Labs), Andy Jassy (PDG d'Amazon Web Services) et Andrew Moore (directeur de Google Cloud AI).

(15) Sandler (R.), 2019, « Peter Thiel says CIA should investigate Google for being "treasonous" », *Forbes*, 15 juillet 2019. Disponible sur : <https://www.forbes.com/sites/rachelsandler/2019/07/15/peter-thiel-says-cia-should-investigate-google-for-being-treasonous/#60a52e53521d>

(16) Voir Thibout (C.), 2018, « L'intelligence artificielle, une géopolitique des fantasmes », *Études digitales*, n° 5, 1, p. 105-115.

En juillet 2017, le Conseil des affaires de l'État dévoila son « plan de développement de la nouvelle génération d'intelligence artificielle<sup>17</sup> », visant à faire de la Chine un acteur prépondérant des technologies d'IA dès 2025 et le premier centre d'innovation mondial à l'horizon 2030. Avec un budget annuel initial de 20 milliards de dollars, censé s'élever à 59 milliards à l'horizon 2025, les autorités chinoises proposent le plan le plus ambitieux dans ce domaine. Pour le mener à bien, elles se fondent sur un complexe techno-partidaire structuré autour du PCC, qui fixe les grandes orientations nationales que les firmes numériques et les laboratoires universitaires ont pour mission de mettre en œuvre par la recherche et le développement de technologies d'IA duales, à la fois civiles ou commerciales et militaires. Aboutissement de la stratégie d'« intégration civilo-militaire » chère à Xi Jinping, le plan chinois se caractérise par l'attribution aux grandes firmes numériques d'un rôle coordonnateur des grands chantiers de développement, selon leurs compétences particulières : Baidu est ainsi en charge du secteur des véhicules autonomes, Alibaba des « villes intelligentes » (*smart cities*), Tencent de l'imagerie médicale, iFlytek du traitement automatique du langage et SenseTime de la vision par ordinateur. Les opportunités économiques et militaires offertes par l'intelligence artificielle semblent telles que Xi Jinping entend s'appuyer sur ce répertoire de techniques pour atteindre son objectif : hisser la Chine au rang de première puissance à l'horizon 2049, année du centenaire de la République populaire<sup>18</sup>.

Ce plan est l'aboutissement d'un changement de stratégie opéré à la tête de l'État à la fin de la Révolution culturelle et l'arrivée au pouvoir de Deng Xiaoping, en 1978. Le développement scientifique et technologique devint une priorité du régime, au milieu des années 1980. Il s'invita au cœur de la loi sur l'éducation du 18 mars 1995 et fit l'objet d'un plan particulier, en 2006 : le plan pour le développement des sciences et des technologies à moyen et long terme (2006-2020). Tourné vers l'accroissement des ressources financières et humaines, l'objectif est de faire de la Chine une nation d'innovation à l'horizon 2020 et un *leader* mondial des technologies en 2050<sup>19</sup>, ce qui est réaffirmé dans le plan *Made in China 2025* (2015) et le plan

IA (2017). Par là même, les autorités chinoises entendent réunir les conditions nécessaires à un développement endogène des sciences et des technologies, qui passe notamment par un fort soutien aux entreprises privées (dégrèvements, zones franches, protection du droit de propriété intellectuelle, réforme du système éducatif, recrutement de « talents », etc.). De fait, entre 1995 et 2017, les dépenses de la Chine en R & D sont passées de 0,57 % à 2,15 % du PIB, alors que la croissance moyenne sur la même période s'élevait à 8,8 % par an. Avec 445 milliards de dollars consacrés à la R & D en 2017, la Chine se place en deuxième position dans le monde après les États-Unis (484 milliards). Depuis 2003, elle dépasse même de loin tous ses rivaux en termes d'exportations de biens liés aux technologies de l'information et de la communication (TIC<sup>20</sup>).

En matière d'intelligence artificielle, la Chine est le pays qui dépose le plus de brevets chaque année depuis 2014. C'est encore elle qui concentre le plus grand nombre de publications scientifiques sur le sujet (341 800 contre 327 900 pour les États-Unis, en juin 2018<sup>21</sup>). Mais l'intégration technoscientifique de l'IA suivant le modèle chinois se manifeste plus clairement encore par les programmes de coopération qui lient le Parti-État aux entreprises du numérique. Nous avons déjà cité le rôle des BATX<sup>22</sup> dans la mise en œuvre sectorielle du plan IA ; il convient également de rappeler que les technologies d'IA développées par ces entreprises sont déjà utilisées par le gouvernement, principalement à des fins militaires et sécuritaires. Dès 2014, l'entreprise iFlytek, spécialisée dans le traitement automatique du langage naturel, et notamment la reconnaissance automatique de la parole, a reçu une « licence de recherche scientifique et de production d'armes et d'équipements » de l'Administration d'État pour la science, la technologie et l'industrie de la défense nationale (équivalent chinois de la DGA), l'autorisant à répondre aux commandes de l'Armée populaire de libération<sup>23</sup>. L'entreprise YaTrans a également mis son outil de traduction automatique (Mavericks), fondé sur la reconnaissance vocale, à la disposition du ministère de la Sécurité de l'État (en charge du contre-espionnage), des gouvernements provinciaux du Tibet et du Xinjiang (deux

(17) Conseil des affaires de l'État, « Plan de développement de la nouvelle génération d'intelligence artificielle ».

(18) Xi Jinping, *Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era*, 19<sup>e</sup> Congrès national du Parti communiste chinois, 18 octobre 2017.

(19) Voir Cao (C.), Suttmeier (R. P.), Simon (D. F.), 2009, « China's Innovation Challenge », *Innovation: Management, Policy and Practice*, vol. 11, n° 2, p. 253-259 ; Cao (C.), Suttmeier (R. P.), Simon (D. F.), « China's 15-Year Science and Technology Plan », *Physics Today*, vol. 59, n° 12, p. 38-43.

(20) OCDE, *Exportations de biens liés aux TIC* (indicateur), 2019. Disponible sur : <https://data.oecd.org/fr/ict/exportations-de-biens-lies-aux-tic.htm>

(21) World Intellectual Property Organization, *WIPO Technology Trends 2019, Artificial Intelligence*, Genève, WIPO, 2019, p. 85.

(22) Pour Baidu, Alibaba, Tencent et Xiami, auxquelles il faudrait ajouter Huawei, ZTE, iFlytek et SenseTime, entre autres.

(23) Liu (X.), 2014, « Keda News a obtenu une licence de production d'armes » (en chinois), *Finance.Sina.com.cn*, 11 avril.



DE FAÇON GÉNÉRALE, LES TECHNOLOGIES D'INTELLIGENCE ARTIFICIELLE SE RÉPANDENT SUR LE CONTINENT EUROPÉEN ET GAGNENT EN ACCESSIBILITÉ. TOUTEFOIS, CES TECHNOLOGIES SONT DANS LEUR MAJORITÉ CONÇUES PAR DES FIRMES ÉTRANGÈRES, Y COMPRIS LORSQU'ELLES SONT UTILISÉES DANS DES SECTEURS SENSIBLES, COMME LA SURVEILLANCE PAR EXEMPLE. AU MOINS SIX PAYS DE L'UNION EUROPÉENNE UTILISENT DES TECHNOLOGIES DE SURVEILLANCE CHINOISE, ET CINQ DES TECHNOLOGIES ÉTATSUNIENNES.



provinces traversées par de forts courants insurrectionnels et séparatistes) et de la région militaire de Shenyang, à la frontière nord-coréenne<sup>24</sup>.

Au total, les autorités chinoises fixent trois principaux buts au développement de l'intelligence artificielle : le renforcement du système productif national qui pâtit d'une croissance économique tendancielle en baisse depuis 2010 ; l'amélioration des dispositifs de contrôle social pour répondre aux tensions séditionnelles et séparatistes ; la montée en gamme de l'arsenal militaire afin de combler l'écart avec l'appareil de défense américain. L'objectif final est de garantir la stabilité sociopolitique du régime et de déchoir les États-Unis de leur statut d'*hégémon*.

## L'Europe à la peine

Face à ces deux puissances technoscientifiques, l'Europe fait pâle figure. Certes, la Commission européenne a annoncé un financement de 20 milliards d'euros pour le développement de l'intelligence artificielle à l'horizon 2030<sup>25</sup>. Cependant, il s'agit davantage ici d'un vœu pieux que d'une véritable stratégie. La Commission hasarde une recommandation auprès des États membres, mais aussi des entreprises privées, tandis que le budget prévu par le gouvernement chinois ne comprend que les investissements d'État, à l'exclusion des initiatives locales

et privées. Quand le principal budget national européen en la matière, celui de l'Allemagne, s'élève à trois milliards d'euros échelonnés sur six ans, celui d'un simple parc scientifique consacré à l'IA par la ville de Pékin rassemble 1,88 milliard d'euros – près de 400 millions d'euros de plus que le plan français (1,5 milliard d'euros sur quatre ans). Pour lors, la priorité à court terme de la Commission européenne est de créer un « réseau de l'intelligence artificielle », mêlant entreprises privées et laboratoires publics. En janvier 2019, dans le cadre du programme Horizon 2020, elle a investi 20 millions d'euros dans le projet AI4EU, coordonné par Thales et destiné à développer une plateforme d'IA à la demande. En juillet 2019, un fonds de 50 millions d'euros supplémentaires a été débloqué pour développer la plateforme et élaborer des projets d'enseignement de l'IA.

De façon générale, les technologies d'intelligence artificielle se répandent sur le continent européen et gagnent en accessibilité. Toutefois, ces technologies sont dans leur majorité conçues par des firmes étrangères, y compris lorsqu'elles sont utilisées dans des secteurs sensibles, comme la surveillance par exemple. Au moins six pays de l'Union européenne utilisent des technologies de surveillance chinoise, et cinq des technologies étatsuniennes. Huawei et Palantir sont les deux entreprises les plus mobilisées : quatre États européens connus sont clients de chacune d'elles (Allemagne, Espagne, France et Italie pour Huawei ; Allemagne, Danemark, Espagne et Royaume-Uni pour Palantir). Viennent ensuite le chinois Hikvision (Danemark, France, Royaume-Uni), l'américain Cisco (Allemagne, Danemark), puis le chinois ZTE et le finlandais Teleste (France), dont une partie de la chaîne de production se situe aussi en Chine, le canadien Avigilon et l'australien BrainChip (Danemark), l'américain IBM (Espagne) et le japonais NEC (Royaume-Uni). Au total, sur les treize entreprises de surveillance auxquelles ces pays font principalement appel, neuf sont extra-européennes. Seuls deux pays ont recours de façon soutenue (mais non exclusive) à des technologies domestiques : l'Espagne (Herta, SICE) et la France (Thales). Globalement, 82 % des entreprises auxquelles recourent les pays cités plus haut ne sont pas européennes<sup>26</sup>. Cette situation fait peser une grave menace sur la maîtrise des technologies et la protection des données qu'elles traitent. L'on sait que les agences de renseignement équipent les technologies produites par les entreprises de dispositifs de surveillance, comme les *backdoors* (« portes dérobées ») implantés dans les routeurs et les serveurs de Cisco par la National

(24) Site web de l'entreprise, YaTrans.com, « Partners », consulté le 1<sup>er</sup> mars 2019.

(25) Commission européenne, SWD (2018) 237 final, « Artificial Intelligence for Europe », Bruxelles, 25 avril 2018.

(26) Feldstein (S.), 2019, *The Global Expansion of AI Surveillance*, Working Paper, Carnegie Endowment for International Peace, septembre.

Security Agency (NSA<sup>27</sup>). Ce risque est particulièrement inquiétant lorsqu'il est question de données recueillies par les services de police ou de renseignement, comme la direction générale de la Sécurité intérieure dont le principal outil d'analyse de données est conçu par Palantir, l'entreprise cofondée par Peter Thiel grâce aux financements d'In-Q-Tel.

L'Union européenne affronte un certain nombre de problèmes structurels qui font obstacle au développement endogène de l'intelligence artificielle. D'abord, elle demeure un espace intergouvernemental, dans lequel l'unanimité est la règle et nombre de prérogatives régaliennes restent attachées aux États membres<sup>28</sup> ; les conditions de possibilité d'une action publique européenne intégrée et structurée autour d'une ou plusieurs instances décisionnelles indépendantes ne sont pas réunies. Et pour cause, l'Union européenne se compose d'une multitude d'États aux aspirations et aux intérêts différents, voire divergents. Par ailleurs, elle fonctionne suivant un cadre juridico-économique qui prohibe toute politique publique d'inspiration chinoise ou américaine. À titre d'exemple, les politiques budgétaires nationales sont encadrées par l'article 140 du traité sur le fonctionnement de l'Union européenne, qui interdit aux États d'accuser un déficit public annuel de plus de 3 % de la valeur du PIB, ou d'émettre une dette publique dépassant 60 % du PIB.

Par ailleurs, au nom du respect de la concurrence libre et non faussée, l'article 107 du même traité défend aux États de soutenir l'activité de leurs entreprises nationales en particulier. Or, ni la Chine ni les États-Unis ne s'appliquent de telles règles ; au contraire, ces pays mènent d'intenses politiques de soutien à leur système productif et limitent drastiquement la concurrence étrangère. À telle enseigne que l'Union européenne renferme par principe non seulement les conditions de son échec, mais également celui de ses États membres.

Conduire une politique réaliste de développement de l'IA dans l'Union européenne présuppose de clarifier les objectifs et les intérêts de chacun. Ce préalable est nécessaire avant d'envisager une stratégie concertée qui ressortit, en dernière analyse, au bon vouloir des États membres ■

(27) Greenwald (G.), 2014, *No Place to Hide. Edward Snowden, the NSA and the Surveillance State*, Londres, Penguin Books, p. 142.

(28) Voir Nabli (B.), 2007, *L'exercice des fonctions d'État membre de la Communauté européenne. Étude de la participation des organes étatiques à la production et à l'exécution du droit communautaire : le cas français*, Paris, Dalloz. Même si la construction européenne s'est doublée d'un « transfert de compétences » des États vers les institutions de l'Union européenne, les États demeurent les seuls organes souverains en dernier ressort.



## Quelques éléments d'une géopolitique du Net...

Gaetan GORCE

**P**assé la ferveur utopiste et militante des fondateurs qui voyaient dans le Net le moyen de permettre à tous d'accéder à la connaissance sans le truchement des États, en enjambant les pouvoirs et les frontières, une autre réalité s'est peu à peu imposée.

Celle d'une formidable concentration économique tout d'abord, et de la constitution de monopoles puissants capables non seulement d'interdire l'accès au marché à toute concurrence potentielle, mais aussi de contrôler la majeure partie de la masse croissante de données circulant sur le Web.

Ce qui ne pouvait manquer de susciter l'intérêt des États tant du point de vue de leur sécurité que de leur indépendance stratégique.

Les États-Unis, s'ils durent partager avec les Européens (notamment au CERN<sup>1</sup>) l'esprit pionnier et d'invention qui fut à l'origine de la révolution numérique, furent les premiers à le comprendre.

Dès la fin des années 1980, sous l'impulsion du sénateur Al Gore, seront mis en place les outils juridiques et de financement qui allaient accompagner le formidable essor de l'industrie et des services numériques. Adopté en 1991, le Bill High Performance Computing Act débloquait déjà 1,7 milliard de dollars au service d'une politique offensive combinant avantages fiscaux et

### Gaetan GORCE



Gaetan Gorce est chercheur associé à l'INHESJ. Il a été membre de la Cnil (2011/2016)

et Président de la mission d'information parlementaire sur la gouvernance d'Internet (2015).

(1) Organisation européenne pour la recherche nucléaire.



commandes publiques. Pour parvenir à assurer cette hégémonie, ne sera négligé par Washington aucun des atouts stratégiques à sa disposition, y compris la monnaie, comme en témoignera la manière dont les États-Unis surent restaurer la suprématie d'IBM et surtout d'Intel en souffrance face à la concurrence japonaise sur le marché des microprocesseurs en contraignant Tokyo à une réévaluation du yen dans le cadre des accords du Plaza en 1985.

Leur suprématie est désormais solidement établie puisque sur les cinquante premières entreprises du secteur, trente-trois sont américaines et aucune européenne, créant une situation d'autant plus préoccupante que les avantages que les États-Unis tirent de cette hégémonie économique sont cumulables et extensibles aux autres domaines stratégiques.

Cette hégémonie s'étend d'abord à tous les étages du système : l'organisation du système de câblage qui permet l'interconnexion mondiale et la répartition (comme la propriété) des *Data-centers* sont telles qu'une très large part des données mondiales transite par une technologie américaine ; les systèmes d'exploitation de nos terminaux sont américains et orientent vers des prestations de services américaines (Google Amazon, Facebook, Apple et Microsoft) traitant ainsi 80 % des données mondiales.

La puissance qui en résulte est déstabilisatrice à plus d'un titre :

- d'abord à travers la force de frappe financière qu'elle confère aux GAFAM dont le chiffre d'affaires respectif, au moins pour deux d'entre eux, tangente le milliard et qui au regard des rendements croissants qu'ils obtiennent (l'essentiel du coût résidant dans l'investissement initial) deviennent de véritables machines à cash, diversifiant de manière foudroyante leur champ d'interventions (cf. la voiture connectée) et absorbant la concurrence émergente (si Facebook a pu racheter What'App pour 18 milliards de dollars, Google a, de son côté, ingéré 150 sociétés depuis sa création !) ;
- ensuite en leur permettant de défier la législation des États (à l'instar du refus de Google d'appliquer la directive sur les droits d'auteur) voire en privant ostensiblement ceux-ci des recettes fiscales que génère leur développement (le conseil du numérique entendu en 2013 par une mission du Sénat a estimé à 1,5 % le taux d'imposition des Gafam rapporté aux bénéfices dégagés par leur activité en France).

Cette position hyper-dominante produit enfin ses effets dans le champ hypersensible de la protection des

personnes, de l'intelligence économique et de la cybersécurité.

La coopération étroite que l'affaire Snowden a clairement mise à jour entre les grands opérateurs du Net et les services du renseignement américain aboutit à des formes d'espionnage politique et commercial sans précédents.

L'interception s'opère à tous les niveaux.

Celui des infrastructures en se branchant directement sur les réseaux en particulier au point d'atterrissage des câbles de fibre optique (voire directement sur les 448 câbles sous-marins d'une longueur cumulée de 1,2 million de km transportant 99 % du trafic intercontinental).

Celui des réseaux en détournant (ou en profitant des failles, parfois volontairement introduites) des protocoles : le programme Génie de la NSA ne visait-il pas au développement d'implants dans des dizaines de milliers d'ordinateurs ? Par réquisition enfin dans le cadre de coopération officieuse avec les opérateurs (via PRISM) ou officielle via le récent *Cloud Act* qui permet aux autorités américaines d'exiger la communication de toutes les données stockées aux États-Unis ou sur des serveurs à l'étranger mais appartenant à des sociétés américaines !

Cette puissance suscite certes des résistances.

Aux États-Unis aussi comme en témoignent par exemple les enquêtes engagées contre les Gafam par une cinquantaine de procureurs ; ou en Europe.

Mais celle-ci ne dispose aujourd'hui que d'un seul véritable atout : l'avance qu'elle a prise dans le secteur juridique de la protection des données (avec la mise en œuvre l'an passé du règlement général sur la protection des données) susceptible de faire jurisprudence dans le monde occidental (mais qu'affaiblit la faiblesse des garanties obtenues dans le cadre des nouveaux accords régissant le transfert des données des citoyens européens aux États-Unis et ceci malgré la vigilance de la Cour de Justice de l'UE).

Absente des microprocesseurs, bousculée sur les logiciels, totalement dépassée sur les services, l'Europe n'existe encore industriellement que via les fournisseurs d'accès ou Nokia. Le combat qu'elle a engagé, au titre du droit fiscal et de la concurrence, gagnerait par conséquent à être doublé d'une politique active de la commande publique et en matière de *cloud* d'un soutien déterminé à la seule entreprise capable de rivaliser à savoir OvH. Mais les engagements pris à grand renfort de déclarations publiques au cœur des années 2000 sont restés lettre morte.



TOUS LES GRANDS PAYS SE SONT AINSI DOTÉS DE CAPACITÉ DE SURVEILLANCE TOURNANT VITE À L'ESPIONNAGE, VOIRE AUX TENTATIVES DÉLIBÉRÉES DE DÉSTABILISATION POLITIQUE OU ÉCONOMIQUE, DONT LES INTRUSIONS RUSSES DANS L'ÉLECTION PRÉSIDENTIELLE AMÉRICAINE NE SONT QU'UN EXEMPLE PARMIS D'AUTRES. SI TOUTES LES ENTREPRISES DU MONDE SONT AUJOURD'HUI SOUMISES À DES MENACES D'INTRUSION TÉLÉCOMMANDÉES OU NON PAR DES ÉTATS, LE PIRATAGE À DES FINS POLITIQUES OU/ET MILITAIRES A PRIS DES PROPORTIONS CONSIDÉRABLES.



Seules au fond la Chine et la Russie, à un degré moindre, se sont donné les moyens de contester cette hégémonie.

Toutes deux en se déconnectant peu ou prou du Web mondial ou, plus précisément, en introduisant un sas entre celui-ci et leurs internautes nationaux. Ainsi, en particulier la Chine, se sont-elles dotées d'un système d'adressage distinct du système mondial. Celui-ci est en effet constitué d'un annuaire mondial des terminaux dont les adresses sont attribuées par une société... de droit américain gérée par la communauté internationale des utilisateurs (opérateurs et citoyens) : l'ICANN. Le sas établi par ces États leur permet en pratique de réorienter les requêtes effectuées par des usagers nationaux vers des sites éventuellement épurés des informations proscrites.

La Chine s'est, par ailleurs, dotée d'un réseau d'acteurs « doublonnant » celui des EU : à chaque entité des Gafam correspond une entreprise chinoise (Baidu, Alibaba, Tencent, Xiaomi) contrôlant le marché domestique, traduisant une capacité industrielle et technologique comparable, et offrant une force de frappe inférieure mais de même nature. Ce dont témoignent d'ailleurs les interrogations répétées sur la fiabilité du matériel proposé par Huawei suspecté d'être infecté par des dispositifs espions, justifiant les réticences de nombreux États à en faire l'opérateur de leur 5 G.

La rivalité s'est, en effet, naturellement déplacée des enjeux industriels à ceux de sécurité dont on a vu qu'ils étaient inévitablement liés.

Sans qu'il soit encore nécessaire de parler de cyberguerre, le Net est devenu le champ clos d'un affrontement multiforme.

Tous les grands pays se sont ainsi dotés de capacité de surveillance tournant vite à l'espionnage, voire aux tentatives délibérées de déstabilisation politique ou économique, dont les intrusions russes dans l'élection présidentielle américaine ne sont qu'un exemple parmi d'autres. Si toutes les entreprises du monde sont aujourd'hui soumises à des menaces d'intrusion télécommandées ou non par des États, le piratage à des fins politiques ou/et militaires a pris des proportions considérables. De l'initiative isolée serbe sur les serveurs de l'OTAN en forme de riposte aux bombardements menés par les États-Unis dans les années 1990 à l'attaque générale dont a fait l'objet l'Estonie dix ans plus tard, on a, à l'évidence, changé d'échelle.

Le sabotage par des logiciels malveillants des infrastructures critiques (eau, énergie, etc.) est désormais un risque possible au point qu'en 2012 le secrétaire américain à la Défense Léon Panetta n'hésitait pas à exprimer ses craintes quant à ce qu'il devait appeler de manière éloquente « *un cyber Pearl Harbor* ».

C'est que chaque pays semble désormais rivaliser d'imagination : le virus américain Stuxnet a ainsi détruit en 2009 plusieurs centrifugeuses de la centrale de Natanz en Iran (provoquant en retour en 2013 l'intrusion de hackers iraniens dans le système informatique d'un barrage près de New York). On ne compte plus les agressions dont la gravité va croissant : le piratage du système de détection aérienne syrien par Israël en 2007 ou celui du système de contrôle des Rafales de la Marine en 2009, cloués au sol ; ou encore celui du NHS en 2017 ; toutes initiatives présentant l'avantage de la précision, de leur caractère asymétrique, bon marché, comme de la discrétion et de la difficulté à en identifier la source.

Dès lors, tous les États, après avoir mis en place des outils de prévention de l'espionnage économique, se dotent progressivement d'unités chargées de conduire le combat numérique (il existe un EU cybercommand depuis 2010 ; la France s'est équipée d'un cyber com en 2016 avec autorité sur toutes les unités opérationnelles spécialisées des trois armes, soit 2 600 hommes et 600 experts de la direction générale de l'Armement (DGA), sans compter 4 400 réservistes).

Le risque d'escalade est désormais sérieux et justifierait un effort de régulation qui en reste malheureusement aux balbutiements, dans cette dimension de la révolution numérique comme d'ailleurs dans les autres.

Certes, on l'a vu, des efforts ont été faits, en particulier à l'initiative de l'UE, pour fixer des règles protégeant les données personnelles et avec elles nos libertés.

La régulation technique du réseau et de ses standards est de son côté bien établie même si elle garde souvent un caractère informel, voire autogéré. En effet, les ingénieurs et techniciens ont imaginé un modèle de gouvernance collégiale indispensable à la définition de standards communs et à l'évolution des réseaux qu'ils ont réussi, envers et contre tout, à préserver... même si l'influence des Gafam y est élevée.

Mais il n'existe toujours pas de cadre politique et juridique partagé internationalement et rappelant les principes fondamentaux de fonctionnement du Net comme les règles applicables aux relations numériques entre États.

Certes, la communauté internationale s'est saisie du sujet.

La perspective d'élaborer un traité international qui définirait et sanctuariserait les règles relatives à Internet est ainsi ouverte depuis que l'ONU a jugé utile de lancer en 2003 le sommet mondial sur la société de l'information qui s'est réuni depuis à de nombreuses reprises encourageant la pratique de forums mondiaux et régionaux associant tous les acteurs du monde numérique.

En 2005, le sommet de Tunis devait même permettre l'adoption à l'unanimité d'une déclaration dite « Agenda de Tunis » importante par les repères qu'elle fixe, mais dénuée de toute force juridique. Du coup, les « quatre grands principes » de gouvernance du Net qu'elle a dégagés restent fragiles qu'il s'agisse de sa neutralité, contestée par les fournisseurs d'accès et abandonnée il y a peu aux États-Unis par la Fédéral communication Commission ; de son unité, fragilisée par les murs de protection élevés par Chinois et Russes ; ou de sa gouvernance multipartite, contestée, on s'en souvient, pour l'influence qu'y exercent en sous-main les Gafam et le gouvernement américain. Seul le principe de protection des données personnelles a semblé progresser sous cette réserve que son caractère juridique n'est pour l'heure pleinement affirmé qu'au sein de l'UE.

L'hypothèse d'un consensus autour d'une sorte de Charte internationale des droits numériques relève par conséquent toujours de l'utopie.

La rivalité entre les puissances se donne en effet libre cours dans les instances de l'ONU (comme lors du débat sur la proposition faite en 2011 par le Brésil et l'Afrique du Sud de créer un comité de l'Onu pour les politiques) ou en dehors (par exemple à travers le projet de « code de bonne conduite intergouvernemental » défendu par le groupe de Shanghai la même année) butant à chaque fois sur le refus des EU, et, à un moindre degré, de l'UE, de placer le Net sous le contrôle même partiel des États les plus restrictifs en matière de liberté numérique, à savoir la Chine et la Russie, sous couvert de l'ONU. Ce qui a eu pour effet de bloquer toute évolution comme l'a illustré l'échec de la Conférence de l'UIT à Dubaï en 2012.

Sans doute faudra-t-il apprendre à se satisfaire d'une évolution progressive comme celle enregistrée par exemple sur les risques de cyberguerre dont chacun s'accorde désormais à penser qu'elle relève du droit international applicable aux conflits armés et dont le *Manuel de Tallinn*, élaboré patiemment par un groupe d'experts internationaux, s'efforce de tirer, de manière seulement indicative, les conséquences.

La prise de conscience des enjeux est, à cet égard, indéniable mais elle n'oblitére pas la préoccupation qu'ont les Puissances de leurs intérêts nationaux : ainsi la Chine s'est-elle engagée auprès du Président Obama voici quelques années à mettre en veilleuse son espionnage industriel et a depuis plutôt tenu cet engagement. Mais c'est qu'elle avait atteint en la matière ces principaux objectifs comme en témoigne le saut technologique accompli par Huawei.

Au final, comment ne pas voir qu'à l'instar des mers et des océans avant-hier, de l'espace aérien puis interstellaire hier, le cyberspace constitue, comme bien commun, un formidable enjeu de régulation ? Et l'on serait en droit d'attendre de la France, dont c'est la vocation, qu'elle soit à la manœuvre pour en favoriser l'émergence.

Mais la contradiction entre un réseau conçu techniquement comme sans frontières ni centre et un système international westphalien restera sans doute indépassable à une époque où la redistribution des cartes entre les puissances bat son plein ■



## Quel cadre juridique pour les outils d'intelligence artificielle dans le domaine du renseignement?

Floran VADILLO

**A** lors que des algorithmes permettent d'optimiser les processus industriels, de guider la prise de décisions stratégiques, d'identifier une fraude bancaire ou encore de contenir la cybercriminalité, certains envisagent déjà des applications au domaine de l'enquête pour favoriser la résolution d'affaires, voire anticiper un passage à l'acte. En effet, l'intelligence artificielle (IA) investit progressivement de nombreux secteurs d'activité, permettant d'élargir le champ des possibles dans le domaine de la connaissance et de l'aide à la décision grâce notamment à des algorithmes de reconnaissance des formes ou de la voix, à des outils capables d'agréger et d'extraire automatiquement des informations

concordantes, etc. De fait, PIA se nourrit des données de masse, fruit de la numérisation des activités humaines, pour générer des potentialités économiques, cognitives ou stratégiques tout à fait considérables.

Cependant, le monde du renseignement semble encore peu ouvert aux potentialités que charrie cette nouvelle technologie et, plus largement, au traitement des données de masse. Ainsi, lorsque la direction générale de la Sécurité intérieure (DGSI) a décidé, en 2016, de recourir aux prestations de la société américaine Palantir, la décision a-t-elle profondément surpris tant le sujet avait été occulté des débats. Comme le résume avec humour Patrick Calvar, ancien directeur général de la Sécurité intérieure de 2014 à 2017 : « *Nous n'avions pas manqué le train du traitement des données de masse, nous ne l'avions pas vu passer*<sup>(1)</sup> ».

Floran VADILLO



Floran Vadillo,  
Docteur  
en science  
politique est  
directeur en  
charge de  
la sécurité

intérieure chez Sopra Steria

(1) Intervention au sein de la BU Défense et sécurité, le 19 janvier 2018.

Mais cette problématique dépasse les seuls services de renseignement pour concerner l'ensemble des administrations qui réalisent des enquêtes, qu'elles relèvent du champ administratif ou judiciaire. Et, au-delà d'un simple retard décisionnel, il faut signaler une carence technologique française et européenne : de manière schématique, en ce domaine, il n'existe pas d'offre industrielle ayant atteint une masse critique autre qu'américaine ou israélienne<sup>2</sup>. Car, au manque d'anticipation de la part des industriels, s'ajoute un cadre juridique applicable au recueil des données qui offre moins de latitude que dans les pays précités. Or, pour être efficace, l'IA doit intégrer d'importants jeux de données multicanaux et multisources. Et si les législations américaine et israélienne offrent de grandes marges de manœuvre (contribuant en partie à la formalisation d'une offre industrielle en la matière<sup>3</sup>), tel n'est pas le cas en France, pays qui a d'autant moins fait évoluer le cadre juridique – au-delà de la question de la protection des droits fondamentaux, notamment le respect à la vie privée – qu'aucun industriel français ou européen n'a manifesté d'ambition pour le sujet, véritable cercle vicieux.

Toutefois, le droit actuel – sans doute incomplet – permet d'entreprendre des projets. Il varie cependant grandement selon que l'on agit en administratif ou en judiciaire. Il convient donc d'interroger ces spécificités françaises et d'esquisser des évolutions sans rompre avec la légitime protection de la vie privée.

## La trop récente massification des données d'enquête

Si les outils d'IA tardent à se développer en France dans le secteur de la sécurité, cela tient sans doute à la quasi-absence de gisements de données de masse du fait d'un cadre juridique construit de manière cahotante, à la mise en œuvre complexe et récente.

### La lente construction d'un outillage d'enquête

Longtemps, les services enquêteurs ont connu des difficultés d'accès à l'information, qu'elle soit ouverte

ou fermée. Cet état de fait n'a donc guère permis de constituer des gisements de données au profit des administrations concernées. Les obstacles en cause étaient d'ordre juridique, mais répondaient aussi à une origine technologique/technique. En effet, on sous-estime trop souvent la lente adaptation de notre droit en ces matières. Au demeurant, ces difficultés touchaient différemment les services de police administrative et ceux de police judiciaire<sup>4</sup>.

À ce titre, jusqu'en 2015, le pouvoir exécutif estimait que les activités de renseignement devaient rester clandestines ; par conséquent, il ne se préoccupait pas du cadre juridique les régissant. Ainsi, les services de renseignement ne disposaient-ils que de trois outils légaux de recueil de données :

- l'accès à différents fichiers (fichiers de police judiciaire, fichiers administratifs, système d'information Schengen, etc.) ;
- les « écoutes téléphoniques », juridiquement nommées « interceptions de sécurité » (IS, régies par la loi du 10 juillet 1991) ;
- et le recueil des données techniques de connexion (*ex post* à partir de la loi du 23 janvier 2006, puis y compris en temps réel à partir de la loi du 18 décembre 2013).

Quant aux services de police judiciaire, leurs lacunes relevaient d'une philosophie du droit obsolète : le Code de procédure pénale prévoyait en effet que le magistrat dirigeant une enquête pouvait prescrire tous les actes nécessaires à la manifestation de la vérité (articles 81 et 151 du Code de procédure pénale, CPP), sans fournir plus de détails. Or, ce manque de clarté et de prévisibilité de la loi (et, par voie de conséquence, de capacités de recours) a justifié de nombreux arrêts de la cour de Cassation (inspirée, quand elle n'était pas suivie, par la Cour européenne des droits de l'Homme, CEDH) qui sanctionnaient l'exploitation de moyens de preuve obtenus par le biais de techniques non prévues *expressis verbis* par les textes :

- les interceptions judiciaires (IJ) subirent, les premières, cette rigueur : un arrêt de 1989 puis deux décisions de la CEDH de 1990 [Huvig et Kruslin] rendirent nécessaire

(2) Pour ce dernier pays, on citera par exemple 5D, Verint, TA9.

(3) L'existence d'un écosystème militaro-industriel propice constitue sans doute l'un des facteurs d'explication les plus pertinents.

(4) Car, en France, la dualité des ordres juridictionnels et les importantes prérogatives de l'État ont conduit à structurer une *summa divisio* entre la police judiciaire (chargée de la répression) et la police administrative (chargée de la prévention). Le Conseil constitutionnel rappelle avec constance cette distinction qui sépare les objectifs et les moyens et, par conséquent, les administrations concernées et les instances de contrôle.



APRÈS DES ANNÉES DE DISETTE NORMATIVE, POLICES ADMINISTRATIVE ET JUDICIAIRE BÉNÉFICIENT DONC DEPUIS PEU DE CADRES JURIDIQUES COMPLETS ET ÉQUIVALENTS EN MATIÈRE DE TECHNIQUES SPÉCIALES D'ENQUÊTE (LA PREMIÈRE S'ÉTANT EN PARTIE INSPIRÉE DE LA SECONDE DANS LE CADRE DE LA LOI DU 24 JUILLET 2015 RELATIVE AU RENSEIGNEMENT, MÊME SI LE CPP MÉRITE SANS DOUTE UNE SIMPLIFICATION DES RÉGIMES D'AUTORISATION POUR UNE PLUS GRANDE LISIBILITÉ). POUR AUTANT, COMME SOULIGNÉ, CET ÉTAT DE COMPLÉTUDE JURIDIQUE EST EXTRÊMEMENT RÉCENT ET SE HEURTE, POUR SA MISE EN ŒUVRE AU PROFIT DE LA POLICE JUDICIAIRE, À DES PROBLÉMATIQUES FINANCIÈRES ET TECHNOLOGIQUES.



L'adoption de la loi précitée de juillet 1991 ;

- plus tard, ce fut au tour de la géolocalisation : un arrêté du 22 octobre 2013 obligea le législateur à adopter la loi du 28 mars 2014.

De fait, ce que la loi ne prévoyait pas explicitement ne pouvait être légitimement mis en œuvre. Les techniques d'enquête judiciaire s'avéraient donc assez pauvres jusqu'à ce que le législateur entreprenne une remise à niveau :

- ainsi la filature, la sonorisation, la captation d'images et l'infiltration firent-elles leur entrée dans le CPP grâce à la loi du 9 mars 2004, dite « Perben II » ;
- la captation de données informatiques procéda de la LOPPSI 2<sup>5</sup> de 2011 ;
- puis, à partir de 2013, les ajouts furent plus rapprochés avec, outre la géolocalisation déjà mentionnée, l'enquête numérique sous pseudonyme (loi du 13 novembre 2014) ou le recours aux IMSI *catchers* (loi du 3 juin 2016).

Après des années de disette normative, polices administrative et judiciaire bénéficient donc depuis peu de cadres juridiques complets et équivalents en matière de techniques spéciales d'enquête (la première s'étant en partie inspirée de la seconde dans le cadre de la loi du 24 juillet 2015 relative au renseignement, même si le CPP mérite sans doute une simplification des régimes d'autorisation pour une plus grande lisibilité). Pour autant, comme souligné, cet état de complétude juridique est extrêmement récent et se heurte, pour sa mise en œuvre au profit de la police judiciaire, à des problématiques financières et technologiques.

### La perpétuation du retard de la police judiciaire

L'équilibre juridique précité se rompt sur les moyens technologiques et financiers à disposition des services de police judiciaire qui accusent un retard croissant. Les investissements n'ont sans doute pas été à la hauteur des besoins, si bien que la captation de données informatiques (pourtant autorisée depuis 2011) n'a jamais été mise en œuvre ; très récemment, l'arrêté du 9 mai 2018 a créé un service à compétence nationale dénommé « Service technique national de captation judiciaire » afin de développer des souches implantables. De même, le projet de la plateforme nationale des interceptions judiciaires (PNIJ) a connu de nombreuses avanies avant que la création de l'Agence nationale des techniques d'enquête numérique judiciaire (ANTENJ) ne permette d'améliorer la situation. À l'inverse, à partir de 2008, les services de renseignement ont bénéficié d'investissements considérables pour effectuer une mue technologique.

Mais au-delà des investissements, c'est la faculté à conduire de grands projets technologiques qui s'est, pour les premiers, avérée déficiente. Henri Verdier l'a parfaitement synthétisé : « *Nous manquons cruellement au sein de l'État de grands chefs de projet, de personnes ayant une culture de production numérique. Nous sommes devenus malhabiles pour acheter, parce que l'on ne sait plus très bien spécifier, négocier ou encadrer nos fournisseurs. Nous devons donc travailler sur les ressources humaines pour réintégrer de nouveaux profils, pour réapprendre la conception et le pilotage de projets*<sup>6</sup> ».

Enfin, la police judiciaire se heurte à une problématique technologique en ce qui concerne l'accès aux données chiffrées (le monde judiciaire ne s'étant pas doté de capacités

(5) La loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure dite « LOPPSI 2 ».

(6) Verdier (H.), 2017, « le vrai sujet : faire advenir l'État d'après la révolution numérique », *Bercy numérique*, 20 décembre.

de déchiffrement analogues à celles de l'administratif). Ce point revêt également une forte dimension juridique, et en particulier de droit international dans une confrontation avec les GAFAM<sup>7</sup> pour l'application de réquisitions judiciaires qui achoppent bien souvent sur un chiffrement de bout en bout.

Pour compenser ces difficultés, la police judiciaire dispose néanmoins d'un avantage sur le domaine administratif au regard des larges capacités de réquisition dont bénéficie l'autorité judiciaire en comparaison avec les services de renseignement, dont les moyens sont limitativement énumérés par la loi précitée du 24 juillet 2015.

En dépit de ces considérations, l'accès à l'information constitue désormais un problème moins aigu que la gestion de la masse de données collectées par les services enquêteurs. La situation est flagrante en police judiciaire du fait de l'obligation de conserver tous les éléments recueillis au cours de l'enquête afin d'assurer la loyauté de la preuve (là où l'administratif est tenu de supprimer ces données à échéance d'un délai fixé par la loi<sup>8</sup>). Cette obligation, liée au droit à un procès équitable, revient à noyer les données pertinentes dans un océan de bruit numérique. L'analyste est désormais débordé par la masse, la diversité d'intérêt et la technicité du traitement. Il n'a pas d'autre choix que de solliciter une aide technique s'il souhaite exploiter l'information recueillie par divers canaux. Le recours à l'IA s'impose donc comme inéluctable. Néanmoins, l'inéluctable n'est parfois juridiquement pas – totalement – possible.

## Complexe et incomplet : le cadre juridique relatif à l'enquête au banc des accusés

Les techniques désormais autorisées par la loi devraient donc permettre de constituer progressivement des gisements de données. Toutefois, le droit applicable à

l'exploitation de ces derniers accuse à la fois une trop grande complexité et un réel retard pour prendre en charge les conséquences des évolutions juridiques précitées.

### La balkanisation du droit de l'enquête

En ce domaine, la binarité doctrinale police administrative/police judiciaire vole en éclat pour introduire un degré de complexité supplémentaire. Ainsi, au sein de la police administrative, quatre familles de renseignement se sont-elles constituées qui répondent à des objectifs et des moyens de contrôle distincts et viennent parfois troubler la séparation des ordres :

- le renseignement de souveraineté concourt à la défense et à la promotion des intérêts fondamentaux de la Nation. Il se compose de deux cercles<sup>9</sup> de services, le premier d'entre eux accueillant la direction générale de la Sécurité extérieure (DGSE), la direction générale de la Sécurité intérieure (DGSI), la direction du Renseignement militaire (DRM), la direction du Renseignement et de la Sécurité de la défense (DRSD), la direction nationale du Renseignement et des Enquêtes douanières (DNRED) et Tracfin. L'ensemble de ce dispositif est placé sous le contrôle de la Commission nationale de contrôle des techniques de renseignement (CNCTR). La loi du 24 juillet 2015 constitue son principal cadre juridique ;
- mais, sous ce même régime, œuvrent également des services de police judiciaire de la direction centrale de la Police judiciaire (DCPJ), de la préfecture de Police de Paris (PP) ou de la direction générale de la Gendarmerie nationale qui agissent alors dans une zone d'indistinction communément appelée « pré-judiciaire ». Ils mobilisent donc des prérogatives administratives à des fins de judiciarisation. Si la CNCTR ne publie pas de statistiques par services demandeurs, sa prédécesseur, la Commission nationale de contrôle des interceptions de sécurité (CNCIS) avait eu l'occasion de souligner que près de la moitié des IS étaient mises en œuvre par des services agissant en pré-judiciaire<sup>10</sup> ;

(7) Google, Apple, Facebook, Amazon et Microsoft.

(8) Article L. 822-2 du CSI.

(9) En application des articles L. 811-2 et 4 du Code de la sécurité intérieure selon une capacité de recourir pleinement ou non aux techniques de recueil du renseignement. La liste des services composant chacun de ces deux cercles a été publiée par le biais du décret du 28 septembre 2015 et du décret du 11 décembre 2015.

(10) Cf. CNCIS, 21<sup>e</sup> rapport d'activité 2012-2013, p. 60 : « Le taux de clôture des demandes d'interception pour ouverture d'une procédure judiciaire [...] témoigne aussi de l'intérêt de ce dispositif de prévention et de police administrative qui permet d'exclure des hypothèses d'enquête et de stopper les mesures d'investigation avant toute phase judiciaire. Il ouvre aussi la possibilité, en cas de confirmation des soupçons quant à des projets d'infractions, de poursuivre par l'ouverture d'une procédure judiciaire avant la commission des faits, ce qui est particulièrement essentiel dans le cadre de la prévention des attentats terroristes ».

- en outre, le Service national du renseignement pénitentiaire, pourtant service de renseignement du deuxième cercle placé au sein du ministère de la Justice, jouit d'un double régime juridique : à la fois l'article L.855-1 du CSI qui le place sous le contrôle de la CNCTR, et l'article 727-1 du CPP qui confie sa supervision au procureur de la République. Cette entité recourt donc, concomitamment et pour les mêmes objectifs, aux deux types de police ;
- on pourrait, en dernier lieu, citer les prérogatives confiées aux services de police et de gendarmerie à la suite de la transposition dans le droit commun de certaines dispositions de l'état d'urgence, et notamment les mesures individuelles de contrôle administratif et de surveillance ou les visites domiciliaires<sup>11</sup>. Ces prérogatives administratives requièrent néanmoins l'intervention de l'autorité judiciaire.

La police administrative se distingue donc par son caractère peu monolithique et applique divers régimes, parfois complémentaires, parfois exclusifs les uns des autres. Un même service peut avoir à gérer des données collectées dans des cadres différents qui ne sauraient, en conséquence, être fusionnées.

Dans le même ordre d'idées, la police judiciaire connaît une diversification similaire :

- les services qui la composent assument des missions classiques de rassemblement des preuves participant à la manifestation de la vérité au profit de la Justice ; ils œuvrent au sein de la direction centrale de la Police judiciaire (DCPJ), de la préfecture de Police de Paris, mais aussi au sein de la direction centrale de la Sécurité publique (DCSP) ou encore de la sous-direction de la Police judiciaire de la gendarmerie nationale (SDPJ). Leur action est alors régie par le Code de procédure pénale (CPP) ;
- en parallèle, ces mêmes services peuvent déployer des activités pré-judiciaires telles que précitées ;
- en outre, la sous-direction de la Police judiciaire de la DGSI et la Sous-direction antiterroriste (SDAT) de la direction centrale de la Police judiciaire (DCPJ) agissent en matière de lutte contre le terrorisme très en amont de la commission d'une infraction grâce au délit d'association de malfaiteurs en relation avec une entreprise terroriste qui, par sa dimension préventive,

permet de mordre clairement sur le champ d'action de la police administrative ;

- enfin, le service d'Information, de Renseignement et d'Analyse stratégique sur la criminalité organisée (SIRASCO, au sein de la DCPJ) ou le service central de Renseignement criminel (SCRC, au sein de la gendarmerie nationale) s'inscrivent dans la sphère dite du « renseignement criminel ». Cette notion, dénuée de cadre législatif, recouvre à la fois une action pré-judiciaire et un soutien aux enquêtes judiciaires (en particulier pour le SCRC). L'indistinction semble donc cultivée, sans doute guidée par la maxime du cardinal de Retz selon laquelle « *On ne sort de l'ambiguïté qu'à ses dépens* ».

En définitive, un même service peut appartenir à une sphère et agir dans l'autre, voire dans les deux simultanément. À cet égard, la *summa divisio* importe moins dans ses conséquences organisationnelles que dans les cadres juridiques autorisés pour collecter les données nécessaires et les exploiter. Cette balkanisation du cadre juridique rend d'autant plus complexe l'alimentation des éventuels outils d'IA qu'elle souligne des lacunes majeures.

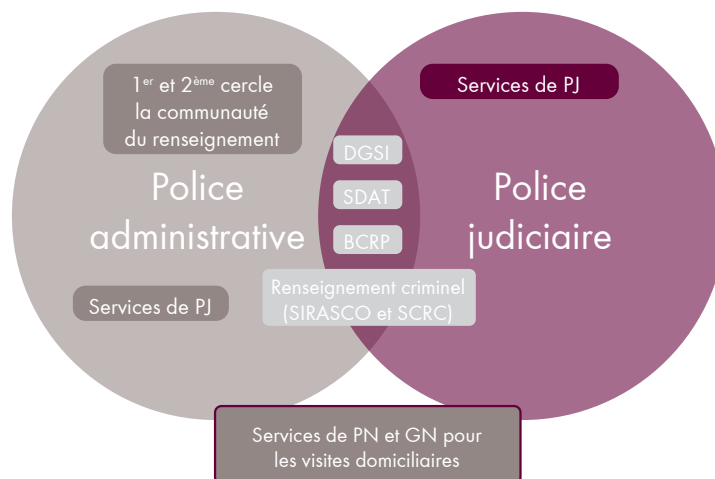
### Quelles perspectives juridiques pour l'exploitation des données recueillies par les services sous l'empire de la loi du 24 juillet 2015 ?

Plus que la notion générique et foisonnante de police administrative, le cadre juridique – et ici la loi relative au renseignement – s'avère pertinent comme cadre d'étude. Il s'agit d'ailleurs plus d'une loi-cadre inaboutie qu'une loi de techniques à proprement parler : la prévalence est accordée aux ingérences dans la vie privée plus qu'aux moyens d'ingérence. Ce caractère novateur explique certaines imprécisions notionnelles et une absence de prise en considération des besoins juridiques des outils d'IA.

En effet, ce texte pose un principe fondamental : une demande de technique de recueil du renseignement (TR) est individualisée tant en ce qui concerne sa cible (une personne ou un groupe de personnes, de manière exceptionnelle) que son commanditaire. À ce titre, l'article L. 821-2 du CSI, s'il ménage une sous-traitance ou une co-traitance (« *le service pour lequel elle est déposée* ») n'en pose pas moins le principe d'absence de mutualisation du produit

(11) Chapitres VIII et IX du titre II du livre II du CSI.





d'une TR. Il s'agit d'un principe qui limite la portée de l'ingérence dans la vie privée de la cible, pensé comme tel par le législateur. Cela relève d'ailleurs de la pure logique puisque les demandes de TR doivent être justifiées par l'un des motifs énumérés à l'article L. 811-3 du CSI et en fonction des missions respectives des services. Par conséquent, et sans que la loi n'explique ce raisonnement, le produit d'une TR ne peut faire l'objet d'une mutualisation entre services. Cela freine considérablement les capacités d'alimenter des outils d'IA.

L'existence de l'article L.863-2 du CSI renforce cette interprétation dans la mesure où il prévoit la capacité pour les services de renseignement d'échanger des données (ce faisant, la disposition souligne la nécessité d'une base juridique), mais également de solliciter ou de recevoir des informations provenant d'autres administrations. Cependant, le décret en Conseil d'État qui devait détailler les conditions de cet échange n'a jamais été pris.

Ces considérations posées, il apparaît que les services de renseignement peuvent appliquer sans peine un dispositif d'IA sur leur base de données interne. En revanche, l'application sur des éléments mutualisés soulève plus de questions. De même, l'interconnexion de fichiers, même temporaire, demeure très strictement encadrée par la CNIL qui la considère comme un nouveau traitement de données devant être soumis à autorisation. Indéniablement, les dispositions législatives limitent les facultés de déploiement de l'IA dans le légitime souci

du respect des droits fondamentaux. Le sujet se situait à ce titre en bonne place dans le discours du président de la République aux préfets, le 5 septembre 2018 : « *Pour améliorer l'exploitation des informations sept décrets relatifs aux fichiers de renseignement viennent d'être également publiés au début du mois d'août. J'ai également demandé au SGDSN<sup>12</sup> d'engager une réflexion sur la modernisation et les possibilités de croisement de certains de ces fichiers* ».

Il revêt, en effet, un intérêt particulier dans la mesure où les services de renseignement ont gagné, au fil des lois, de vastes droits de consultation de fichiers et que les recoupements sont effectués soit de manière manuelle (l'enquêteur consulte successivement différents fichiers), soit dans le cadre de cellules interagences dédiées (Hermès au sein du CPCO, Allat au sein de la DGSI). Le cadre juridique est donc respecté puisque aucune interconnexion informatique n'est opérée, l'ingérence dans la vie privée, au regard de la loi, existe sans pour autant s'avérer parfaitement efficace pour les enquêteurs du fait des moyens utilisés dans cet objectif.

En réponse à ces limites, cinq optiques paraissent envisageables :

- la première suppose une réécriture de l'article L. 863-2 dans le but d'inscrire dans la loi de plus amples précisions afin de se garder d'une éventuelle censure du Conseil constitutionnel pour incompétence négative<sup>13</sup>. On pourrait ainsi prévoir un régime d'échanges

(12) Secrétariat général de la Défense et de la Sécurité nationale (SGDSN).

(13) Cette hypothèse s'avère d'autant plus prégnante qu'un recours devant le Conseil d'État a été déposé le 25 juin dernier par la Quadrature du Net. Il porte spécifiquement sur l'article L. 863-2. Il est probable que l'association saisisse cette occasion pour déposer une question prioritaire de constitutionnalité.

de données, voire d'effacement, soumis au contrôle de la CNCTR ou de la formation spécialisée du Conseil d'État compétente en matière de contentieux lié aux TR et aux fichiers de souveraineté [Évolution n° 1] ;

- à défaut, pourquoi ne pas imaginer, sur la base de cet article, la création d'un fichier de souveraineté thématique, déclaré à la CNIL, afin d'exploiter les données collectées ? [Évolution n° 2]. Certes, la jurisprudence du Conseil constitutionnel se montre peu clément à l'égard des traitements généraux de données. Mais on peut légitimement estimer qu'un fichier de souveraineté thématique (lutte contre le terrorisme ou contre-espionnage) ne rencontrerait pas d'objection ;
- la troisième option consisterait à promouvoir le principe d'une interface « hit/no hit » appliquée aux fichiers des services de renseignement (sur le modèle du Fichier national des objectifs en matière de stupéfiants, FNOS) : les recoupements pertinents induiraient un « hit » qui donnerait lieu à une levée d'anonymat, selon les modalités prévues à l'article L. 851-3 relatif à la surveillance algorithmique (demande à la CNCTR qui statue). Toutes les potentialités des fichiers ne seraient pas exploitées, mais il s'agirait d'une avancée très notable [Évolution n° 3] ;
- la quatrième supposerait l'interconnexion de fichiers aux données pseudonymisées qui, en cas de recoupement pertinent, entraînerait une levée de pseudonyme selon le mécanisme décrit ci-avant [Évolution n° 4]. Afin de pleinement respecter la logique de la loi de 1978, sans doute faudrait-il anonymiser certaines données et en pseudonymiser d'autres dans l'objectif de limiter le risque concernant la vie privée des personnes concernées ;
- enfin, et prenant en compte la doctrine de la CNIL en matière d'interconnexion, cette dernière pourrait devenir une technique de recueil du renseignement à part entière : soumise à autorisation du Premier ministre après avis de la CNCTR, elle serait mise en œuvre



DES MODIFICATIONS LÉGISLATIVES QUI NE CHANGERAIENT PAS RADICALEMENT L'APPROCHE FRANÇAISE SONT ENVISAGEABLES POUR OFFRIR À DES DISPOSITIFS D'IA UN TERRAIN D'ACTION PLUS CONSÉQUENT QU'AUJOURD'HUI, AU PROFIT DES MISSIONS DES SERVICES DE RENSEIGNEMENT ET DANS LE RESPECT DES DROITS FONDAMENTAUX. EN REVANCHE, LA POLICE JUDICIAIRE SEMBLE BÉNÉFICIER DE MARGES DE MANŒUVRE AMOINDRIES.



de manière temporaire concernant un individu. Les renseignements sans lien avec la demande seraient détruits dans les plus brefs délais et ne seraient conservés que ceux en lien direct avec la demande formulée pendant 30 jours. La CNCTR exercerait un contrôle *a priori* et *ex post* [Évolution n° 5]. Cette perspective a le mérite de s'insérer dans un cadre légal précis, lequel met en œuvre les principes de proportionnalité (voire de subsidiarité) en même temps qu'il offre des mécanismes de contrôle et des voies de recours, y compris juridictionnel. Les garanties apportées justifieraient pleinement la

mise en œuvre de cette mesure.

Des modifications législatives qui ne changeraient pas radicalement l'approche française sont envisageables pour offrir à des dispositifs d'IA un terrain d'action plus conséquent qu'aujourd'hui, au profit des missions des services de renseignement et dans le respect des droits fondamentaux. En revanche, la police judiciaire semble bénéficier de marges de manœuvre amoindries.

### **Le renseignement judiciaire borné par la jurisprudence du Conseil constitutionnel**

En principe, les capacités judiciaires en matière de travail sur les données ne connaissent guère de limitations. Toutefois, la Représentation nationale a peu légiféré sur ce sujet et les mécanismes d'exploitation ont été encadrés par la jurisprudence du Conseil constitutionnel.

En effet, deux dispositifs existent dans notre droit qui permettent de fusionner des données afin de leur appliquer un traitement d'IA : l'analyse sérielle appliquée aux crimes et délits présentant un caractère sériel punis d'au moins 5 ans de prison, et le rapprochement judiciaire mis en œuvre à l'occasion d'une enquête portant sur des infractions de petite et moyenne gravité. Dans les deux cas, mais selon des paramètres variables (cf. tableau ci-après), les officiers de police judiciaire peuvent croiser

	Analyse sérielle	Rapprochement judiciaire
Objet	Rassemblement des preuves et identification des auteurs	
Base juridique	230-12 à 18 CPP R40-35 à 37 CPP Décret du 22 novembre 2013	230-20 à 27 CPP R40-39 à 41 CPP
Modalité d'autorisation	Décret en CE après avis CNIL pour les services de PN et GN chargés d'une mission de PJ	
Infractions concernées	Crimes et délits présentant un caractère sériel punis d'au moins 5 ans de prison	À préciser dans le décret en CE. Selon la CNIL, les infractions de petite et moyenne gravité ; selon le Gouvernement celles punies de moins de 5 ans d'emprisonnement
Contexte d'utilisation	Permanent	Pour les seuls besoins d'une enquête déterminée, sur autorisation du magistrat ou sauf décision contraire en cas de flagrance. Aucune finalité statistique.
Trace en procédure	Non	- Mise en œuvre mentionnée - Rapport de fin d'exploitation
Sources	Fichiers résultant des infractions concernées : - enquêtes préliminaires ou de flagrance - investigations sur commission rogatoire - recherche des causes de la mort ou d'une disparition	
Abondement	Recherches supplémentaires autorisées	Recherches supplémentaires interdites
Identification	- auteurs ou complices établis ou supposés - indicateurs cités en procédure - victimes et disparus	Uniquement si non fortuite
Conservation des données personnelles révélées	Données effacées : - quand personne retrouvée - quand auteurs ou complices présumés, indicateurs ou victimes le demandent, sauf avis contraire du magistrat - au bout de 15 ans pour les délits/20 ans pour les crimes <sup>14</sup>	Données personnelles effacées : - à la clôture de l'enquête ou dans les 3 ans - lorsque personne retrouvée ou crime écarté
Données personnelles du I de l'art. 8 loi 1978	Oui (prévu par la loi)	À indiquer dans le décret
Contrôle	- CNIL - procureur de la République compétent - magistrat référent	
Modalités de contrôle	Magistrat référent sollicite des éléments	Le Procureur et le magistrat référent disposent d'un accès direct
Traçabilité	Prévue dans le décret	Non précisée

(14) Pour l'analyse sérielle, la CNIL accepte des délais de conservation supérieurs à la prescription, mais souhaite un effacement automatique (délibération du 20 septembre 2012 portant avis sur un projet de décret relatif à la mise en œuvre de fichiers d'analyse sérielle dénommés « bases d'analyse sérielle de police judiciaire »).

certaines données afin d'établir des correspondances en vue de concourir à l'élucidation d'une affaire.

Ces dispositions législatives semblent répondre aux besoins juridiques identifiés. Pourtant, dans sa décision n° 2011-625 DC du 10 mars 2011 (considérant 71), le Conseil constitutionnel a très strictement encadré ce second dispositif en réalisant des considérations de portée générale. Il n'approuve pas la possibilité de : « mise en œuvre d'un traitement général des données recueillies à l'occasion des diverses enquêtes ». En outre, il a restreint le rapprochement judiciaire aux « seuls besoins de ces investigations ». De fait, il ne peut exister un fichier abondé par des enquêtes judiciaires pour aider à la résolution de tous les crimes et délits, sans distinction de gravité, pour une durée illimitée.

Ces réserves d'interprétation, conséquentes, sont-elles incapacitantes pour les activités de police judiciaire ? Cela paraît douteux. En premier lieu, les crimes et délits punissables de moins de 5 ans de prison représentent l'écrasante majorité de l'activité des tribunaux et le rapprochement judiciaire leur est donc applicable. Au-dessus de ce *quantum* de peine, les crimes sériels bénéficient de l'analyse sérielle tandis que terrorisme et criminalité organisée relèvent généralement du champ administratif ou pré-judiciaire en même temps qu'ils bénéficient de dispositions spécifiques au sein du CPP (principalement des techniques spéciales d'enquête). Si l'on excepte le besoin d'interconnexion des fichiers, la zone non couverte pour ces dispositions légales dans un domaine purement judiciaire de répression des infractions constatées semble assez restreinte ; suffisamment restreinte pour ne pas nuire au travail habituel des enquêteurs et justifier de tenter un revirement jurisprudentiel du Conseil constitutionnel. En revanche, certaines des propositions formulées plus haut, nourries des mêmes constats, trouveraient à s'adapter au cadre judiciaire. En effet,

- le principe d'une interface « hit/no hit » aiderait les enquêteurs à recouper différentes bases dont ils disposent [Évolution n° 6] ;
- de même, l'interconnexion de fichiers aux données pseudonymisées qui, en cas de recoupement pertinent, donnerait lieu à une levée de pseudonyme sur réquisition judiciaire paraîtrait utile [Évolution n° 7] ;
- enfin, l'interconnexion pourrait gagner le statut de technique d'enquête spéciale sur réquisition judiciaire individualisée et temporaire. Le contrôle de ces opérations et notamment de l'effacement à échéance de l'enquête serait confié à un magistrat ainsi qu'à la CNIL [Évolution n° 8].

En définitive, les évolutions nécessaires au cadre d'enquête judiciaire paraissent relativement limitées en dehors de la question de l'interconnexion des fichiers. Elles n'en demeurent pas moins souhaitables afin de préserver un équilibre entre police judiciaire et police administrative, au profit de l'œuvre de Justice. Ce constat soulève plus de difficultés lorsqu'il s'agit d'envisager des moyens d'anticiper la criminalité.

### **Le renseignement criminel : avant-garde ou combat perdu d'avance ?**

Lorsqu'ils viennent en appui d'enquêtes judiciaires, les services de renseignement œuvrent dans un cadre balisé, celui du pré-judiciaire précédemment évoqué. En revanche, le renseignement criminel suppose une démarche proactive d'anticipation et d'analyse des phénomènes criminels qui dépasse le seul rassemblement des preuves dans le but de la manifestation de la vérité. La question se pose dès lors de savoir si le renseignement criminel appartient au domaine administratif – y compris dans sa déclinaison pré-judiciaire –, au domaine judiciaire, ou s'il constitue une voie tierce.

On peinerait à saisir les éléments qui justifieraient de sortir du cadre de la *summa divisio* précitée dans le cas du renseignement criminel. Il constitue une activité non de répression, mais de prévention et appartient, de ce fait, pleinement au domaine administratif. Au sein de ce dernier, il ne relève pas du renseignement de souveraineté (caractérisé par l'extrême acuité de la menace) et correspond à ce que l'on pourrait désigner comme du « renseignement pré-judiciaire de bas de spectre » (sans connotation négative puisque la notion s'inspire de la lutte antiterroriste qui se répartit entre « haut de spectre » – relevant de la DGSJ et du renseignement de souveraineté – et le « bas de spectre », déterminé selon le degré de menace et l'imminence du passage à l'acte et qui incombe notamment au service central du Renseignement territorial). Car les faits concernés par une enquête du renseignement criminel ne sauraient être graves (en dessous d'une peine de cinq années d'emprisonnement encourues) sous peine de voir apparaître des dispositifs redondants.

Une fois acté cela, demeure la question de l'instance de contrôle. Celui-ci peut échoir à une autorité administrative indépendante (CNCTR, personnalité qualifiée), mais également à l'autorité judiciaire (à l'instar du Service national du renseignement pénitentiaire qui, pour la prévention des évasions et les questions de sécurité pénitentiaire – activités préventives et non répressives

– relève du contrôle du procureur de la République en application de l'article 727-1 du CPP).

On pourrait dès lors imaginer la création d'un traitement automatisé de données spécifique au renseignement criminel qui mêlerait données administratives et judiciaires [Évolution n° 9], comme le Conseil constitutionnel en ouvre la possibilité dans sa décision 2003-467 DC du 13 mars 2003 : « aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire » dans la mesure où l'objet n'est pas général. Cela supposerait d'assigner certains objectifs précis au renseignement criminel (atteintes aux biens et aux personnes par exemple) afin d'en circonscrire le périmètre et de respecter la jurisprudence constitutionnelle.

Dans le même ordre d'idées, cette entité de renseignement criminel pourrait intégrer le deuxième cercle de la communauté du renseignement ou devenir l'une des branches d'un des services de la communauté [Évolution n° 10] et ainsi pleinement bénéficier du cadre juridique en vigueur, voire des cinq propositions d'évolutions législatives formulées plus haut.

À rebours, une inscription pleine et entière dans le cadre judiciaire priverait le renseignement criminel :

- des données administratives, en particulier celles protégées au titre du secret de la défense nationale puisque, par nature, elles n'ont pas vocation à être versées en procédure sauf lorsqu'il en est décidé autrement ;
- de l'opportunité d'apprécier le recours à l'article 40 du CPP lorsqu'un enquêteur souhaite mener à bien des enquêtes plus approfondies ;
- des bénéfices d'un travail d'anticipation qui, par définition, ne répond pas aux mêmes exigences de preuve qu'une enquête judiciaire et gagne ainsi en souplesse ;
- de la conduite d'un fragment de politique publique en matière de sécurité publique puisqu'elle confierait cette mission à l'autorité judiciaire, en contradiction avec notre système actuel.

De telle sorte que tout plaide en faveur de l'émergence d'un renseignement criminel pleinement inscrit dans la sphère administrative afin de développer une analyse de la délinquance et de la criminalité du quotidien et de gagner en capacité de réaction sur ce secteur.

## Conclusion

L'irruption de l'intelligence artificielle dans notre quotidien constitue l'une des principales mutations technologiques de ce début de siècle. Pour l'univers des services de renseignement et d'enquête, elle pourrait induire une mutation majeure dans la conduite des investigations. Car, face à un agent débordé par les données hétérogènes et un bruit numérique toujours plus présent, elle incarnerait un gain de temps et d'efficacité au service de la sécurité de nos concitoyens. En effet, en distinguant de la masse des informations l'élément probant ou le signal faible, la capacité d'anticipation et de répression s'en trouverait affermie.

Mais pour que l'usage de l'IA soit pleinement fructueux, il conviendrait de nourrir cet outil (car il s'agit d'un instrument plus que d'une méthode) de données – nettoyées<sup>15</sup>. Or, le champ de la sécurité impose légitimement des restrictions afin que l'objectif final ne prévale sur les droits et libertés individuels. Cela nécessite de conférer à ce nouvel outil un cadre juridique clair et des moyens de contrôle efficaces. La démarche suppose également d'avoir précisément défini les objectifs assignés à sa mise en œuvre et, par voie de conséquence, les missions des services utilisateurs.

Et, plutôt que d'adapter des solutions sur étagère à un contexte juridique particulier, la définition de l'outil pourrait s'opérer selon un principe de « *Legal by design* », option destinée à exploiter au maximum l'ensemble des dispositions législatives tout en assurant le plus haut niveau de protection pour les droits fondamentaux. La norme, loin de passer pour une contrainte, viendrait structurer le fonctionnement des outils des enquêteurs. Il s'agit une nouvelle philosophie d'approche qui est requise, au profit de la sécurité mais aussi d'une démarche industrielle souveraine ■

(15) C'est-à-dire purgées d'erreurs de saisies ou de catégorisation par exemple, mais aussi respectant le cadre juridique de conservation.



## Algorithmes prédictifs pour la police et la justice : nouveaux oracles ou simples outils de gestion du risque ?

Léo AMSELLEM, Vincent BERTHET<sup>1</sup>

Léo AMSELLEM



Léo Amsellem est diplômé de Sciences Po Paris en science politique et de l'Université Sorbonne

Paris-IV en philosophie. Il est étudiant-chercheur à la London School of Economics (LSE) en économie européenne.

Vincent BERTHET



Vincent Berthet est maître de conférences à l'université de Lorraine et chercheur associé au

Centre d'économie de la Sorbonne. Il est docteur en sciences cognitives et diplômé en science politique de l'université Paris 1 Panthéon-Sorbonne. Il est l'auteur de *L'erreur est humaine - Aux frontières de la rationalité*, paru chez CNRS Éditions (2018).

Dès 1956 dans sa nouvelle *Minority Report* – adaptée avec succès au cinéma par Steven Spielberg – Philip K. Dick imagine une ville en 2054 parvenue à éradiquer la criminalité sanglante. La formule est simple : des *precogs*, humains dotés du don de précognition, avertissent l'unité pré-crime avant la survenance d'un meurtre. Leur vision quasi infallible de l'avenir est garante de la fiabilité du système. L'idée fondamentale associée à *Minority Report* est aussi simple que

puissante : décider ou agir sur le fondement d'une prédiction. La réalité a déjà rattrapé la fiction. En effet, le Parlement britannique adopte le *Children Act* dès 1989, sous le gouvernement de Margaret Thatcher. Cette loi, toujours en vigueur, vise à protéger les enfants d'éventuels actes de maltraitance qui pourraient survenir dans leur foyer. Elle permet aux services sociaux britanniques de retirer leurs enfants à des parents présentant une « probabilité de faire du mal » trop élevée. La France n'est pas non plus étrangère à cette logique de prévention : la loi du 25 février 2008 relative à la rétention de sûreté prévoit la possibilité d'une privation de liberté intervenant après l'exécution de la

(1) Vincent Berthet et Léo Amsellem publient en 2020 un ouvrage chez CNRS éditions sur les algorithmes prédictifs et leur utilisation par les services de l'État dans les domaines de la police, de la justice et de la reconnaissance faciale.

peine. Lorsque le droit prévoit la possibilité de retenir un détenu avant qu'il ne commette son forfait, la réalité juridique s'approprie le changement de paradigme illustré dans *Minority Report*. Le commentaire de Robert Badinter à l'époque était d'ailleurs sans équivoque : « *À la justice de liberté fondée sur la responsabilité de l'auteur prouvé de l'infraction, va succéder une justice de sûreté basée sur la dangerosité diagnostiquée de l'auteur potentiel d'un crime virtuel* ». Cet article traitera d'abord des nouvelles méthodes de prédiction policière, avant de développer une analyse de la prédiction de la récidive dans la justice pénale. Enfin, il proposera une réflexion sur le tournant que représente l'avènement d'une société de la prédiction.

## Anticipés coupables : l'ère de la prédiction policière

L'apport des méthodes prédictives au domaine policier relève d'un véritable changement de paradigme. Par essence, l'action de la police est davantage tournée vers la répression des crimes et des délits, elle agit en réaction à un événement illicite ou illégal. Pourtant, des modèles mathématiques sont apparus qui permettraient non seulement d'améliorer l'action des unités de police, mais aussi et surtout de prédire le crime, de l'anticiper. Prédire pour prévenir, tel pourrait être leur nouveau mantra. Une publicité d'IBM met en scène sur un ton humoristique un braqueur de station essence qui s'équipe, se prépare mentalement à commettre son forfait, pour finalement arriver sur le lieu du futur crime et y trouver un policier qui l'attend en buvant tranquillement un café. Économique en effectifs de police, cette technologie épargnerait donc aux victimes de subir un crime, serait efficace, voire infaillible. Mais cette mise en scène est-elle seulement proche de la façon dont les algorithmes de police prédictive procèdent ? Ces derniers sont-ils plus proches de l'univers futuriste des *precogs* de *Minority Report* ou de simples améliorations des outils de police déjà en vigueur ?

La police prédictive est l'application d'un ensemble de méthodes (principalement quantitatives) visant à identifier des objectifs en vue d'interventions policières, de prévenir le crime. Ces algorithmes prédictifs, qui se veulent de véritables « devins du crime », sont nés en Californie avec la création de Predpol en 2006. Ils sont la parfaite hybridation entre les fantasmes futuristes hollywoodiens et l'extraordinaire capacité d'innovation de la Silicon Valley. Ils sont le fruit d'une étonnante collaboration entre anthropologues et sismologues. S'il est difficile pour les sismologues de prévoir un tremblement de terre, il

semble en revanche plus aisé, une fois le séisme survenu, de prédire ses répliques. La prédiction ne se fonde pas sur une connaissance théorique mais empirique. De même, les pionniers de la police prédictive considèrent que le comportement humain est répétitif et donc prédictible. Il est dès lors possible d'utiliser les bases de données de la délinquance constatée pour prédire l'occurrence des prochaines infractions. Rappelons tout de même que ces dispositifs ne concernent pas la criminalité sanglante, dont les faits sont trop rares et incertains pour former une base de données suffisante. La méthode s'intéresse surtout aux faits de criminalité courants sur la voie publique : vols de voiture, cambriolages, petits délits, dégradations, vente de drogues au détail. De plus, contrairement aux scénarios de science-fiction et aux publicités, ces dispositifs prédictifs ne s'attachent en général pas à prédire quel individu va commettre ou être victime d'un crime mais plutôt dans quel lieu un délit sera commis – à l'exception de deux dispositifs à l'épreuve à Los Angeles et Chicago.

Le postulat de la méthode prédictive est le suivant : trois facteurs permettent de quantifier statistiquement le risque qu'un acte de délinquance soit commis. Il s'agit du type de délinquance, du lieu, et du moment. Les données sont issues des statistiques de la délinquance enregistrées précédemment. Avec une base de données suffisamment importante, on peut commencer à déceler les « patterns », les schémas de la criminalité qui se répètent. Il faut ensuite modéliser la ville ou la zone géographique et la diviser en carrés d'aires égales. Ce quadrillage peut être très précis. Jusqu'à ce point, il ne s'agit que d'une amélioration des cartes de chaleur dont disposait déjà la police. Le logiciel Predpol est justement le descendant du logiciel Promap, qui cartographie la criminalité. Mais l'intelligence artificielle permet non seulement de faire une analyse plus complète quantitativement, mais aussi d'agréger et de pondérer d'autres critères pour affiner la recherche, qui sont supposés apporter le caractère véritablement prédictif et novateur. Il s'agit de critères exogènes ayant une influence sur le crime : horaire de lever et coucher du soleil, données météorologiques, présence d'un bar ou d'un point de distribution d'alcool, proximité avec un carrefour de transports en commun, etc. Une base de données initiales importante et des données exogènes précises permettent ainsi de construire un outil prédictif de meilleure qualité. Avec cette information, il devient aisé de déployer les patrouilles disponibles dans les lieux où elles seront les plus utiles, si on prend comme mesure de l'efficacité pour une patrouille de police le fait d'empêcher un crime ou de le constater et d'appréhender les auteurs.

Mais la prédiction policière souffre de limites techniques et pose des questionnements de fond. D'abord, la mise en place de telles méthodes nécessite de disposer de

vastes bases de données sur la criminalité passée. Encore faut-il pour cela l'enregistrer rigoureusement et de façon intelligible pour un ordinateur. Dans le cas français, les statistiques de la délinquance sont compilées dans l'état 4001, qui n'est pas exempt de critiques. Dans l'état actuel, il pourrait difficilement servir de base à la mise en place d'un système de police prédictive d'ampleur nationale. La pertinence de cet outil pour orienter l'action des forces de sécurité n'apparaît pas immédiatement. Dès lors, peut-on imaginer des algorithmes auto-apprenants qui se nourriront directement de cette matière ? Pour chacun des 107 index de l'état 4001 correspond une unité de compte (soit fait, soit victime, soit auteur, etc). Construire un algorithme se basant sur un ensemble si divers peut paraître hasardeux. Par ailleurs, il faudrait également s'assurer de l'approbation de telles techniques au sein des forces de police et de gendarmerie sur le terrain afin de permettre une utilisation optimale de ces nouveaux outils.

Mais au-delà de défis techniques, c'est une analyse en profondeur de l'efficacité et des conséquences sur la société de ces algorithmes qui est nécessaire. Identifions deux critiques principales : l'inefficacité présumée et l'effet de rétroaction. La première revient à interroger les résultats exceptionnels promis par les entreprises qui commercialisent ces algorithmes. Elles s'appuient pour cela sur leur réussite démontrée dans certaines localités (surtout américaines) dans lesquelles elles ont pu se déployer. Pourtant, la ville de Richmond, près de San Francisco, a décidé de rompre son contrat avec le *leader* du marché Predpol. L'entreprise a longuement maintenu sur son site l'exemple de Richmond comme celui d'un succès évident, attesté par les chiffres. Mais d'après les autorités de la ville, cette analyse serait fallacieuse en ce qu'elle présenterait la baisse de la criminalité comme la conséquence de leur action, alors que cette baisse est tendancielle depuis plus d'une décennie, soit bien avant le contrat conclu avec Predpol. Ce serait donc confondre corrélation et causalité, peut être volontairement. Or, c'est un véritable problème : nous soutenons l'idée que pour décider d'utiliser ou non des algorithmes, il est important d'établir un calcul coût-avantage. Or, pour ce qui est des avantages, il est difficile dans la plupart des situations dans lesquelles de tels logiciels ont été utilisés, d'établir avec certitude qu'un résultat est le fruit de leur action et non d'un autre facteur. En effet, trop de facteurs rentrent en jeu dans la définition de la délinquance : des facteurs sociaux, mais aussi l'organisation et l'intensité de l'action de police. Il faut se souvenir que les chiffres dont on dispose sont ceux de la criminalité ou de la délinquance perçue par les services et non pas de la criminalité ou de la délinquance totale d'une ville ou d'un secteur. C'est donc un reflet de l'appréhension de la délinquance par la police. En mars 2019, un audit interne du Los Angeles

Police Department (LAPD) concluait qu'il n'y avait pas suffisamment de données pour conclure favorablement sur l'efficacité de Predpol. Or, pour Predpol, le LAPD est à la fois la principale vitrine, mais aussi l'institution qui a contribué à les fonder en soutenant leur recherche à l'université de Californie à Los Angeles (UCLA).

Par ailleurs, ces algorithmes tendent à concentrer l'action de police dans des zones fortement criminogènes, ce qui peut sembler rationnel puisque la probabilité d'assister à un délit ou de l'empêcher y sera plus forte qu'ailleurs. Mais ce faisant, il s'agit d'une simple application de la loi de Pareto, datant du XIX<sup>e</sup> siècle, selon laquelle 80 % des faits se produisent dans 20 % du territoire. Les policiers qui opèrent de façon traditionnelle connaissent d'ailleurs bien ces lieux et y concentrent souvent leur action. Pour démontrer que le logiciel Predpol n'est pas si novateur, le chercheur français Ismael Benslimane a utilisé la méthode dite de la « rétro-ingénierie ». En effet, puisqu'ils sont commercialisés par des entreprises à des fins lucratives, le code de ces algorithmes n'est pas rendu public. Les chercheurs doivent procéder à rebours : partir des fonctionnalités et usages du programme, pour en deviner le code. Ismael Benslimane a donc créé son propre algorithme pour le comparer à Predpol et l'utiliser comme contrefactuel. Ses conclusions sont sans appel : un simple algorithme pondérant les déplacements de police aux taux de criminalité connus des territoires quadrillés peut faire aussi bien que Predpol. Il en déduit donc que Predpol n'a rien de prédictif. Pour lui, c'est une simple « carte de chaleur » améliorée. Son expérience démontre une règle simple : on bat les prédictions aléatoires, comme Predpol, en concentrant l'action des services de police sur un secteur toujours plus restreint. D'autant que ces dispositifs sont souvent auto-évalués et que les unités de police peuvent être amenées à valider les prédictions de l'algorithme s'ils pensent avoir dissuadé des individus de commettre un délit ; sentiment d'autant plus répandu dans une zone criminogène.

Notre seconde interrogation concerne l'effet de rétroaction. Cette analyse est partagée par Bernard E. Harcourt, de l'université de Chicago [Harcourt, 2011]. Il estime que les méthodes visant à « profiler » le plus précisément possible les catégories de populations susceptibles d'être délinquantes, *a fortiori* par algorithmes, selon la méthode actuarielle, présentent un « coût social négligé ». Celui-ci serait le fait d'une discrimination statistique. En effet, Harcourt se fonde sur la distinction entre délinquance réelle et délinquance appréhendée par les services de police. Il prend l'exemple d'une minorité, qui représenterait 25 % de la population totale. En revanche, cette minorité serait responsable de 45 % de la délinquance. Il serait donc rationnel pour les services de



police de cibler les individus de cette minorité, même sans aucun *a priori* raciste : ce serait juste plus efficace si l'objectif est bien d'arrêter plus de délinquants, dans l'objectif assumé de réduire la criminalité. Présumons donc de la parfaite objectivité des forces de police, qui n'agissent que selon la logique de maximiser les arrestations. Ce faisant, cette minorité représentera 67 % des délinquants repérés et appréhendés. Il y a donc un effet de distorsion. Or, l'effet pervers de cette situation est à l'origine d'un cercle vicieux : d'une part, cela confirme la stratégie de la police, qui peut l'intensifier encore. D'autre part, les membres de cette minorité seront donc plus souvent incarcérés, moins susceptibles de poursuivre des études ou de trouver un emploi, donc auront davantage d'incitations à se tourner vers la délinquance et à récidiver. Validant une nouvelle fois la prédiction initiale, devenue performative. Harcourt va plus loin, en rappelant qu'« *une condamnation et une incarcération de longue durée n'affectent pas seulement les individus ciblés, mais aussi les communautés dont ils sont issus, produisant des effets rétroactifs sur celles-ci et d'autres* ». C'est ce qu'Harcourt qualifie d'« *effet de cliquet* » ; il s'agit d'un engrenage.

Cependant, rappelons que si un biais existe, c'est parce que les données utilisées pour entraîner l'algorithme comportent ce biais. Or, ces données, qui correspondent aux statistiques de la délinquance, sont le reflet des pratiques des forces de police. Autrement dit, si un biais racial se retrouve dans un algorithme, c'est avant tout parce que ce biais caractérise la pratique humaine. Idem pour la concentration de l'activité de police dans certaines zones. Les algorithmes sont ainsi jugés plus durement que leurs collègues humains. Le bouleversement provoqué par leur développement doit justement être l'occasion d'un grand débat public, auquel doivent participer les citoyens qui veulent redéfinir les principes de leur police et ainsi contribuer à la structuration d'une nouvelle relation entre police et population. Il faut aussi remettre en cause la portée « prédictive » de ces outils, appellation marketing, et les voir plutôt comme une amélioration des outils de police déjà en vigueur. Il s'agit surtout de mieux modéliser et comprendre la délinquance pour organiser la réponse la plus adaptée. Ce sont des outils de gestion du risque, d'estimation de probabilités. À cet égard, ils sont donc plus proches d'outils actuariels que des *precogs* de *Minority Report*. Contrairement à ce que la publicité d'IBM met en avant, l'utilité n'est pas vraiment d'interpeller avant la survenance d'un délit. Le colonel de gendarmerie du groupement Nord, Philippe Mirabaud, rappelait à juste titre lors d'un colloque à l'INHESJ en 2017 : « *on n'est pas du tout dans une logique de prévoir le fait pour faire du flagrant délit. On est dans une logique de comprendre quelle est la délinquance à laquelle nous faisons face, et en conséquence, comment nous devons nous organiser* ». C'est d'ailleurs le sens de l'expérimentation de Predvol dans l'Oise par les forces de gendarmerie,

logiciel censé prédire les vols de voitures en agrégeant 650 variables pertinentes. Il a été abandonné l'an dernier au profit du logiciel Paved. Ce dernier n'a pas de prétention prédictive, mais consiste seulement en une carte de chaleur d'usage très simple. C'est aussi l'apport de ces nouvelles technologies venues de l'économie numérique : elles sont d'un usage simple, permettent une bonne visualisation, participent de la rationalisation des effectifs déployés. Elles sont des améliorations, des évolutions des systèmes déjà existants. Il faut donc sans doute dédramatiser leur portée prédictive, leur vocation « d'oracle » pour préférer les analyser en tant qu'outils de gestion et de visualisation prometteurs qui peuvent avoir une utilité et sont voués à s'améliorer dans les prochaines années.

## Prédire et juger : les algorithmes prédictifs dans la justice pénale

Le lien entre prédiction et décision prend tout son sens dans le cas de la justice pénale. En effet, certaines décisions pénales reposent sur une prédiction relative au comportement futur des détenus. Pour décider s'il accorde ou non la libération conditionnelle à un détenu, le juge de l'application des peines se demandera d'une façon ou d'une autre « Quel est le risque que cet individu récidive s'il est remis en liberté ? ». Dans certains pays, la réponse à cette question est fournie en quelques minutes par un algorithme qui réalise des statistiques sur un large ensemble de cas passés similaires. L'utilisation des algorithmes prédictifs dans la justice pénale est croissante, cette évolution marquant un glissement de l'expertise humaine vers une approche objective. Ces outils suscitent à la fois optimisme et réticences. En principe, ils ont la possibilité de corriger la faillibilité des juges : leur tendance à surestimer le risque de récidive (produisant une surincarcération), leur subjectivité (produisant un aléa judiciaire), et leurs biais (produisant une discrimination). Néanmoins, ces outils présentent aussi le risque de reproduire certains biais, auquel cas leur utilisation généralisée institutionnaliserait une certaine inégalité des justiciables devant la loi. L'utilisation de ces outils pose également un ensemble de questions, à la fois philosophiques, juridiques, et techniques. Peut-on juger un détenu sur la base d'un calcul statistique de son risque de récidive ? Est-il juste de juger un cas particulier sur la base de cas similaires passés ? Comment s'assurer que les algorithmes ne sont pas biaisés ?

Construits sur la base de données historiques (des millions de cas déjà jugés issus de centaines de juridictions américaines), des algorithmes prédisent à partir de



LE LIEN ENTRE PRÉDICTION ET DÉCISION PREND TOUT SON SENS DANS LE CAS DE LA JUSTICE PÉNALE. EN EFFET, CERTAINES DÉCISIONS PÉNALES REPOSENT SUR UNE PRÉDICTION RELATIVE AU COMPORTEMENT FUTUR DES DÉTENUS. POUR DÉCIDER S'IL ACCORDE OU NON LA LIBÉRATION CONDITIONNELLE À UN DÉTENU, LE JUGE DE L'APPLICATION DES PEINES SE DEMANDERA D'UNE FAÇON OU D'UNE AUTRE « QUEL EST LE RISQUE QUE CET INDIVIDU RÉCIDIVE S'IL EST REMIS EN LIBERTÉ ? ». DANS CERTAINS PAYS, LA RÉPONSE À CETTE QUESTION EST FOURNIE EN QUELQUES MINUTES PAR UN ALGORITHME QUI RÉALISE DES STATISTIQUES SUR UN LARGE ENSEMBLE DE CAS PASSÉS SIMILAIRES.



facteurs relatifs à l'histoire pénale du prévenu (son casier judiciaire) et de facteurs sociodémographiques (âge, sexe, emploi, situation familiale, etc.) un niveau risque (par exemple au travers d'un score de risque allant de 1 à 10). L'individu est-il un homme ou une femme ? A-t-il moins de 21 ans ? Combien de fois a-t-il été arrêté auparavant ? Dans le secteur pénal, la prédiction du comportement était déjà un enjeu avant l'essor des algorithmes prédictifs, les criminologues et psychologues ayant travaillé sur l'estimation du risque de récidive dès les années 1920. L'arrivée des données massives et des techniques d'IA a permis de donner une autre ampleur aux outils prédictifs, mais il s'agit davantage d'un changement de degré plutôt que de nature. Ces outils sont initialement utilisés pour les décisions pénales qui reposent le plus sur une estimation du risque de récidive : la décision de mise en détention provisoire et l'application des peines. En effet, ces deux décisions reposent essentiellement sur la réponse à la question : quelles sont les chances que cet individu récidive ? Mais depuis quelques années, ces outils tendent à être utilisés aussi pour la détermination de la peine dans certains États américains (l'État de Virginie par exemple). Contrairement aux décisions précédentes, la fixation de la peine par le juge du fond ne repose pas seulement sur la prédiction de la récidive, car la peine remplit plusieurs fonctions. Par exemple, elle inflige une sanction à l'individu pour ce qu'il a commis (fonction rétributive) et elle dissuade les potentiels criminels. Quoiqu'il en soit, cette généralisation de l'utilisation des outils prédictifs

est sous-tendue par une volonté de rationalisation de la justice pénale : tendre vers une justice plus objective, plus transparente, plus performante, plus rapide, bref, plus efficace.

Dans un contexte où l'efficacité de la justice est souvent questionnée en raison de ses ressources limitées, l'utilisation d'algorithmes présenterait deux vertus majeures. D'une part, elle permettrait de rendre la justice pénale plus efficace. En effet, la décision pénale est de toute façon fondée sur une prédiction : même s'il ne se réfère pas à un outil prédictif, le juge fait explicitement ou implicitement une prédiction sur le niveau de risque que présente un détenu. Or, la recherche scientifique a établi que les formules objectives sont plus performantes que l'expertise humaine dans l'exercice de la prédiction en général, et dans la prédiction de la récidive en particulier. Dans un ouvrage de référence paru en 1981, le professeur de droit et de psychiatrie John Monahan estimait que l'évaluation de la dangerosité par un clinicien est exacte une fois sur trois [Monahan, 1981]. Le passage aux outils actuariels, en particulier dans le monde anglo-saxon, a substantiellement augmenté ce niveau de précision. L'une des raisons à la supériorité des outils prédictifs est que les psychiatres présentent un biais : ils ont tendance à surestimer le risque de récidive. En raison de leur meilleur pouvoir prédictif, les algorithmes permettraient de mieux identifier d'une part les délinquants à haut risque, et donc d'améliorer la sécurité publique (en réduisant les cas de récidive), d'autre part les délinquants à faible risque, et ainsi de désengorger les prisons (en réduisant le taux et la durée d'incarcération de ces individus). Les outils d'évaluation du risque sont effectivement réputés pour réduire le niveau global d'incarcération. En moyenne, ces outils classent 75 % des délinquants comme étant à risque faible ou modéré-faible et seulement 7 % à risque élevé. Au Canada, où ils sont largement utilisés depuis la fin des années 1990, les sentences sont deux à trois fois moins lourdes qu'en France. Dans l'État de Virginie aux États-Unis, la commission des condamnations pénales a publié un rapport en 2014 montrant que les taux d'incarcération et de récidive ont significativement diminué depuis l'utilisation d'outils d'évaluation du risque dans la détermination de la peine. Identifier les individus à faible risque afin de les aiguiller vers des alternatives à la prison revêt une importance cruciale, car en cas d'incarcération, côtoyer des détenus à risque élevé augmente le risque qu'ils en deviennent eux-mêmes à leur tour. Réduire l'incarcération (et la dépense publique correspondante) tout en améliorant la sécurité publique, voilà les traits d'une justice pénale efficace.

D'autre part, l'utilisation d'algorithmes prédictifs contribuerait à rendre la décision judiciaire plus objective

et transparente en bornant le pouvoir discrétionnaire du juge pénal. Le pouvoir souverain d'appréciation des juges du fond signifie que les juges sont libres dans la qualification des faits (s'agit-il bien d'un adultère ?), l'appréciation des éléments de preuve (cette preuve est-elle crédible ?), et l'appréciation de l'ampleur de la sanction (accorde-t-on des délais de paiement au débiteur ?). Mais cette liberté d'appréciation donne la possibilité au juge d'exprimer – volontairement ou non – sa subjectivité et ses biais. La première produit un aléa judiciaire, les seconds sont sources de discrimination. Aux États-Unis, l'utilisation des outils prédictifs doit être comprise dans un contexte d'incarcération de masse qui touche principalement les Afro-Américains pauvres. La surreprésentation de cette partie de la population dans la population carcérale pose inévitablement la question de l'impartialité des magistrats et de leurs biais, conscients ou inconscients. L'erreur est humaine, et ceci vaut dans le champ de la justice pas moins qu'ailleurs. En réduisant cette erreur, les algorithmes permettraient, en principe, d'améliorer l'égalité des justiciables devant la loi.

L'histoire de l'évaluation du risque de récidive chez les criminels montre que la faillibilité de l'évaluation humaine a suscité le développement d'une évaluation objective supposée plus fiable. Une religion a ainsi remplacé une autre, mais la vigilance est de mise, car les outils d'évaluation du risque, dont leur version algorithmique, demeurent en l'état imparfaits. Cette imperfection concerne tout d'abord l'efficacité, c'est-à-dire la précision de la prédiction. Par exemple, plusieurs études rapportent que le logiciel COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), utilisé par de nombreuses juridictions américaines, prédit correctement si un prévenu récidivera (dans les deux années suivant l'infraction) dans 60-65 % des cas [Dressel et Farid, 2018]. L'imperfection des algorithmes concerne également leur équité, c'est-à-dire leur capacité à évaluer les individus de façon non biaisée. Là aussi, un rapport du site d'investigation américain ProPublica montre que le logiciel COMPAS présenterait un biais racial envers les prévenus noirs (mais cette conclusion est discutable). Si le cas COMPAS a eu le mérite d'attirer l'attention sur le caractère potentiellement biaisé des algorithmes prédictifs de la récidive, ce cas ne devrait pas laisser croire que ces algorithmes présentent nécessairement un biais racial. Et surtout, il ne devrait pas nous faire oublier que les humains aussi sont potentiellement biaisés. L'erreur est algorithmique, mais l'erreur est avant tout humaine. Reconnaître ce principe implique une démarche pragmatique qui consiste à comparer rigoureusement l'humain et l'algorithme, dans la continuité des travaux que Paul Meehl avait réalisés dans les années 1950 sur la problématique prédiction clinique *vs.* statistique [Meehl, 1954]. Alors que ce dernier avait conclu

à la supériorité générale de la prédiction statistique, Dressel et Farid [2018] parviennent à la conclusion opposée dans le cas particulier de la prédiction de la récidive chez des criminels. Dans la comparaison humain *vs.* algorithme, l'algorithme ne sort pas toujours vainqueur.

L'arrivée des algorithmes prédictifs dans la justice (pénale) est à la fois déstabilisante, inquiétante, et prometteuse. Déstabilisante, car ils permettent à la justice d'intervenir non plus seulement *post delictum* en sanction d'un acte délictueux commis, mais *ante factum* en prévention d'un acte délictueux estimé probable. Ce faisant, ils font entrer le principe *Minority Report* dans le monde de la justice. La police prédictive instaure la possibilité d'agir sur le fondement d'une prédiction algorithmique, on peut désormais juger sur le fondement d'une telle prédiction.

Inquiétante, car fonder une décision affectant une personne sur le résultat d'un algorithme prédictif reposerait sur une vision déterministe des trajectoires de vie. La prédiction de l'algorithme n'enferme-t-elle pas l'individu dans un certain destin ? Si un algorithme identifie un prévenu comme présentant un risque de récidive élevé, le juge sera enclin à lui infliger une peine sévère, laquelle augmentera les difficultés de la personne à se réinsérer dans la société, et *in fine* la probabilité qu'elle récidive. En enfermant la personne dans une trajectoire fixe, la prédiction de l'algorithme sera auto-réalisatrice. N'oublions pas cependant que les comportements humains suivent des régularités statistiques, comme l'avaient compris les sociologues de l'Université de Chicago dans les années 1920. En dépit de notre attachement à l'idée de libre arbitre, les faits montrent qu'il y a moins d'aléatoire dans nos vies que ce que l'on imagine. Les algorithmes prédictifs capturent ces régularités. C'est précisément parce qu'ils capturent ces régularités qu'ils sont efficaces. Et c'est parce qu'ils sont efficaces que les outils prédictifs de la récidive sont aujourd'hui utilisés dans le monde entier, en Amérique du Nord, Asie, Australie, et Europe (Suisse et Belgique particulièrement). On interroge souvent le caractère éthique de l'utilisation des outils prédictifs. Mais renversons la perspective : est-il éthique de ne pas utiliser des outils dont la science a démontré qu'ils étaient plus performants que l'expertise humaine ? Aux États-Unis, une commission des libérations conditionnelles (celle de l'Illinois) utilisait une table actuarielle pour estimer le risque de récidive des détenus dès les années 1930. En France, l'évaluation de la dangerosité des criminels repose toujours sur l'expertise humaine. En 2020, les décideurs publics peuvent-ils se permettre d'ignorer la science sur des questions liées à la sécurité et la justice ?

Prometteuse, car les algorithmes prédictifs offrent la possibilité d'instaurer une justice à la fois plus efficace et

plus équitable. Y parviennent-ils ? Une justice augmentée par des algorithmes est-elle meilleure qu'une justice purement humaine ? Répondre à cette question requiert une attitude pragmatique suivant laquelle les situations avec et sans algorithme sont comparées sur deux critères, l'efficacité et l'équité. Cette comparaison devrait être réalisée de façon objective, sans *a priori*. En mars 2019, un article du *Point* sous-titrait « *L'expérience montre que les algorithmes sont source d'erreurs et de discriminations. Une première charte éthique énonce les règles du jeu* ». Dans l'imaginaire collectif, les algorithmes sont désormais associés à la notion de biais. Mais c'est oublier un peu vite que les humains aussi sont source d'erreurs et de discriminations [Berthet, 2018]. Dès lors, une comparaison rigoureuse humain *vs* algorithme s'impose, dans la continuité des travaux de Paul Meehl dans les années 1960. À cet égard, l'étude de Dressel et Farid [2018] sur le logiciel COMPAS est exemplaire. Rappelons que cette étude montre – entre autres – que dans la prédiction de la récidive chez des criminels, les humains et COMPAS présentent le même biais racial. Dès lors, rejeter par principe l'algorithme au motif qu'il est biaisé au profit du *statu quo* (l'expertise humaine) serait fallacieux. Le choix d'utiliser ou non un algorithme prédictif devrait être un choix pragmatique, non idéologique.

## Vers une société de la prédiction ?

Si l'on conçoit volontiers l'avantage que donnent les algorithmes prédictifs à la puissance publique, il faut toutefois rappeler le danger que ceux-ci peuvent constituer. Le glissement vers un régime qui culpabiliserait les individus dont on estime la potentielle nuisance pour la société élevée s'accorde assez mal avec les fondements de notre système juridique et sociétal : présomption d'innocence, charge de la preuve et libertés individuelles. Cet avertissement est formulé par Marc Dugain et Christophe Labbé dans *L'homme nu : la dictature invisible du numérique* [2016, p. 126-129] : ces auteurs s'inquiètent de l'avènement d'une ère de la « *criminalisation de l'intention* » marquant le passage de la notion de « *culpabilité à celle nettement plus subjective de dangerosité* ». La permanence d'un contrôle scrupuleux du juge et le renforcement des garanties procédurales s'avèrent dès lors plus que jamais nécessaires

Or, les prédictions algorithmiques sont désormais possibles et le seront d'autant plus à l'avenir que la masse de données disponibles augmente et que l'intelligence artificielle s'améliore. Nous vivons désormais dans l'ère

de la donnée. Chaque jour, nous générons 2,5 trillions d'octets de données, et selon le McKinsey Global Institute, le volume mondial de données double tous les trois ans. L'IA s'avère décisive, car elle permet de construire des algorithmes qui traitent ces données de façon automatisée et les rendent intelligibles. Dans un article publié le 28 décembre 1948 dans *Le Monde*, le logicien Dominique Dubarle avait anticipé l'avènement d'une société gouvernée par la collecte d'informations, la mesure et la prédiction, ce qu'il qualifiait de « *surgissement d'un prodigieux Léviathan politique* ». Il évoquait cette évolution qui mènerait à la création d'une véritable « *machine à gouverner* ». On peut espérer ou redouter l'avènement d'une société de la prédiction, qui, malgré les risques qu'elle charrie, emporte la séduisante promesse d'une société sans crime. Le fantasme sécuritaire n'est pas nouveau. Il prend racine dans la raison d'être de l'État, dans ses fonctions les plus régaliennes. Il est la raison même du contrat social. Dès lors, l'idée de protéger les citoyens de crimes avant même qu'ils ne soient commis semble être puisée à la source, dans l'essence même de l'État. C'est une perspective alléchante pour le décideur public comme pour le citoyen qui voit son contrat avec l'État amélioré, sans *a priori*, consentir à davantage de sacrifices ou d'efforts. La version 2.0 du contrat social, en somme, à peu de frais. Néanmoins, il faut souligner que contrairement aux *precogs* de *Minority Report* ou même aux oracles de l'Antiquité, les algorithmes prédictifs n'ont aucune connaissance du futur et ne formulent aucune vision. Il y a là une différence de nature : là où les *precogs* apportent une certitude, car ils ont vu le futur, les algorithmes proposent une probabilité, car ils analysent le passé et peuvent ainsi repérer des régularités statistiques. Les décisions prises sur la base de leurs prédictions doivent donc en tenir compte et ne sauraient relever d'une foi aveugle, comme l'illustre ce dialogue dans *Minority Report* entre deux personnages principaux :

« - Cette boule, pourquoi l'avez-vous rattrapée ?

- Parce qu'elle allait tomber.

- Vous en êtes sûr ?

- Oui.

- Pourtant elle n'est pas tombée.

- Puisque je l'ai rattrapée...

- Alors en la rattrapant vous avez empêché que cela se produise... mais que vous l'ayez empêché n'enlève rien au fait que cela allait se produire. »

Cette certitude n'est pas possible avec la prédiction algorithmique. C'est encore moins le cas lorsqu'il s'agit de la prédiction de comportements humains, avec ce qu'ils comportent d'inattendu et d'irréductible.

Soyons plus explicites : une prédiction n'est pas une décision. Elle est une indication ou une aide à la décision, mais ne peut se substituer complètement au choix humain. L'automatisation des décisions est la première crainte qui émerge avec le développement de l'intelligence artificielle, qui remplacerait l'intelligence humaine au lieu de la compléter. L'homme doit avant tout garder la main sur la décision. L'essor des algorithmes prédictifs fait plus que jamais résonner les mots d'Ernest Renan, pour qui « *Organiser scientifiquement l'humanité, tel est donc le dernier mot de la science moderne, telle est son audacieuse mais légitime prétention* ». Avec ces algorithmes, émerge la tentation croissante de substituer la prédiction à la décision, une tendance qui participe de ce que Basdevant et Mignard [2018, p. 141] appellent le « *coup data* » : le renversement du pouvoir par les données. Il ne faut toutefois pas désespérer : en France et en Europe, la législation a bien rappelé le principe selon lequel une décision ne peut pas être entièrement fondée sur un algorithme et une intervention humaine est nécessaire pour entériner ladite décision (article 10 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et article 22 du règlement européen du 27 avril 2016 sur les données à caractère personnel).

Ces considérations nous mènent à faire valoir une approche pragmatique vis-à-vis des algorithmes afin d'éviter les positions réductrices. Le solutionnisme technologique n'est pas davantage une solution que la technophobie. Dès lors, comment analyser objectivement la valeur d'un algorithme ? Il s'agit d'effectuer, dans toutes les situations dans lesquelles l'utilisation d'un algorithme est possible comme alternative à une action humaine, un calcul coût-bénéfice complet. Celui-ci doit s'effectuer de façon très exhaustive, comprenant aussi les coûts sociaux (comme

ceux par exemple qu'un algorithme biaisé en défaveur d'une minorité imposerait à une société qui se veut ouverte et égalitaire). Il faudra réaliser l'arbitrage entre efficacité et équité. Ce calcul doit se faire sans complaisance envers les algorithmes, en mettant en lumière leurs limites, les obstacles techniques auxquels ils font face et leurs biais. Néanmoins, nous constatons que les algorithmes sont souvent mal jugés : on compare en général leur utilisation à une situation idéale, à la notion de justice, d'équité, etc. Mais une réflexion réaliste devrait les comparer au *status quo*, qui est celui qui prévaut actuellement et donne la

primauté aux humains. Or, ces derniers sont parfois biaisés et leurs biais sont même à l'origine des défauts des algorithmes [Berthet, 2018]. Un algorithme est toujours limité et imparfait, mais comparé à la pratique humaine, il peut permettre de gagner en efficacité sans réduire pour autant l'équité.

Les algorithmes sont porteurs d'une promesse d'efficacité, mais ce gain ne doit pas se faire au détriment des libertés individuelles. Le risque qu'elles courent est grand eu égard aux bouleversements induits par nos nouveaux outils. Ce problème est inhérent à l'algorithme en ce que ce dernier utilise une puissance de calcul et donc d'action inégalée par le

passé. Ses potentialités sont infinies, ou tout du moins exponentielles. En tant que société, le défi était jusqu'alors de repousser les limites, notamment technologiques. L'enjeu consiste désormais à fixer les limites. Or le débat sur les libertés individuelles est crucial : celles-ci sont le fondement de nos démocraties. Les algorithmes ont démultiplié nos capacités à surveiller toute une population en récoltant et analysant ses métadonnées. Si la logique qui prévalait était de surveiller les individus suspects, on préfère désormais surveiller l'ensemble de la population pour identifier les suspects. C'est un passage à une méthode holiste de renseignement. Un ancien patron de la NSA, le général Keith Alexander, avait théorisé ce tournant que nous qualifions d'ère de la surveillance de masse avec la métaphore de l'aiguille et de la botte de foin. Pour lui, « *le meilleur moyen de retrouver*

SI L'ON CONÇOIT VOLONTIERS L'AVANTAGE QUE DONNENT LES ALGORITHMES PRÉDICTIONNELS À LA PUISSANCE PUBLIQUE, IL FAUT TOUTEFOIS RAPPELER LE DANGER QUE CEUX-CI PEUVENT CONSTITUER. LE GLISSEMENT VERS UN RÉGIME QUI CULPABILISERAIT LES INDIVIDUS DONT ON ESTIME LA POTENTIELLE NUISANCE POUR LA SOCIÉTÉ ÉLEVÉE S'ACCORDE ASSEZ MAL AVEC LES FONDAMENTS DE NOTRE SYSTÈME JURIDIQUE ET SOCIÉTAL : PRÉSOMPTION D'INNOCENCE, CHARGE DE LA PREUVE ET LIBERTÉS INDIVIDUELLES.

*l'aiguille, c'est de contrôler toute la botte de foin* ». De même, l'analyse d'images et la reconnaissance faciale permettent désormais de suivre un individu dans une foule, d'analyser son comportement, ses gestes, de suivre sa voiture avec des caméras de surveillance capables de lire une plaque minéralogique. Se posent aussi les questions de savoir dans quelle mesure et à quelles fins on peut exploiter les données personnelles des citoyens, ou si une décision de justice peut se fonder sur des régularités statistiques.

Finalement, les algorithmes nous forcent à redéfinir notre corpus de valeurs et nos principes afin de tracer des lignes rouges strictes. La question n'est pas technologique : c'est une question de société. On retrouve là une intuition de Martin Heidegger selon qui « *l'essence de la technique n'est rien de technique* » ■

## Bibliographie

---

BASDEVANT (A.), MIGNARD (J.-P.), 2018, *L'empire des données : essai sur la société, les algorithmes et la loi*, Paris, Don Quichotte, p. 141-201

BERTHET (V.), 2018, *L'erreur est humaine*, Paris, CNRS Éditions, 224 p.

DRESSEL (J.), FARID (H.), 2018, «The accuracy, fairness, and limits of predicting recidivism», *Science advances*, n° 4 : eao5580.

DUGAIN (M.), LABBÉ (C.), 2016, *L'homme nu : la dictature invisible du numérique*, Paris, Plon, p. 126-129

HARCOURT (B.), 2011, « Surveiller et punir à l'âge actuariel. Généalogie et critique », *Déviance et Société*, n° 1, p. 5-33.

MEEHL (P. E.), 1954, *Clinical vs. statistical prediction: A theoretical analysis and a review of the evidence*, Minneapolis, University of Minnesota Press, 149 p.

MONAHAN (J.), 1981, *Predicting Violent Behavior: An Assessment of the Clinical Techniques*, Beverly Hills (CA), Sage, 183 p.

# L'impact de l'intelligence artificielle dans la conduite de l'enquête judiciaire

Général Patrick TOURON

« Beaucoup en parlent et peu la comprennent : qui suis-je ?

L'intelligence artificielle, bien sûr ! »

## L'intelligence artificielle et l'enquête judiciaire

**A**u regard de l'importance sociale que revêt l'enquête judiciaire pénale dans une société, il est essentiel d'approcher ce sujet sans fantasme ni passion. Définir ce qu'est l'intelligence artificielle (IA), à ce jour, décrire en quoi l'enquête judiciaire subit ou a subi des transformations ces dernières années et comment, naturellement, et ce de manière inexorable, ce nouvel outil technologique, va venir enrichir la palette déjà large des moyens mis à la disposition des enquêteurs et magistrats dans la conduite des enquêtes, nécessite d'y consacrer un peu de temps. Je gage qu'à l'identique des avancées technologiques qui ont effrayé le public à travers le temps, ces algorithmes viendront renforcer l'importance de la dimension humaine dans la conduite de notre action, pour peu que nous décidions de l'appréhender, de nous en saisir et de l'employer avec notre intelligence. S'il est évident que demain la conduite d'une enquête judiciaire se fera différemment, elle le sera toujours par des enquêteurs et magistrats nécessairement à l'aise avec ces outils et formés à leur emploi.

Lorsque l'on regarde les capacités des algorithmes actuels, on est bien loin des fantasmes qui laissent à penser que l'esprit humain sera supplanté dans toutes ses dimensions. En revanche, devant la multiplicité infinie des données, l'IA les classe mieux, les lie mieux et surtout se souvient de tout, et cela dans un temps très court. À l'aide de cet assistant, l'enquêteur et le magistrat pourront voir, analyser et confronter plus de pièces dans un dossier toujours plus volumineux et complexe. « *L'œil ne voit dans les choses que ce qu'il y regarde et il ne regarde que ce qui est dans l'esprit*<sup>1</sup> ». La multitude des pièces d'un dossier pénal nous permet-elle, encore, de tout regarder ?

### L'intelligence artificielle

L'IA n'est pas un objet unique et homogène en soi et cela se constate dans la définition ambitieuse et non atteinte que l'on retrouve dans le dictionnaire le *Trésor de la langue française* (TLF) élaboré par ATILF<sup>2</sup>, : « *Intelligence artificielle : recherche de moyens susceptibles de doter les systèmes informatiques de capacités intellectuelles*

Patrick TOURON

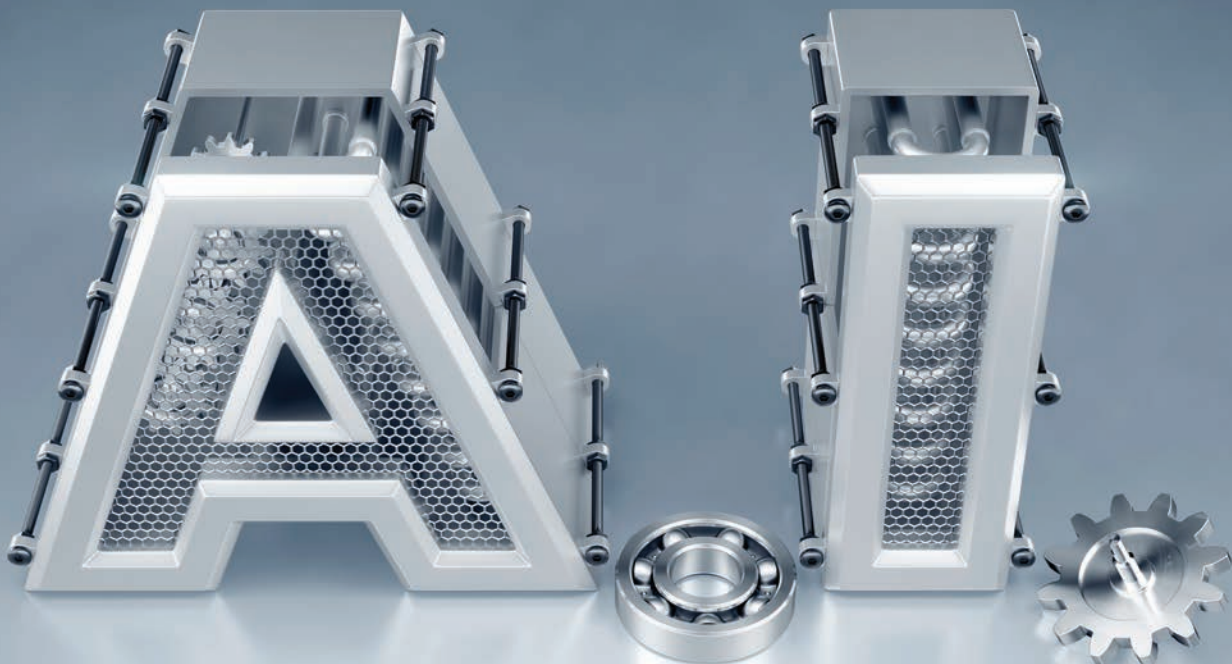


Patrick Touron est général de gendarmerie, commandant du Pôle judiciaire situé à Pontoise

et ancien directeur de l'Institut de recherche Criminelle de la gendarmerie nationale (IRCGN). Diplômé de l'École des sciences criminelles de Lausanne (ESC) et ancien élève du Collège interarmées de défense (CID) promotion 2004, il est ancien auditeur de l'Institut des Hautes études pour la science et la technologie (IHEST promotion « Léonard de Vinci » 2012-2013). Membre du conseil scientifique de la gendarmerie nationale et co-président de l'Observatoire national des sciences et technologies de la sécurité (ONSTS) et expert en investigations criminelles, spécialisé dans le domaine des explosifs et l'identification de victimes lors de catastrophes de masse, il a rédigé de nombreux articles scientifiques dans le domaine des sciences forensiques.

(1) Devise attribuée par Lacassagne à Bertillon [Niceforo, 1907].

(2) Laboratoire analyse et traitement informatique de la langue française, membre du CNRS.



*comparables à celles des êtres humains* ». Pour remplir son objectif il lui faut nécessairement disposer de données en grande quantité (*big data*), des outils statistiques et probabilistes et si possible des algorithmes permettant de classer, valoriser et confronter ces données.

## Les données

La loi n° 2016-1321 du 7 octobre 2016 pour une république numérique (PRN) ouvre à tout un chacun un champ extraordinaire de données jusque-là confidentielles ou éparses. Des limites sont établies et liées à la confidentialité, la sécurité ou à l'anonymisation de ces données<sup>3</sup>. Néanmoins, ces données peuvent être naturellement couplées à d'autres données elles aussi librement accessibles, ou non, afin de constituer des bases ressources pour les utilisateurs d'outils numériques à même de les lier, les classer, les contextualiser, les croiser, en un mot d'en retirer une information supérieure à celle de départ. Si les données scientifiques issues des outils communément employés en sciences forensiques sont nativement ordonnées, celles, écrites, issues de la procédure judiciaire nécessitent des outils de traitement du langage naturel (TAL) afin de préparer leur exploitation automatique par des algorithmes dédiés.

## Les outils

Il convient tout d'abord de distinguer deux familles de programmes : les systèmes experts (SE) et l'apprentissage automatique (*Machine Learning*) faisant partie intégrante du domaine de l'intelligence artificielle [Conseil de l'Europe, 2018]. Dans le premier cas, on apprend à l'outil en lui fournissant des exemples ; dans le second cas, on demande à l'outil de retrouver, parmi les données à sa disposition, ce qui est susceptible de nous intéresser.

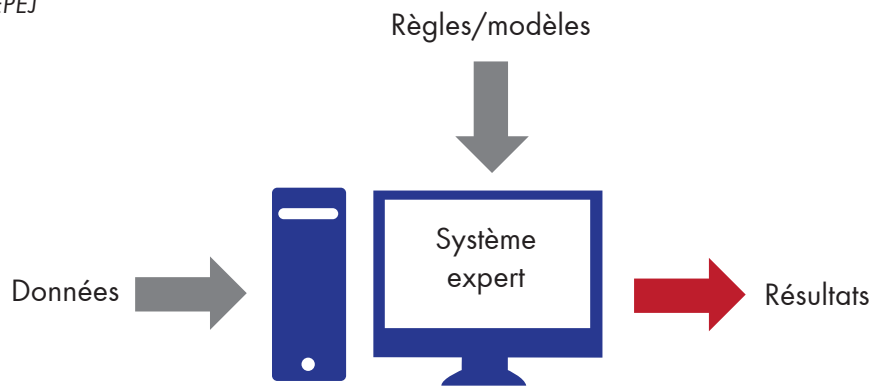
Les systèmes experts<sup>4</sup> se fondent sur un modèle explicatif auquel il faut associer des paramètres permettant d'établir un ou plusieurs résultats. L'utilisation d'algorithmes d'apprentissage automatique s'emploie dans des situations où une démarche déterministe n'est pas concevable. Ainsi, l'apprentissage machine va consister à élaborer un modèle de corrélation réaliste entre des variables prédictives (données d'entrées) et des variables cibles (résultats). Pour cela, l'apprentissage automatique s'appuie sur un ensemble d'outils statistiques et d'algorithmes informatiques permettant d'automatiser la construction d'une fonction de prédiction.

(3) Depuis l'entrée en application du règlement général sur la protection des données (RGPD), la Cour de justice de l'UE pseudonymise elle aussi les parties personnes physiques : voir son communiqué n° 96/18 du 29 juin 2018.

(4) Commission européenne pour l'efficacité de la justice (CEPEJ), Charte éthique, p. 34.

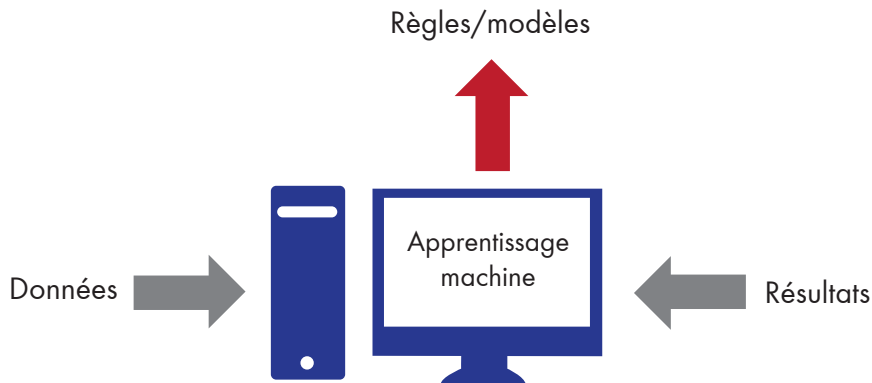


Fig 1 - Système expert  
Figure CEPEJ



Un système expert est un outil capable de reproduire les mécanismes cognitifs d'un expert, dans un domaine particulier. Plus précisément, il s'agit d'un logiciel capable de répondre à des questions, en effectuant un raisonnement à partir de faits et de règles connues. Il se compose de 3 parties : une base de faits, une base de règles, un moteur d'inférence. Le moteur d'inférence est capable d'utiliser des faits et des règles pour produire de nouveaux faits, jusqu'à parvenir à la réponse à la question experte posée.

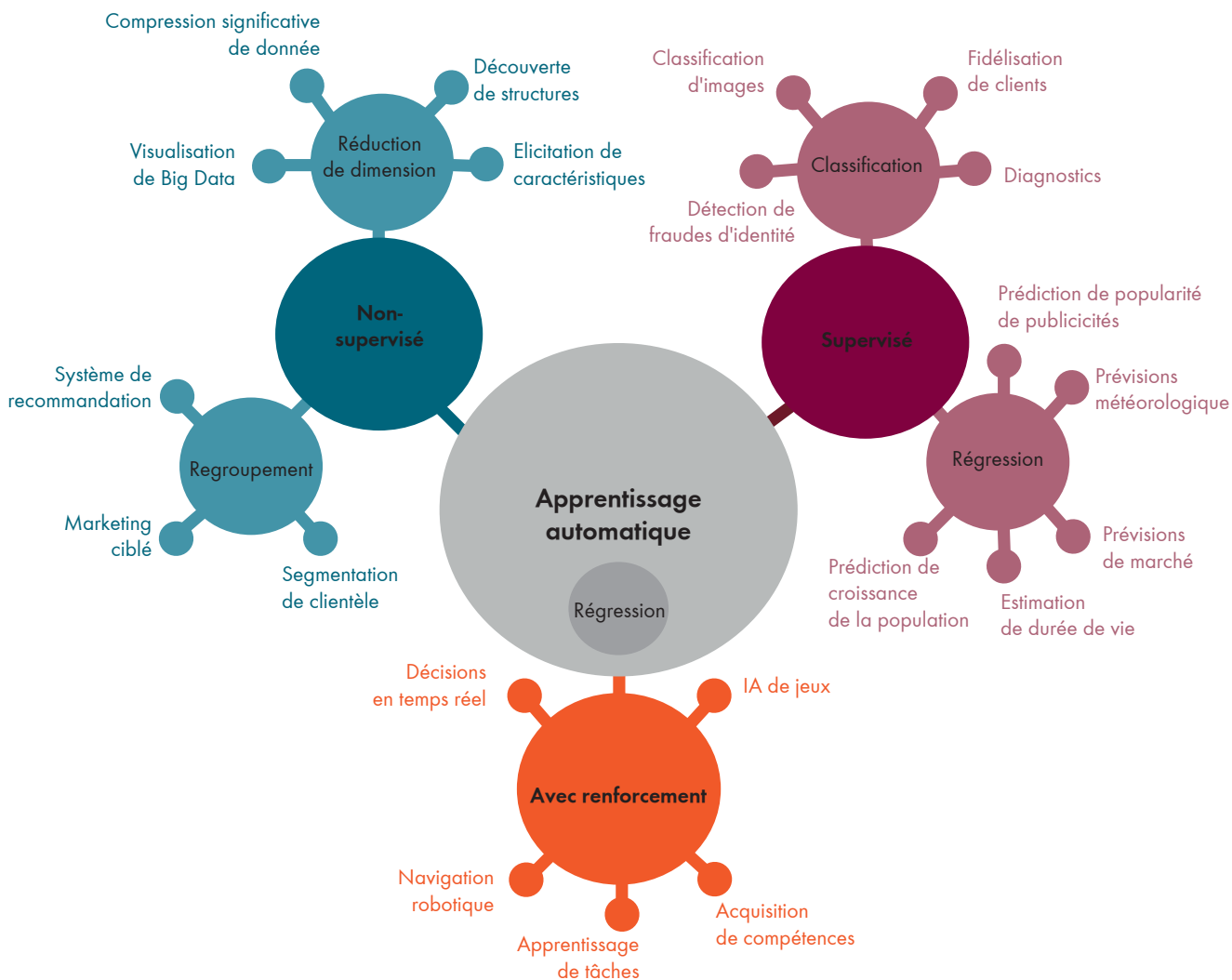
Fig 2 - Apprentissage automatique  
Figure CEPEJ



L'apprentissage machine fonctionne par une approche inductive et permet de construire un modèle mathématique à partir de données, en incluant un grand nombre de variables qui ne sont pas connues à l'avance. Les paramètres sont configurés au fur et à mesure lors d'une phase d'apprentissage, qui utilise des jeux de données d'entraînement pour trouver des liens et les classifie. Les différentes méthodes d'apprentissage machine sont choisies par les concepteurs en fonction de la nature des tâches à accomplir.

Précurseurs, de l'intelligence artificielle, les systèmes experts s'appuient sur la logique formelle et utilisent le raisonnement déductif. Les systèmes experts ont connu un rapide développement dans les années 1990, néanmoins différentes études ont montré leurs limites en performance et maintenance au-delà de 200 règles d'encodages. Dans le cas où le raisonnement nécessite un

très grand nombre de règles ou qu'il est trop complexe à expliciter, il est préférable de se tourner vers un système d'apprentissage automatique qui va rechercher des corrélations entre données d'entrées et résultats. La figure 3 illustre les différentes catégories et sous-catégories d'apprentissage automatique ainsi que les activités qu'il est ainsi possible d'automatiser à ce jour.

Fig 3 - Carte des possibilités d'apprentissage automatique<sup>5</sup>

En dépit de leur performance accrue dans de nombreux domaines, il est souvent très difficile d'expliquer les décisions proposées par les algorithmes de manière intelligible. Cette méconnaissance est principalement due aujourd'hui au changement de paradigme introduit par l'avènement de l'apprentissage, en particulier l'apprentissage profond (*deep learning*<sup>6</sup>).

Une attention particulière doit être portée quant au développement de l'outil numérique en fonction de son utilisation dans l'enquête. Ainsi le choix de la technique

d'apprentissage employée, l'éthique en conception, la loyauté, l'absence de biais et l'absolue nécessité de pouvoir expliciter les arguments qui ont permis à l'outil de prendre une décision en particulier, constituent le fil rouge dans la construction initiale de ces outils d'aide à l'enquête judiciaire<sup>7</sup>.

Néanmoins, la description qui vient d'être faite *supra* des outils proposés par l'IA n'éclaire pas vraiment l'enquêteur et le magistrat en charge d'une enquête judiciaire quant au processus qui aura conduit l'IA à leur faire des

(5) Commission européenne pour l'efficacité de la justice (CEPEJ), Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, p. 74.

(6) Villani (C.), 2018, *Donner un sens à l'intelligence artificielle*.

(7) Rapport CNIL : comment permettre à l'homme de garder la main ? Décembre 2017

propositions, ce qui génère une appréhension quant à l'emploi de ces outils dans un domaine aussi important que celui de la justice pénale.

## Une solution

Il existe, fort heureusement, un « *Deus ex machina* » à ce dilemme. Dans le cadre de la conduite d'une enquête, nous nous trouvons devant le même problème théorique que celui de la résolution d'une équation complexe (du quatrième degré que l'on apprend à résoudre au lycée) qui comporte de nombreux facteurs inconnus et dont on recherche une solution.

Fig 4 - Exemple d'une équation du 4<sup>e</sup> degré

$$4x^4 + 10x^3 - 28x^2 - 46x + 60 = 0.$$

En appliquant la méthode de Ferrari (1522-1565), la résolution s'opère en une vingtaine d'étapes. En utilisant un logiciel adapté en quelques millisecondes, je gage que la plupart d'entre nous optent pour l'emploi d'un logiciel dédié. Les solutions de l'équation de départ sont fournies par le logiciel et sont ( $x = -3$ , ou  $-5/2$ , ou  $1$  ou  $2$ ). Tout comme pour l'IA, la majorité d'entre nous ne maîtrise pas la conception de l'outil logiciel de résolution. En revanche nous faisons confiance à la machine, car nous pouvons vérifier le résultat, en remplaçant «  $x$  » par une des solutions directement dans l'équation.

Fig 5 - Vérification d'une solution proposée par le logiciel

$$4x^4 + 10x^3 - 28x^2 - 46x + 60 = 0,$$

$$\text{ce qui donne } 4(1)^4 + 10(1)^3 - 28(1)^2 - 46(1) + 60 = 0$$

$$4 + 10 - 28 - 46 + 60 = 0 \text{ et donc } 0 = 0$$

De la même manière, lorsque l'exploitation des données d'enquête par l'IA à qui nous aurons confié l'ensemble des données, conduira le logiciel à nous proposer un lieu, une personne, un temps particulier, une action ou qu'il soulèvera une contradiction entre les déclarations ou les faits, nous aurons tout loisir de reprendre les éléments

proposés par l'outil informatique et de le confronter à la réalité du dossier. D'autant plus facilement que l'ergonomie des outils fournira des indexations pour retrouver aisément les pièces nécessaires au sein du dossier quel qu'en soit son volume.

L'utilisateur, magistrat ou enquêteur, d'outils informatiques complexes utilisant l'IA pour exploiter l'ensemble des données disponibles dans un dossier judiciaire, se retrouve dans une situation qu'il connaît déjà en police judiciaire, et qui consiste à disposer d'une pièce de procédure provenant d'un renseignement issu d'une source anonyme, et qui vient éclairer des faits. Cette information pourra être confrontée aux pièces du dossier existant et guider la suite des investigations. Ainsi, qu'elle provienne d'une source anonyme ou d'itération complexe réalisée par des algorithmes, enquêteurs et magistrats sont familiers des propositions ou des informations dont ils n'ont pas la compréhension complète, mais qu'ils peuvent vérifier.

## Les données d'entrée dans l'enquête judiciaire

La pratique professionnelle quotidienne permet très rapidement de comprendre que le volume des dossiers judiciaires, en dehors de la complexité juridique, s'accroît considérablement au fil des ans. En découpant la conduite d'une enquête en trois phases, nous pouvons constater que le domaine des constatations s'est enrichi, celui des auditions, multiplié, et bien entendu celui des expertises complexifié. Nous sommes actuellement à un point où il me semble difficile pour un cerveau d'appréhender de manière holistique toutes ces données. L'IA, avec les capacités décrites ci-dessus, représente donc une chance pour nous permettre d'assurer l'exploitation, efficace, de ces données d'enquête. Car, bien entendu, personne ne peut accepter ne pouvoir exploiter les données dont il dispose ou risquer de passer à côté d'une information, car il n'aura pas pu se rappeler une contradiction entre un fait et un témoignage, noyé parmi des centaines d'autres.

## Les constatations

« *Les premières constatations faites dans n'importe quel crime ou délit sont la pierre angulaire de tout procès* » explique Bischoff en 1938<sup>8</sup>. En dressant à gros traits la partie constatation systématique à travers le dernier siècle, nous sommes

(8) Bischoff (M.), 1938, La police scientifique, Payot, Paris.

passés du croquis au début du XX<sup>e</sup> siècle à la photographie noir et blanc, puis couleur vers le milieu du siècle, dans des dossiers photos toujours plus volumineux, complétés pour terminer le siècle par des films vidéo. Nous démarrons le XXI<sup>e</sup> siècle avec des numérisations, des lasers scanner, du tachéomètre, de la photogrammétrie, pour aboutir à de la visite panoramique, voire de l'immersion 3D numérique, couplés à des capacités d'intégration de scénario ou de calcul de trajectoire ou de son<sup>9</sup>. Au sein du pôle judiciaire, nous conduisons un projet « Janus » qui permet de travailler sur des scènes de crimes virtualisées et des indices dématérialisés afin d'étudier les faits à plusieurs, de retravailler les indices et de vérifier les hypothèses en réalité augmentée. Ces développements se font en lien étroit avec le comité éthique du pôle judiciaire de la Gendarmerie nationale (PJGN), comme pour tout développement portant sur l'emploi de nouvelles technologies.

### L'aspect collecte

Le recueil des déclarations, des témoignages, les différentes auditions constituent la base du travail d'investigation<sup>10</sup> et bien souvent le premier pas dans la recherche des contradictions ou la vérification des faits. Ce sont désormais plusieurs centaines de pièces qui viennent communément enrichir un dossier. Bien

entendu ces pièces sont encore essentiellement transcrites par un enquêteur, mais de plus en plus fréquemment, ou lorsque cela est prévu par la loi, elles sont filmées et enregistrées. Demain elles seront directement enregistrées et retranscrites automatiquement pour des raisons évidentes de coût. Ce sont donc désormais des milliers d'informations à exploiter et confronter.

### Les traces et expertises

Le relevé des traces et indices désormais ne se limite plus aux seuls objets présents, ni aux quelques indices visibles, mais aussi à ceux invisibles à l'œil nu. Ce sont des équipements optiques ou physiques qui viennent améliorer la détection et la recherche de ces traces (sang, fibres, pollen, log réseau, données numériques, etc.) Tous ces éléments, une fois prélevés, vont venir enrichir un dossier<sup>11</sup>, sans que l'on sache *a priori* s'ils seront utilisés ou nécessaires à la compréhension du déroulé des faits. Néanmoins on doit les rechercher et les relever dès le départ. Leur analyse vient encore complexifier le dossier, car chacun est porteur d'une information qu'il faut croiser et qui apporte son lot de contradictions lorsqu'ils sont confrontés aux autres indices (un mégot transporté, un ADN de transfert...). Demain, ce sont de nouveaux indices qu'il faudra prendre en compte comme l'empreinte olfactive<sup>12</sup> et toutes les informations présentes à travers

Photo 2 - usage de la réalité augmentée  
« Innover aujourd'hui pour mieux protéger demain ». Photo IRCGN



(9) Daudigny (H.) *et al.*, 2014, « Fixation de l'état des lieux par moyens spéciaux (IRCGN) », *Revue géomètre XYZ*, n° 138.

(10) Guéniat (O.), 2012, « les secrets des interrogatoires et des auditions de police », *Presse romande*.

(11) Ribaux (O.), 2014, « Le renseignement par la trace », *Presse Romande*.

Fig 6 - L'empreinte olfactive : un nouvel indice de la présence d'un individu.  
« Innover aujourd'hui pour mieux protéger demain ». Photo IRCGN



les objets connectés ou sur le *cloud*. Désormais l'ère de l'exploitation des documents numérisés est derrière nous, nous entrons dans celle de l'exploitation de la donnée numérique, que seule l'IA peut porter.

artificielle arrive pour accomplir ce travail de mémoire, de classification, de valeurs et de connexions entre les faits et les indices, qui sont retrouvés dans les dossiers judiciaires, afin de rechercher cette vérité exposée au procès pénal.

### Valeur indiciale

En un siècle, nous sommes passés de dizaines de données à des milliers au XX<sup>e</sup> siècle, puis à des millions, voire des milliards en ce début de XXI<sup>e</sup> siècle et il est flagrant que les outils pour les exploiter ne peuvent plus être un crayon et un cerveau. D'ailleurs, la plupart des données sont stockées sur des disques durs ou clés USB afin d'être conservées. Il est désormais impossible de réaliser le tirage papier du contenu d'une clé USB (photos, documents, fichiers divers) ou de la mémoire d'un ordinateur. Des outils d'assistance à même de croiser et lier ces données sont nécessaires. Les poids respectifs et relatifs des indices selon les hypothèses ne peuvent plus être réalisés à la main, les réseaux bayésiens<sup>13</sup> sont autant d'outils qui vont venir demain remplacer chacun à sa place, les contextualiser dans le temps et l'espace afin de donner une fiabilité aux éléments de preuves exposés au procès. L'intelligence

### L'usage de l'IA

L'IA s'inscrit dans la continuité de l'informatique augmentée par la masse de données. L'accès à ces données, combiné avec la possession d'outils informatiques communs et des algorithmes adaptés, confère un savoir et une connaissance que l'on ne peut pas laisser hors de notre conduite d'enquête. Tous les métiers, dont les dimensions de créativité et de réflexion sont faibles, seront directement concurrencés par l'IA, et au regard de la variété des affaires et de la créativité et de l'imagination toujours renouvelées des criminels. La dimension humaine ne pouvant être supplantée par des machines, enquêteurs et magistrats ne risquent pas de voir substituer par de l'IA.

(12) Cuzuel (V.), Cognon (G.), 2017, «Origin, analytical characterization and use of human odor in forensics», *J Forensic Sci.*

(13) Taroni (F.), 2014, Bayesian networks for probabilistic inference and decision analysis in forensic science, Hardcover.



L'IA S'INSCRIT DANS LA CONTINUITÉ DE L'INFORMATIQUE AUGMENTÉE PAR LA MASSE DE DONNÉES. L'ACCÈS À CES DONNÉES, COMBINÉ AVEC LA POSSESSION D'OUTILS INFORMATIQUES COMMUNS ET DES ALGORITHMES ADAPTÉS, CONFÈRE UN SAVOIR ET UNE CONNAISSANCE QUE L'ON NE PEUT PAS LAISSER HORS DE NOTRE CONDUITE D'ENQUÊTE. TOUS LES MÉTIERS, DONT LES DIMENSIONS DE CRÉATIVITÉ ET DE RÉFLEXION SONT FAIBLES, SERONT DIRECTEMENT CONCURRENCÉS PAR L'IA, ET AU REGARD DE LA VARIÉTÉ DES AFFAIRES ET DE LA CRÉATIVITÉ ET DE L'IMAGINATION TOUJOURS RENOUVELÉES DES CRIMINELS. LA DIMENSION HUMAINE NE POUVANT ÊTRE SUPPLANTÉE PAR DES MACHINES, ENQUÊTEURS ET MAGISTRATS NE RISQUENT PAS DE SE VOIR SUBSTITUER PAR DE L'IA.



## L'automatisation

Actuellement les techniques d'apprentissage permettent de retrouver la photo d'un individu, d'un objet, d'une arme parmi les milliers de photos contenues communément dans un ordinateur, un téléphone ou même le Web. Personne ne souhaite rechercher un individu parmi des milliers de photos, dans le cadre d'une enquête judiciaire afin de dresser assez rapidement un environnement des connaissances d'un intéressé, de la même manière en ce qui concerne l'exploitation de centaines d'heures de vidéo à la recherche du passage d'un véhicule ou d'un individu. La vidéosurveillance intelligente (VSI) dispose, quant à elle, d'une extraordinaire capacité de détection et d'identification pour modéliser des données et anticiper des situations. Les techniques d'apprentissage de l'IA dédiées à la reconnaissance d'objets ou de formes dans un contenu numérique sont naturellement acceptées pour notre confort et constituent un apport non contesté. L'usage de l'IA dans ces domaines n'est quasiment jamais remis en cause, dans le respect de principes éthiques garantis au sein du pôle judiciaire de la Gendarmerie nationale par son comité d'éthique.

## Les liens relationnels

Parmi les éléments d'enquêtes que l'on aura à étudier avec ces nouveaux outils, nous disposons d'auditions, de relevés bancaires, téléphoniques, et des déclarations qui sont l'objet d'exploitation par des logiciels dédiés à relever des incohérences, à repositionner dans une échelle de temps et géographique ou à générer des schémas relationnels. L'incrémentation de ces données à partir des documents papiers ou numériques est longue. Les outils de l'intelligence artificielle permettent de détecter ces éléments directement dans des textes, à les identifier et les classer selon leur signification et à générer presque automatiquement ces schémas relationnels *supra*. Le gain de temps et la souplesse d'emploi rendent l'acceptation de ces outils évidente. Être en mesure de procéder à ces classements et ces liens, en temps réel à partir d'enregistrements sonores ou numériques correspond à une automatisation quasi naturelle qui ne saurait tarder. Les algorithmes en viendront naturellement à souligner au fil de l'eau des incohérences, et ainsi suggérer des questions qui appuieront le travail des enquêteurs et des magistrats. La reconnaissance vocale lors de l'écoute d'un enregistrement utilise l'IA (un apprentissage profond) et les outils comme GendVox (développé à l'Institut de recherche criminelle de la gendarmerie nationale) permettent d'attribuer un nom à chaque locuteur dans une conversation, cela représente un gain de temps évident.

## La détection d'incohérence

L'étape suivante et logique qui est rendue possible par le développement actuel des algorithmes mettant en œuvre de l'intelligence artificielle reviendra à détecter au travers les phrases employées ou les mots, les tonalités, le comportement global ou le rythme des déclarations, les omissions, les tentatives de mensonges ou la vraie détresse dans la voix. L'emploi de l'IA dans le cadre d'un appel au 112 par exemple qui permettrait de détecter dans la voix une réelle angoisse, voire signaler une maladie, sera faiblement remis en question. Comment ne pas utiliser ces nouveaux outils qui permettront à la justice ou au monde des urgences de rendre un travail plus fiable et plus efficient ? La détection du mensonge est à portée de l'IA. Tout comme actuellement un enquêteur ou un magistrat, par son travail de mémoire et son expérience, doit être en mesure de révéler les incohérences dans une déclaration, les contradictions dans les auditions ou le comportement anormal d'un individu tout en gardant la distance par rapport à ses *a priori* sociaux.

La rapidité de traitement des données, liée à l'optimisation des logiciels sur des environnements maîtrisés, permet

déjà de détecter des comportements anormaux d'individus dans une foule, ce qui permet à l'outil informatique d'attirer l'attention de l'opérateur vidéo sur ces individus. Cela peut être considéré comme une levée de doute. Et pourtant lorsque l'on essaie de comprendre tous les mécanismes qui ont été nécessaires pour que le logiciel détecte tel individu dans la foule, nous devons constater et admettre qu'il a suivi des phases d'apprentissage et qu'il a affiné son pouvoir discriminant en apprenant par lui-même, c'est-à-dire en modifiant d'initiative quelques variables, grâce à des données fournies par son concepteur ou qu'il aura récupérées. Ce mode de fonctionnement de l'intelligence artificielle qui consiste à agréger des couches de logiciels, souvent disponibles en *open source*, ne permet pas de remonter le processus décisionnaire. C'est la raison pour laquelle l'aspect contrôle et vérification par l'opérateur, d'un résultat fourni par l'IA, reste une nécessité, tant dans ses aspects opérationnels que déontologiques et éthiques.

### Les faux

À l'heure actuelle, l'IA est déjà utilisée en masse par les criminels, et je ne parlerai que des cas les plus flagrants comme l'utilisation de virus, de vers<sup>14</sup> ou de *malware*. Mais il existe de plus en plus de modifications de photos, de films, de voix qui sont l'œuvre d'utilisateurs malveillants, d'outils facilement employables et très puissants du fait des algorithmes employés et ce à faibles coûts et faibles compétences. Seule l'IA est en mesure de les combattre, car elle permet des détections en temps réel et sur des flux très importants, ce que des opérateurs humains ne peuvent faire. Une réputation peut être détruite, une élection influencée, et, en matière criminelle, la maîtrise de ces outils pourrait permettre de donner des faux indices pour incriminer un individu innocent. Je n'ose même pas aborder le fait de la prise en compte à distance et leur modification dans des véhicules connectés. L'enquêteur et le magistrat ne peuvent se passer de l'IA pour se prémunir de ces fausses preuves.

## Conclusion

L'enquêteur ou le magistrat de demain devra être en mesure de comprendre les résultats fournis par ces nouveaux « sens » développés grâce à l'IA et appréhender les biais générés par ces nouveaux outils. Il devra être en mesure de distinguer la statistique (science de la donnée du passé) de la probabilité (science de la donnée du devenir), et de les utiliser. Le sixième sens dont nous dote l'intelligence artificielle va devoir être intégré et géré par notre cerveau afin qu'il ne fasse pas qu'amplifier nos capacités individuelles, mais qu'il affine notre intelligence humaine. La disponibilité étendue de la connaissance offerte par l'IA est une opportunité qu'un professionnel ne peut laisser de côté. Comme nous le savons tous, l'histoire regorge d'exemples démontrant que l'évolution technique ne devient progrès qu'en fonction de la pertinence de ses applications et, qu'en la matière, les risques de dérives sont légion, surtout si on ne l'accompagne pas. L'intelligence artificielle c'est l'expertise partout et accessible à tous, la conduite de l'enquête judiciaire ne sera pas épargnée et il ne paraît pas concevable que la justice se fasse hors des tribunaux, par des utilisateurs de données et d'algorithmes, dont la déontologie et l'éthique ne seraient pas éprouvées. La présence d'un individu dans tel magasin est désormais connue de nos applications informatiques, il serait regrettable que l'enquête l'ignore.

À travers le *machine learning* (apprentissage de la machine) et l'exploitation de données de masse, c'est la capacité de faire des analyses prédictives qui est en jeu. À aucun moment, il ne s'est agi ici de parler de justice prédictive ou de police prédictive, qui font appel à d'autres paradigmes, car la problématique de la conduite de l'enquête se suffit à elle-même. Au regard des milliards de données constituant un dossier pénal ce jour, il n'apparaîtrait pas responsable de se passer de l'IA dans la recherche de la vérité judiciaire ■

(14) <https://www.lemondeinformatique.fr/actualites/lire-la-gendarmerie-nationale-stoppe-un-botnet-geant-controle-depuis-la-france-76248.html>



# L'intelligence artificielle au service des politiques publiques de prévention

Jérôme LAGASSE

« Toute politique doit prendre en compte l'état des connaissances techniques, scientifiques et créer les conditions de leur production. Pour ce faire, les villes doivent se donner les moyens de s'assurer que leurs politiques sont déterminées et guidées par des données probantes tant qualitatives que quantitatives, et non pas par des préjugés ou postures idéologiques.<sup>1</sup> » L'intelligence artificielle, par ses solutions, peut contribuer à améliorer le pilotage des politiques de prévention de la délinquance. Cette nouvelle technologie de rupture impacte, à terme, les stratégies de sécurité, la culture des organisations policières et l'exercice du monopole de la violence légitime par l'État.

## Jérôme LAGASSE



Jérôme Lagasse est chef du Département stratégie-recherche au Centre

de recherche de l'École des officiers de la gendarmerie nationale (CREOGN) et doctorant en science politique à l'université Paris V Descartes (directeur de Thèse, Thierry GARCIN, politologue, chercheur associé (HDR) à l'Université Paris Descartes).

« Any policy must take into account the state of technical and scientific knowledge and create the conditions for their production. To do this, cities must be empowered to ensure that their policies are determined and guided by both qualitative and quantitative evidence, not ideological prejudices or postures. » Artificial intelligence through its solutions can help improve the steering of crime prevention policies. This new disruptive technology ultimately impacts security strategies, the culture of police organizations and the exercise of the monopoly of legitimate violence by the state.

(1) Forum européen pour la sécurité urbaine (Efus), *Manifeste d'Aubervilliers et de Saint-Denis*, 2012, p.7. <https://efus.eu/files/2013/06/Manifeste-VF-2.pdf>



La transformation digitale marque-t-elle une disruption dans les politiques publiques de sécurité ? Ces dernières étant à la recherche d'un pilotage équilibré, évoluant telle une ligne de crête qui délimite les versants de la répression et de la prévention. Sur ce dernier point, l'espace public constitue le réceptacle naturel des politiques de la prévention. Émanation du « vivre ensemble », l'espace public<sup>2</sup> est l'« étendue », le « lieu » et la « place » des citoyens où les enjeux de cohésion sociale<sup>3</sup> insufflent l'esprit de toute politique de prévention.

Dans ce contexte, l'emploi de l'intelligence artificielle (IA), dans un processus décisionnel, revisite en premier chef les méthodologies statistiques<sup>4</sup>. La transformation numérique apporte une nouvelle fraîcheur dans l'interprétation des données de masse. De fortes attentes sont placées tout particulièrement sur la méthodologie statistique inductive<sup>5</sup>. À ce sujet, les algorithmes de type *machine learning*<sup>6</sup> apportent une plus-value qui s'exprime par leur aptitude à mettre en évidence des corrélations qui sont autant de signaux faibles dans l'aide au diagnostic de sécurité.

Dans l'identification des causes de la délinquance et dans le diagnostic de sécurité, l'analyse « prédictive » peut compléter utilement les méthodes statistiques traditionnelles qui se fondent sur des raisonnements déductifs.

Des acteurs des politiques publiques de sécurité ont perçu l'intérêt de maîtriser l'exploitation et l'interprétation

des données. Dès 2015, le 1<sup>er</sup> rapport d'activité de l'administrateur général des données (AGD) citait comme bonne pratique<sup>7</sup> l'usage des données par la gendarmerie nationale dans la conception d'algorithmes<sup>8</sup> dits « prédictifs ». Le programme concerné, *PredVol*<sup>9</sup>, a été conçu pour apporter un éclairage sur les tendances à court et moyen terme des actes de vols de véhicules à l'échelle d'un département.

Cette contribution fera sienne la définition de l'intelligence artificielle adoptée par la Commission d'enrichissement du vocabulaire<sup>10</sup> : « *Un champ interdisciplinaire théorique et pratique qui a pour objet la compréhension de mécanismes de la cognition et de la réflexion, et leur imitation par un dispositif matériel et logiciel, à des fins d'assistance ou de substitution à des activités humaines* ». À travers cette définition, il est possible de distinguer ce que les spécialistes nomment IA « forte<sup>11</sup> » et IA « faible<sup>12</sup> ». Sur un plan plus idéologique, il existe une opposition parmi ces spécialistes entre les partisans d'une IA symbolique<sup>13</sup> et ceux d'une IA connexionniste<sup>14</sup>.

C'est précisément à partir de la définition *supra* que cet article se propose de s'interroger sur la place de l'IA dans les politiques de prévention de la délinquance. L'IA est actrice d'un nouveau paradigme suscitant des doutes sur la capacité de l'humain « à garder la main<sup>15</sup> ». Elle pose, à bien des égards, des questionnements sur la place de l'État dans son rôle de coordonnateur des politiques de prévention et plus généralement sur son action à l'égard des populations.

(2) L'espace public peut être entendu comme : « un bien commun à plusieurs titres. Il est à la fois l'étendue sur laquelle chacun possède un droit d'accès, le lieu où les individus se croisent sans établir de relations et la place où s'échangent et se débattent les opinions. Dans ce dernier sens il est même le bien commun par excellence puisqu'il fonde la cité démocratique ». Rapport ENA, cf. Ayse Ceyhan, *Cultures & Conflits*, Rapport final, *Étude gendarmerie et technologies de sécurité, l'impact de la haute technologie sur la sécurité, analyse comparée*, 2005, p. 27.

(3) Cohésion sociale, définition du Conseil de l'Europe : [https://www.coe.int/t/dg3/socialpolicies/socialcohesiondev/source/GUIDE\\_fr.pdf](https://www.coe.int/t/dg3/socialpolicies/socialcohesiondev/source/GUIDE_fr.pdf)

(4) Cf. Adolphe Quételet (1796-1874) - Mathématicien et statisticien qui a conceptualisé l'expression « homme moyen » - Cf. *Lettre sur la théorie des probabilités appliquée aux sciences morales et politiques*, 1846.

(5) « Dans le raisonnement inductif, les prémisses fournissent des arguments forts, mais pas des preuves de la conclusion. Nous passons des faits à des règles et les mathématiques permettent de mesurer l'incertitude pesant sur ces règles, dépendant notamment des faits sur lesquels ces règles sont basées », Pierre Delort, *Le Big Data*, Coll. Que sais-je ?, PUF, 2015, p. 42.

(6) *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 », *Algorithmes et décisions publiques*, CNRS Éditions, coll. Les Essentiels d'Hermès, glossaire p. 242, 2019.

(7) AGD, Rapport au Premier ministre sur la gouvernance de la donnée 2015, Les données au service de la transformation de l'action publique : *Lutter contre le vol de voiture à l'aide des data sciences*, p. 7.

(8) Algorithme : mot dérivé du nom d'un mathématicien Perse, Al-Kwarizmi (783-850) est un ensemble d'instructions informatiques permettant de réaliser un calcul.

(9) Gauthier (F.), 2017, « Prédire les vols de voiture », *Revue de la gendarmerie nationale*, n° 260, p. 147-153.

(10) Commission d'enrichissement du vocabulaire, avis, JO du 9 décembre 2018, Texte 58/84.

(11) IA forte : IA dotée de conscience, de sensibilité et d'esprit ou IA générale capable d'appliquer l'intelligence à tous les problèmes.

(12) IA faible : IA non sensible qui se concentre sur une tâche précise. Tous les systèmes actuels sont considérés comme des IA faibles.

(13) IA symbolique : fondée sur la modélisation du raisonnement logique, sur la représentation et la manipulation de la connaissance par des symboles formels. Approche top-down.

(14) IA connexionniste : vise l'émergence de phénomènes relevant de la conscience ou de l'intelligence, à partir d'un agencement de mécanismes élémentaires... inspirés du vivant. Approche bottom-up.

(15) Commission nationale de l'informatique et des libertés, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, décembre 2017, 75 p.

## Intelligence artificielle et prévention de la délinquance : de la prévention situationnelle au *predictive policing*

La prévention de la délinquance est un ensemble de mesures dissuasives visant à produire un effet significatif, dans l'espace et dans le temps, sur la commission d'actes de délinquance. Ces mesures peuvent être « passives », au sens où elles s'inscrivent de manière globale dans le cadre d'études de sûreté de sécurité publique rendues obligatoires. Elles se complètent par des mesures « actives » à partir d'une analyse territoriale des données de la délinquance.

La prévention situationnelle entre dans le périmètre des mesures « passives ». Celle-ci part du constat qu'une politique de prévention de la délinquance ne peut se limiter à des mesures dites « primaires », c'est-à-dire à caractère éducatif et social. Pour ce faire, des technologies de sécurité, déployées dans l'espace public, jouent un rôle dissuasif en inhibant la petite délinquance dans sa volonté de passer à l'acte. Dès 1995, le criminologue Ronald V. Clarke affirmait qu'en « *inversant radicalement la perspective, la prévention situationnelle se veut agir non plus sur le criminel potentiel, mais bien sur les conditions matérielles et objectives du délit à commettre. Cette approche volontairement pragmatique et technicisée place de facto la technologie au centre des dispositifs de prévention*<sup>16</sup> ». L'IA accentue ainsi davantage la place faite aux stratégies de prévention de la délinquance en permettant, par exemple, d'interpréter dans un centre de supervision urbain certains faits et gestes d'individus dans l'espace public.

## Le *predictive policing* un prolongement de l'intelligence *led policing*<sup>1</sup> (ILP) ?

La terminologie « police prédictive<sup>18</sup> » soulève des discussions dans l'aire francophone, car elle ne traduit pas fidèlement la portée du sens *Predictive Policing*<sup>19</sup>. Même si l'emploi de cette terminologie se révèle utile pour la compréhension du plus grand nombre, elle n'en demeure pas moins très connotée<sup>20</sup>. Une étude commanditée par le Centre des hautes études du ministère de l'Intérieur<sup>21</sup> (Chemi) a le mérite d'ouvrir une discussion en proposant une définition pertinente de la police prédictive : « *Toute opération de maintien de l'ordre fondée sur l'anticipation spatio-temporelle du phénomène criminel, ou d'une partie de celui-ci, dans le but de mettre en place des opérations de prévention, d'investigation ou de répression d'une infraction selon un cadre juridique adapté* ».

### Les enjeux

Le rapport du député Cédric Villani, intitulé : *Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne*, porte un regard prospectif des activités de police et de justice<sup>22</sup>. Son rapporteur souligne l'indispensable dimension éthique dans l'usage des logiciels prédictifs corrélée à celle de la responsabilité. Sur ces points, les politiques de prévention de la délinquance ont intégré dans le passé une dimension éthique dès la phase de conception de la loi<sup>23</sup>. Sur un plan juridique, le Conseil constitutionnel rappelle qu'il appartient au législateur, sous le contrôle du juge, de rechercher un équilibre entre les objectifs poursuivis et les atteintes portées aux droits

(16) Ronald V. Clarke, « Les technologies de sécurité, de nouvelles ressources pour la sécurité », *Les Cahiers de la sécurité intérieure*, n° 21, 1995, p. 101-113.

(17) *Activités de police fondées sur le renseignement* (Office québécois de la langue française - 2014).

(18) « Prédiction : action de prédire, d'annoncer ce qui doit advenir », dictionnaire électronique de l'académie française, 9<sup>e</sup> édition.

(19) *Predictive policing : prévision policière*.

(20) En ce sens : « *écarter, au présent et à l'avenir [...] le recours massif et indiscriminé à des technologies intrusives qui permettraient de prédire la probabilité qu'un fait délictueux ou criminel se produise à tel endroit et à tel moment. Pour futuriste qu'elle soit en France, cette perspective est d'ores et déjà une réalité dans certains pays qui se sont dotés, en matière de sécurité urbaine, de techniques de police prédictive* », cf. : Assemblée nationale, Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, *Numérique et libertés : un nouvel âge démocratique*, Rapport n° 3119, XIV<sup>e</sup> législature, Christian Paul et Christiane Féral-Schuhl, coprésidents. p. 168.

(21) Chemi, *Rapport sur la police prédictive et la résilience organisationnelle des acteurs de la sécurité intérieure*, projet porté par l'équipe de recherche Louis Josserand de l'Université Jean-Moulin Lyon 3, Anne-Sophie Chavent-Leclere et al : Hélène Monier et Cyril Piotrowicz, mai 2018, p. 13.

(22) Cf. partie 5, p. 150 : *Quelle éthique pour l'IA ?*

(23) La saisine des sénateurs sur la loi 95-23 du 21 janvier 1995 débutait par : « *Big Brother is watching you* ». Cette prédiction de George Orwell ne s'est heureusement pas réalisée, comme il le craignait, en 1984. Dix ans plus tard, les habitants de telle importante commune des Hauts-de-Seine font l'expérience de la sollicitude électronique, omniprésente et oppressante, de leur municipalité. Et demain ? », DC n° 95-352 du 18 janvier 1995 - Saisine par 60 sénateurs.

et libertés constitutionnels. S'agissant du *predictive policing*, cette technologie a pour objectif parfaitement légitime la prévention d'infractions. En revanche, il appartient au législateur de déterminer quelles seront les données pertinentes à fournir à une IA *lambda* pour parvenir à ce but. En fonction des choix opérés, il pourrait s'agir soit de prévenir le passage à l'acte d'individus sur la base de données de profilage<sup>24</sup>, soit d'utiliser des données tenant aux biens à protéger exploitées par un système géomatique<sup>25</sup>. Dans ce dernier cas de figure, une IA délivre des prévisions sur la commission d'actes susceptibles de se commettre dans un territoire circonscrit. Celle-ci se limite à une fonction d'aide à la décision. En l'état du droit positif, une décision<sup>26</sup> du Conseil constitutionnel semble indiquer que la première hypothèse ne peut prospérer en France. La haute juridiction a rappelé que les algorithmes devaient rester sous le contrôle et la supervision de l'humain.

Au cœur de cette problématique, le rapport de la Commission nationale de l'informatique et des libertés (CNIL) : *Comment permettre à l'homme de garder la main ?*, a identifié cinq fonctions<sup>27</sup> potentielles pour l'IA au sein de sept secteurs d'activité<sup>28</sup>. S'agissant des fonctions dites « Sécurité », le champ de la prévention de la délinquance est plus marqué que celui de l'investigation. Dans ce secteur, il en ressort des attentes en termes de détection, de prédiction et de suggestion.

Au vu de ce premier constat, peut-on considérer que l'ILP a constitué un tremplin vers le *predictive policing*<sup>29</sup> ? Pour les tenants de cette thèse, l'ILP repose sur l'analyse et le renseignement comme fonctions pivots. L'objectif est de prioriser dans un processus décisionnel les lieux les plus sensibles de la délinquance, les victimes répétées, les délinquants les plus prolifiques et les groupes criminels.

*De facto*, l'ILP facilite la réduction de la criminalité et les dommages sociaux causés. Elle permet de créer des points de rupture, de mettre en œuvre des actions préventives au travers de la gestion, du déploiement de la force et de l'application de la loi tant au niveau stratégique que tactique.

L'ILP, tout comme le *predictive policing*, repose bien sur le partage et l'utilisation d'informations et d'observations pour orienter, analyser et agir en temps réel. Pourrait-on alors admettre que le *predictive policing* est une version « augmentée<sup>30</sup> » de *intelligence led policing* ?

Dans l'affirmative, l'IA contribuerait à améliorer les capacités cognitives d'un décideur, à développer son sens critique, en l'assistant sous forme de recommandations dans la réalisation de sa mission.

## L'émergence d'un nouveau paradigme des politiques publiques de prévention de la délinquance

Selon Easton, un paradigme de politique publique se décompose en trois phases : une première dite « de crise », suivie d'une deuxième qualifiée de « concurrentielle » et enfin une troisième qui consacre une nouvelle norme.

1. Une phase de crise : différentes séquences de politiques publiques de prévention et/ou de répression se sont succédé. Chacune d'elles a connu, au gré des législatures, des résultats en demi-teinte. Une des causes trouve son

(24) L'art. 4 du Règlement général sur la protection des données définit le « profilage » comme : « Toute forme de traitement automatisé de données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

(25) « La géomatique est [...] la constitution progressive d'un champ de pratiques et de savoirs à partir de la prise de conscience progressive que des formes distinctes d'information convergent vers une structure numérique commune [souligné par nous]. Plus la numérisation des technologies de l'information à référence spatiale avance, plus aisée devient la connexion entre les différentes applications et métiers liés à cette information ». Cf. Jean-Paul Bord, <http://www.univ-montp3.fr/ateliermercator/wp-content/uploads/pdf/introColloque130110.pdf>

(26) DC n° 2018-765 du 12 juin 2018, loi relative à la protection des données personnelles, §71. « En dernier lieu, le responsable du traitement doit s'assurer de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard. Il en résulte que ne peuvent être utilisés, comme fondement exclusif d'une décision administrative individuelle, des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement ».

(27) Les grandes fonctions : générer de la connaissance, faire du matching, prédire, recommander et aider la décision, p. 22.

(28) Ces sept grands secteurs sont : éducation, justice, santé, sécurité, travail/RH, culture et autres (idem note 26).

(29) Ratcliffe mais aussi l'European Crime Prevention Network.

(30) L'humain augmenté désigne « "l'amélioration" technique des performances humaines, aussi bien physiques, intellectuelles qu'émotionnelles. », cf. Dévédec (N. le) et Guis (F.), 2013, « L'humain augmenté, un enjeu social », *Sociologies* [En ligne], premiers textes, mis en ligne le 19 novembre 2013, consulté le 2 juin 2019. URL : <http://journals.openedition.org/sociologies/4409>

explication dans les capacités de calculs insuffisantes au regard du nombre considérable de données pertinentes à analyser ;

2. Une phase concurrentielle : la méthodologie statistique en est l'illustration. Il s'agit d'identifier quel modèle d'analyse de la donnée sera le chef de file. Avant la transformation numérique, le modèle reconnu est la statistique déductive, conforme à la vision dominante de la statistique comme étant « *le produit de convention sociale* »<sup>31</sup>. Dans le champ des politiques publiques de sécurité, les décideurs opérationnels s'inscrivent dans une tendance tournée vers une posture pro-active. Cette dernière posture les conduit à recourir à la méthode de raisonnement statistique inductive<sup>32</sup>, plus propice à apporter un avantage manifeste dans la détection de signaux faibles et générer de nouvelles connaissances. La statistique inductive permet ainsi de repérer des liens insoupçonnés pour la résolution d'enquêtes, de prédire l'occurrence future de crimes et délits ;

3. Une séquence de « normalisation » : dans le domaine des politiques publiques de sécurité, cette séquence n'est pas complètement stabilisée en raison notamment des progrès que procure l'IA en termes d'analyse cognitive. Il est raisonnable d'envisager que l'IA apportera une action publique de la donnée « augmentée » qui se traduira, pour les politiques de prévention, par une excroissance du périmètre des sciences forensiques.

Face à ce changement de paradigme, le ministère de l'Intérieur oriente sa vision prospective de l'intelligence

artificielle<sup>33</sup>. Il s'agit de concevoir le rôle de l'humain, plus particulièrement celui des dirigeants tenus à des obligations d'*accountability*<sup>34</sup> et de *compliance*<sup>35</sup>.

## Comment permettre à l'homme de garder la main ?

Pour IBM<sup>36</sup>, les systèmes d'IA sont conçus pour améliorer les performances humaines et non pour les remplacer. Cette thèse va à rebours de l'approche généralement présentée du risque d'une IA qui supplanterait l'humain. Cela dit, l'approche augmentée de l'humain, dans ses capacités cognitives, pose surtout la question du risque d'instrumentalisation d'une IA par les recommandations formulées. Dans cette partie, nous verrons la nécessité d'un *leadership* rénové tourné vers une approche transdisciplinaire<sup>37</sup>.

## Quel commandement pour quel leadership ?

L'adoption de solutions IA dans des fonctions métiers (sécurité publique, police judiciaire, renseignement, ordre public) pose également la question des critères de détection des hauts potentiels de la sécurité intérieure. De récents travaux<sup>38</sup> mettraient en évidence qu'un *leadership* inspiré

(31) La statistique est au service de politiques publiques qui tendent à tempérer certaines inégalités pour assurer le maintien de la cohésion sociale. Cf. Alain Desrosières, [www.cairn.info/revue-sociologies-pratiques-2011-1-page-15.htm](http://www.cairn.info/revue-sociologies-pratiques-2011-1-page-15.htm)

(32) « Dans le raisonnement inductif, les prémisses fournissent des arguments forts, mais pas des preuves de la conclusion. Nous passons des faits à des règles et les mathématiques permettent de mesurer l'incertitude pesant sur ces règles, dépendant notamment des faits sur lesquels ces règles sont basées », *op. cit.* note 5.

(33) Cf. Règlement de l'appel à projets du fonds d'investissement en études stratégiques et prospectives 2019.

Axes de recherche :

- « Les méthodologies de traitement des données de masse pour améliorer la sécurité publique et la sécurité civile ;
- Les nouveaux usages des réseaux sociaux dans les nouvelles dynamiques de contestation ;
- L'aide à la décision (anticipation et conduite en temps réel modélisation ainsi que le pilotage de la performance par des plateformes d'infocentre intelligentes ;
- L'automatisation du traitement d'appel (chatbot) ».

[https://allchemi.eu/pluginfile.php/17698/mod\\_resource/content/2/Appel%20C3%A0%20projets%20FIESP%202019.pdf](https://allchemi.eu/pluginfile.php/17698/mod_resource/content/2/Appel%20C3%A0%20projets%20FIESP%202019.pdf)

(34) Obligation de rendre compte : devoir incombant à une personne physique ou morale responsable d'une tâche de répondre des résultats et du choix des moyens mis en œuvre, Commission générale de terminologie et de néologie, JO n°215, 16 septembre 2006, p. 13668.

(35) Peut se définir comme : la conformité aux actes et procédures prévues par les lois, les règles de bonne conduite tout en sensibilisant le personnel à celles-ci.

(36) Perrin (V.), 2019, *Watson AI Technical Leader*, IBM, Université Paris Descartes, Colloque : « "Intelligence artificielle et management", Projet interdisciplinaire de recherche. Quelle régulation pour l'intelligence artificielle ? » 4 juin.

(37) Déf. : « La transdisciplinarité concerne, comme le préfixe "trans" l'indique, ce qui est à la fois entre les disciplines, à travers les différentes disciplines et au-delà de toute discipline. Sa finalité est la compréhension du monde présent, dont un des impératifs est l'unité de la connaissance », <http://agora.qc.ca/dossiers/Transdisciplinarite>

(38) Veyssière (M.), Montgomery Conseil, *Manager l'intelligence artificielle dans l'entreprise aujourd'hui et demain ?* Idem note 36.

AVANT	APRÈS
Diriger & Superviser	Oser diriger & collaborer
Planifier & organiser	S'adapter/être agile, Organiser
Persuader & influencer	Communiquer
Gérer la pression & les déceptions	Se préparer à échouer
S'adapter & réagir au changement	Avoir le désir d'apprendre, Résoudre les problèmes
Avoir l'esprit entrepreneurial et le sens du business	Avoir un esprit entrepreneurial, Être orienté résultats/performance
Atteindre ses propres buts et objectifs	Se montrer volontariste

d'une culture *Soft skills*<sup>39</sup> se substituerait progressivement au modèle *Hard skills*<sup>40</sup>.

Commentaires : les compétences originelles attendues ne se limitent plus à fixer un cap (des objectifs chiffrés) et à le conserver (culture du résultat). Dans un environnement incertain et instable par nature, il devient complexe de tracer une ligne d'horizon pérenne. *A priori*, les hauts potentiels seront ceux capables d'inscrire leur politique de prévention de la délinquance dans une dimension transdisciplinaire qui fait sens. Cette philosophie pourrait se résumer : « *Dans la vie, je ne perds jamais, soit je gagne, soit j'apprends*<sup>41</sup> ».

Parallèlement, il se crée un rapport nouveau entre l'homme et la machine où l'IA est au service de la réflexion<sup>42</sup> par ses effets de *stimuli*.

Les humains	Les systèmes cognitifs
Bon sens	Trouver l'information
Morale	Identifier des modèles
Imagination	Le langage naturel
Compassion	Machine Learning
Abstraction	Éliminer les biais
Dilemme	Capacité illimitée
Rêve	Détection des signaux faibles
Généralisation	

Commentaires : l'association des diptyques : abstraction/détection des signaux faibles ; morale/élimination des biais ; bon sens/trouver l'information mettent en évidence une complémentarité sous l'angle intuition (humain)/rationalité (machine). Dans ce contexte global de transformation numérique, l'IA pourrait être « ... à notre cerveau, ce que le moteur à vapeur a été pour nos muscles<sup>43</sup> ».

De ces éléments, il est possible d'émettre comme thèse que loin de se substituer à l'homme, l'IA constitue une part d'« humain augmenté » dans tout ce qui concerne le potentiel cognitif.

## L'éthique au service des politiques de prévention de la délinquance

L'IA et les algorithmes ont suscité auprès de la CNIL une vigilance qui a justifié, de sa part, un débat public en 2017. Pour l'organisme de contrôle, « ... permettre à l'homme de garder la main » implique l'instauration de principes de loyauté et de vigilance associés à la réflexivité. Il est à souligner que ces principes, tant dans l'esprit que dans la lettre, transparaissent au sein du Code de déontologie<sup>44</sup> commun à la police et à la gendarmerie nationales. Son *corpus*, par bon nombre de dispositions<sup>45</sup>, pourrait se

(39) *Softskills* : savoirs comportementaux.

(40) *Hardskills* : connaissances spécialisées.

(41) Citation de Nelson Mandela.

(42) Source : université Paris Descartes, Colloque : « Intelligence et Management », 4 juin 2019, op. cit. 36.

(43) Hannes Gassert.

(44) Code de la sécurité intérieure, Art. R 434-1 et suivants.

(45) Art. R 434-4 - 1 : « L'autorité investie du pouvoir hiérarchique prend des décisions, donne des ordres et les fait appliquer. Elle veille à ce que ses instructions soient précises et apporte à ceux qui sont chargés de les exécuter toutes informations pertinentes nécessaires à leur compréhension. L'autorité hiérarchique assume la responsabilité des ordres donnés ».



L'IA ET LES ALGORITHMES DE TYPE MACHINE  
LEARNING PRODUISENT DEUX EFFETS  
PARADOXAUX : CÔTÉ PILE, UNE RÉELLE  
PLUS-VALUE DANS UNE FONCTION  
D'APPUI DANS L'ÉVALUATION DES OPTIONS  
OPÉRATIONNELLES ; CÔTÉ FACE, UN  
DÉTERMINISME PRÉDICTIF SUSCEPTIBLE  
D'INHIBER TOUTE FORME D'ESPRIT CRITIQUE.



révéler un atout dans l'accompagnement du changement à l'égard de l'ensemble des membres des forces de sécurité. En effet, l'IA et les algorithmes de type *machine learning* produisent deux effets paradoxaux : côté pile, une réelle plus-value dans une fonction d'appui dans l'évaluation des options opérationnelles ; côté face, un déterminisme prédictif susceptible d'inhiber toute forme d'esprit critique.

## Quelle place pour l'État au sein des futures politiques de prévention de la délinquance ?

La philosophie politique et du droit apporte une hauteur de vue sur les questions de prévention de la délinquance. Ainsi, Michel Foucault, dans ses concepts de gouvernementalité<sup>46</sup> et de biopolitique<sup>47</sup>, aborde les dispositifs de sécurité au service des circulations.

Pour le philosophe, les dispositifs de sécurité ont pour finalité non plus « de fixer et marquer le territoire, mais laisser faire les circulations, contrôler les circulations, trier les bonnes et les mauvaises, faire que ça bouge toujours, que ça se déplace sans cesse, que ça aille perpétuellement d'un point à un autre, mais d'une manière telle que les dangers inhérents à cette circulation en soient annulés<sup>48</sup> ». Et d'en déduire : « Non plus sûreté du prince et de

son territoire, mais sécurité de la population et, par conséquent, de ceux qui la gouvernent ». L'enjeu entre l'État et la population ne se place plus au niveau d'un pacte territorial, mais bien d'un pacte de sécurité. Ce changement de pacte crée un nouveau paradigme entre la population et l'État qui s'accélère sous les effets de l'IA. L'État n'est pas attendu exclusivement dans son rôle régalien de défense des frontières, mais surtout dans sa capacité à garantir « contre tout ce qui peut être incertitude » : [...] « il y a des délinquants ? On va vous assurer leur redressement, une bonne surveillance policière ! » d'où en conséquence « ... que ce pacte de sécurité ne peut pas être de même type que le système de légalité par lequel, autrefois, un État pouvait dire : Écoutez, voilà, vous serez punis si vous faites telle chose, et vous ne serez pas punis si vous ne la faites pas ». Et Foucault d'affirmer que : « l'État qui garantit la sécurité est un État qui est obligé d'intervenir dans tous les cas où la trame de la vie quotidienne est trouée par un événement singulier, exceptionnel<sup>49</sup>. Du coup, la loi n'est plus adaptée ; du coup, il faut bien ces espèces d'interventions, dont le caractère exceptionnel, extra-légal, ne devra pas paraître du tout comme signe de l'arbitraire ni d'un excès de pouvoir, mais au contraire d'une sollicitude ». Pour Foucault, les politiques publiques de sécurité montrent leur impuissance si l'État, une fois le trouble à l'ordre public consommé, exerce son monopole de contrainte de la violence légitime *a posteriori*. Dans ce cas, le lien de confiance entre l'État et la population subit une altération. Pour restaurer ce lien de confiance et donc se voir reconnaître sa légitimité dans son monopole, l'État est tenu de prendre une posture pro-active dans ses dispositifs de sécurité. Le philosophe décrit l'esprit qui anime l'État : « Regardez comme nous sommes prêts à vous protéger, puisque, dès que quelque chose d'extraordinaire arrive, évidemment sans tenir compte de ces vieilles habitudes que sont les lois ou les jurisprudences, nous allons intervenir avec "tous les moyens qu'il faut". Ce côté de sollicitude omniprésente, c'est l'aspect sous lequel l'État se présente. C'est cette modalité-là de pouvoir qui se développe ».

Peut-on considérer que les politiques contemporaines de prévention de la délinquance sont marquées du sceau d'une « sollicitude omniprésente » ? Sur un plan juridique, l'intention du législateur semble manifeste. Le Code de la sécurité intérieure stipule<sup>50</sup> que constituent des orientations permanentes d'une politique de sécurité publique « l'extension à l'ensemble du territoire d'une police de proximité répondant aux attentes et aux besoins des personnes en

(46) Ensemble complexe d'institutions, de savoirs, de normes, de procédures et de calculs permettant à l'État moderne de consolider sa puissance en renforçant son contrôle sur la population. *Lexique de science politique*, Dalloz, 3<sup>e</sup> édition, 2014, p. 254.

(47) Toutes les formes de pouvoir s'exerçant directement sur les personnes, sur leur vie et sur leur corps. *Idem*, 46.

(48) Extrait de l'entretien de Foucault, *La sécurité de l'État* (entretien avec R. Lefort), *Tribune socialiste*, 24-30 novembre 1977, p. 3-4. En gras et souligné par nous.

(49) *Idem* note 48. En gras et souligné par nous.

(50) Art. 112-2 al.1.

*matière de sécurité*». Certains programmes d'action publique y répondent. Ainsi, l'instauration d'une Police de sécurité du quotidien (PSQ), les brigades de contact, les opérations tranquillité vacances (OTV), tout comme la création du Schéma national d'intervention pour faire face aux tueries de masse, sont autant de manifestations de sollicitudes envers la population. Dans toutes ces actions, l'IA, par ses capacités à réaliser des corrélations au sein de masses de données structurées ou non, apporte aux politiques de prévention de la délinquance une vision augmentée dans le champ des possibles en matière de scénarios prévisionnels de troubles à l'ordre public.

## L'influence de l'IA accélère la trajectoire d'un État post-moderne

Le développement de l'IA au service des politiques de prévention rebat les cartes sur la place et le rôle respectif de l'État, des collectivités territoriales, des acteurs privés de la sécurité et du tissu associatif. L'IA fera bouger les lignes de la coproduction de sécurité. En cela, l'intégration de solutions d'IA dans les dispositifs de vidéoprotection, comme la reconnaissance faciale ou l'analyse comportementale, affermit les partenaires de l'État dans cette coproduction.

Plus globalement, l'IA fait partie des réponses qui s'inscrivent dans la trajectoire d'un État dit « post-moderne<sup>51</sup> » dont les traits caractéristiques sont pour Jacques Chevallier : « ... un État... marqué par l'incertitude, la complexité et l'indétermination<sup>52</sup> ». Les champs algorithmiques de l'IA incarnent une disruption, remodelant l'exercice du *leadership* de l'État, tant dans l'exercice de son monopole de la violence légitime, que comme régulateur et coordonnateur des mesures de prévention de la délinquance.

À ce stade, la maîtrise du cycle de la donnée est un préalable au développement de l'IA. Elle exige des investissements conséquents par des partenariats public/privé<sup>53</sup>. Ces investissements s'inscrivent apparemment dans une problématique de « la montée des risques » qui « appelle le recours à des stratégies nouvelles » consistant en « l'adoption de mesures non seulement réparatrices, mais encore préventives<sup>54</sup> ». Les programmes d'IA « augmentée », à destination des politiques de sécurité publique ne préfigurent-ils pas l'amorce d'une doctrine du « pivot<sup>55</sup> » ? Celle-ci se manifesterait, dans toutes les fonctions métiers, par des capacités d'anticipation accrues et par un mode d'organisation et de fonctionnement pro-actif, le tout ayant pour socle de valeur commun une culture de la résilience.

## Conclusion

La mobilité accrue des personnes, des biens et des services, par le biais de la transformation numérique, amène l'État à reconsidérer ses modes d'action de prévention de la délinquance. Les solutions d'IA, vues sous le prisme de la prévention de la délinquance, annoncent-elles à l'intérieur de ce qu'il est convenu de nommer la *datasphère*<sup>56</sup> la mise en place d'« une sorte de chaîne qui laisse toute liberté de faire le bien et qui ne permette que très difficilement de commettre le mal<sup>57</sup> » ? Il est loisible de mesurer l'existence d'un lien ténu entre, d'un côté, une sollicitude omniprésente à l'égard des populations, et, de l'autre, le sentiment d'un glissement vers un modèle de surveillance de masse. Pour autant, l'ouverture des données procure aux citoyens l'exercice d'une démocratie *smartphone*. La multitude d'applications à base d'IA permet à chaque citoyen de mettre en œuvre, dans une finalité de contre-pouvoir, des mesures de « sousveillance<sup>58</sup> » ■

(51) Chevallier (J.), 2017, « L'État post-moderne », LGDJ, Paris, 328 p.

(52) *Idem* note 51, cf. page de couverture.

(53) Ville de Nice et Société Thalès, Projet d'expérimentation « Safe City » : délibération CM du 7 juin 2018, N° 40.1.

(54) *Op.cit.*, note 48.

(55) Terme désignant la nouvelle doctrine américaine déplaçant son centre de gravité militaire et diplomatique de l'Europe vers l'Asie-Pacifique.

(56) « Un nouvel espace à l'intérieur duquel circule une multitude de données.[...] Cette sphère numérique est une sorte de reflet du monde physique dans lequel on trouve trace de l'activité humaine [...] », Bergé (J.-S.), 2018, « Les flux au-delà du contrôle : vers la maîtrise d'un risque invisible », *LIREC*, n° 57, juin, p. 4-7.

(57) Guillaudé (A.), 1974, *Mémoire sur la réformation de la police de France, soumis au Roi en 1749 par M. GUILLAUDÉ, officier de la Maréchaussée de l'Île-de-France*, Paris, Édition Hermann, p. 35.

(58) Néologisme forgé par le technologue Steve Mann : « ... dans la sous-veillance, ceux qui sont soumis à l'autorité prennent et diffusent l'information pour contrôler ceux qui possèdent une situation d'autorité », Ganascia (J.-G.), 2014, « De la surveillance à la "sousveillance" », p. 129, in Chardel (P.-A.) (coord.), *Politiques sécuritaires et surveillance numérique*, Coll. « Les Essentiels d'Hermès », CNRS Éditions, 215 p.

## Bibliographie

- ABITEBOUL (S.), DOWEK (G.), 2017, *Le temps des algorithmes*, Paris, Le Pommier, 192 p.
- BASDEVANT (A.), MIGNARD (J.-P.), 2018, *L'empire des données, Essai sur la société, les algorithmes et la loi*, Paris, Don Quichotte éditions, 275 p.
- BAUER (A.), SOULLEZ (C.), 2011, *Les politiques publiques de sécurité*, Paris, Presses Universitaires de France, 128 p.
- BAUER (A.), FREYNET (F.), 2009, *Les études de sûreté et de sécurité publique*, Paris, Presses Universitaires de France, 128 p.
- BENBOUZID (B.), 2014, « Dans l'esprit de la prévention situationnelle. Victimization à répétition, modélisation et cartographie prospective », *Cahiers de la sécurité et de la justice*, n° 27/28, Paris, La documentation Française, p. 207 à 216.
- BENBOUZID (B.), 2017, « Des crimes et des séismes, La police prédictive entre science, technique et divination », *Réseaux*, 6 (n° 206), p. 95-123. DOI 10.3917/res.206.0095  
<https://www.cairn.info/revue-reseaux-2017-6-page-95.htm>
- CARDON (D.), 2019, *Culture numérique*, Paris, Sciences Po Les Presses, p. 385-398.
- Conseil d'État, 2014, *Le numérique et les droits fondamentaux*, Paris, Étude annuelle, 446 p.
- DELTON (J.-M.), 2017, « La protection des données personnelles face aux algorithmes prédictifs », *Revue des droits et libertés fondamentaux*, RDLF 2017, chron. N° 12, 27 p.
- DESCLÈVES (E.), 2018, « À propos d'intelligence artificielle », Paris, *Revue de la Défense Nationale*, n° 807, février, p. 106 à 112
- FOUCAULT (M.), 2004, *Sécurité, territoire, population, Cours aux collèges de France. 1977-1978*, collection « Hautes Études », Éditions EHESS, Paris, Gallimard, Seuil, 435 p.
- FOUCAULT (M.), 2004, *Naissance de la biopolitique, cours au Collège de France. 1978-1979*, collection « Hautes Études », Éditions EHESS, Paris, Gallimard, Seuil, 355 p.
- GROS (F.), 2012, *Le principe de sécurité*, Paris, Gallimard, coll NRF, 304 p.
- HEILMANN (É.), *Comment surveiller la population à distance ? La machine de Guillaumet et la naissance de la police moderne*. [https://archivesic.ccsd.cnrs.fr/sic\\_00125574/document](https://archivesic.ccsd.cnrs.fr/sic_00125574/document)
- JEANKOWSKI (M.), 2015, « Big data, de la police préventive à la police prédictive », *Revue de la Défense Nationale*, n° 779, p. 19 à 21.
- LYON (D.) et BAUMAN (Z.), 2013, *Liquid surveillance, a conversation* (surveillance liquide, dialogue), Cambridge, Policy, 152 p.
- LOUBET DEL BAYLE (J.-L.), 2001, *Police et politique, une approche sociologique*, Paris, Éditions L'Harmattan, 320 p.
- LOUBET DEL BAYLE (J.-L.), 2012, *De la police et du contrôle social*, Paris, La nuit surveillée, 220 p.
- PERROT (P.) et ROHARD (A.), 2015, « Géomatique et renseignement criminel : accroître l'efficacité de la lutte contre la criminalité », *Géomatique Expert*, n° 105, juillet-août, pages 46 à 51.
- PERROT (P.), 2017, « What about AI in criminal intelligence ? From predictive policing to AI perspectives », *European Police Science and Research Bulletin*, Issue 16, Summer 2017, p. 65 à 76.
- PERROT (P.), 2014, « L'analyse du risque criminel, émergence d'une nouvelle approche », *Revue de l'électricité et de l'électronique* (REE 2014-5).
- PERROT (P.), CAMARA (D.), VALESCANT (N.), 2017, « Anticiper le risque dans le processus décisionnel, Applications en renseignement criminel », *Revue de l'électricité et de l'électronique* (REE 2017-5). [www.researchgate.net/publication/274071556](http://www.researchgate.net/publication/274071556)
- PERROT (P.), 2017, « Disruption et révolution numérique : une nouvelle ère pour la sécurité », *Sécurité Globale*, n° 11, automne, p.81 à 88.
- SUPIOT (A.), 2015, *La gouvernance par les nombres, Cours au Collège de France (2012-2014)*, Paris, Fayard, 520 p.
- TOUILLET (M.) et al., 2017, *Le Code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, Paris, Dalloz, 260 p.



# Trois empires et un garde- manger

Pierre BELLANGER



**L**e 8 octobre 2019, l'entreprise informatique américaine Adobe a fermé tous les comptes de ses clients au Venezuela laissant ainsi, soudain, des milliers d'utilisateurs sans accès à Photoshop, le principal logiciel de retouche photographique et à Acrobat Reader que nous connaissons pour les documents en PDF.

Ce faisant, la société californienne Adobe se mettait en conformité avec l'ordre exécutif du président Trump qui, publié début août, interdisait aux sociétés américaines quasiment tout commerce avec le Venezuela.

*Le Venezuela... Cela n'arrivera jamais en France...* » me direz-vous.

Comme disait, en substance, le général chinois Sun Tzu : « *Il ne faut pas se demander ce que l'adversaire va faire mais ce que l'adversaire peut faire* ». Une telle situation est-elle donc possible en France ?

La réponse est oui.

« *Mais les États-Unis sont nos alliés!* », entendra-t-on.

Oui, bien sûr et des alliés précieux. Pour autant, les relations internationales ne sont que rapports de force. Il n'y a là ni amis, ni alliés inconditionnels, il n'y a que des intérêts communs à un moment donné. Et ces conjugaisons opportunes n'empêchent nullement, et simultanément, entre lesdits alliés, les rivalités les plus dures en termes économiques, en compétition commerciale, en stratégie de renseignement et plus généralement en luttes géopolitiques.

Nous sommes donc à la merci d'autrui.

Les conditions d'utilisation de la plupart des services numériques que nous acceptons, sans d'ailleurs les lire, autorisent ces services à être interrompus pour des périodes indéfinies sans que cela ne nous donne droit à une quelconque compensation. Nous avons tous signé et donné notre accord, comme les utilisateurs du Venezuela.

« *Mais quand même la France, ce n'est pas le Venezuela!* » dira-t-on fort justement.

C'est pourquoi nous allons prendre un autre exemple. Un pays qui a près de cinq fois notre PIB : la Chine. Une de ses plus belles entreprises de technologie Télécom est Huawei. Huawei est le second fabricant mondial de mobiles et le premier fournisseur mondial d'équipements de réseaux de

## Pierre BELLANGER



Pionnier des radios libres, entrepreneur et expert d'Internet, Pierre

Bellanger est

le fondateur et PDG de la radio Skyrock. Il publie depuis plus de vingt ans sur les médias et le réseau, en 2014, il publie *La souveraineté numérique* aux Éditions Stock. Il a lancé en 2017 SKRED, la messagerie sécurisée, avec aujourd'hui plus d'un million d'utilisateurs dans le monde. Pierre Bellanger est à l'origine de l'adoption en France d'Alerte-Enlèvement, le système national d'alerte en cas d'enlèvement d'enfants.



téléphonie cellulaire. Après s'être, pour le moins, inspirée de sa concurrence, l'entreprise chinoise s'est désormais propulsée en tête en termes de technologie.

Le 15 mai 2019, le département du Commerce des États-Unis plaçait Huawei sur la liste des entreprises « susceptibles de mettre en péril la sécurité nationale ». Dans la foulée, Google, Qualcomm, Intel et Broadcom interrompaient leur relation avec Huawei. Huawei est ainsi privé, pour ses futures ventes de terminaux, d'Android, le premier système d'exploitation mondial pour mobile et de ses services associés : YouTube, Maps, Gmail ainsi que de la plateforme d'applications : PlayStore. Cette interdiction concerne donc également les fournisseurs de composants, elle s'étend notamment aux processeurs et modems vendus par les sociétés américaines précédemment citées.

Ainsi, dans le cadre d'une tension entre puissances, l'une d'entre elles peut frapper l'autre en utilisant l'arme de la dépendance technologique. Du jour au lendemain, les logiciels, les systèmes d'exploitation, les processeurs et autres équipements informatiques d'une nation peuvent être suspendus par une autre.

Et les données ?

Les échanges sur Internet transitent par quelques centaines de câbles sous-marins. Comme le dit Jean-Luc Villemin, directeur des réseaux internationaux d'Orange : « la sensibilité d'une économie est proportionnelle à la quantité et à l'importance des informations qui transitent sur ces câbles ».

En France, 80 % du trafic national part aux États-Unis.

Ce qu'on appelle le *cloud* et qui est, en fait, l'ordinateur de quelqu'un d'autre, se trouve généralement aux États-Unis. Nous y conservons notre mémoire, notre propriété intellectuelle et notre activité économique.

Une coupure de trafic, à ce niveau de dépendance, à ce niveau d'optimisation des processus par les données, est une interruption de nation. C'est le bouton *off* du pays.

Là encore, les conditions générales d'utilisation de ces services de *cloud* – en français : télématique – sont éclairantes : « dans la mesure où la loi le permet, le service n'offre aucune garantie, expresse ou implicite, quant aux services offerts ». Nous voilà pleinement rassurés, puisque nous avons tous signé.

Mieux encore, la majorité du trafic assuré jusqu'à présent par des opérateurs de télécommunications traditionnels l'est désormais par les principaux acteurs numériques eux-mêmes, cette part prise devrait atteindre les 90 % dans les premières années de la prochaine décennie. Mais, ce n'est pas grave puisque la fameuse « neutralité du Net » garantit l'égalité de traitement... Sauf que cette disposition ne s'applique pas au trafic sous-marin...

« On ne va pas couper le trafic d'un pays tout de même ! »

L'Algérie a vu son trafic interrompu pendant cinq jours en 2015, c'est arrivé aussi en Guinée et au Liban. Une coupure offensive est possible. Les moyens existent et les nations tout autant averties qu'en capacité se testent et s'épient sous les océans.

Plus de logiciels, plus d'informatique, plus de données. C'est tout à la fois le moteur et le carburant qui est sous le contrôle d'autrui. Nous étions des citoyens, nous sommes devenus des utilisateurs.

Certains imaginaient jadis Internet comme un métamonde, un ailleurs utopique et bienveillant et prédisaient d'ailleurs la fin des nations, résidus guerriers et autoritaires des siècles précédents. Ils avaient raison, les nations sont supplantées par des empires, des « cyber-empires ».

Une nation est délimitée par ses frontières avec d'autres nations et, à moins d'exceptions, s'en contente. Un empire croît sans cesse, dépasse ses limites, conquiert, absorbe, englobe, soumet et ne s'arrête qu'à la rencontre d'un autre empire... Le réseau est le lieu de ces empires en affrontement constant.

Un cyber-empire contrôle ses données, ses logiciels, ses protocoles, ses adresses, ses chiffrements, ses serveurs, ses composants, ses systèmes et ses processeurs. Un

cyber-empire est souverain sur le réseau. Cela s'appelle la maîtrise de son destin numérique, cela s'appelle la « souveraineté numérique ».

Actuellement, le cyber-empire américain règne et deux autres prétendent accéder à ce statut, chacun à sa manière : le chinois et le russe.

Les États-Unis ont pris politiquement conscience de l'économie de la connaissance et des autoroutes de l'information au début des années 1990 avec l'administration Clinton-Gore. L'armée, le renseignement et Internet ont, depuis, formé un écosystème étatique et privé que les guerres antiterroristes n'ont cessé d'amplifier jusqu'à atteindre une puissance globale unique et exceptionnelle. C'est la nouvelle dimension de l'empire américain. C'est, pour ce pays, une nécessité absolue pour amortir le choc numérique, la montée en puissance chinoise et s'assurer, dans ce contexte, la continuité de sa primauté mondiale.

La Chine fut probablement la première puissance mondiale jusqu'au XVIII<sup>e</sup> siècle. Deux siècles de perdu que le pays s'efforce de rattraper à marche forcée. Et le déséquilibre démographique qui s'annonce du fait du vieillissement de sa population l'oblige à encore accélérer la cadence. Ici, comme partout, le réseau est la chance de surmonter les épreuves et d'aller encore plus vite. La course chinoise a trouvé son envol par la captation tous azimuts de la propriété intellectuelle occidentale, elle cherche aujourd'hui à garantir son autonomie en développant ses propres ressources.

La Russie, plus vaste pays du monde, mais avec le PIB de la Corée du Sud, a les plus grandes difficultés à se constituer en cyber-empire. Elle s'est pourtant engagée dans cette voie en privilégiant deux axes : l'autarcie et l'offensive. L'autarcie, par la capacité à se couper volontairement du reste du réseau mondial, une loi – la loi *Runet* – a été votée en ce sens à la Douma. La Russie, elle-même très active auprès des câbles sous-marins étrangers, veut se prémunir d'une coupure agressive et garantir le fonctionnement de son réseau. Pour ce faire, elle établit un système d'adressage alternatif, se substituant à l'actuel sous-contrôle américain, rapatrie toutes les données sur le territoire russe et centralise les interconnexions des fournisseurs d'accès nationaux.

Quant à l'offensive, il n'est pas un jour sans qu'il soit fait état d'une attaque provenant selon toute vraisemblance de Russie. Le 14 octobre 2019, le secrétaire général de l'Organisation du traité de l'Atlantique nord (OTAN), Jens Stoltenberg, a pointé la montée des menaces cyber contre son organisation et a cité un seul acteur étatique agresseur : la Russie.

Notre Europe est restée, à bien des points de vue, sidérée par le développement du réseau. Elle y a vu des anges – en anglais : *business angels* – des nuages et des licornes. Elle y a vu des *start-up*, des *tee-shirts*, des *likes* et des *smileys*. Elle n'y a pas vu des machines de guerre en croissance exponentielle : une dynamique protéiforme associant de façon symbiotique opérateurs privés et fonds publics. Elle a compris trop tard qu'Internet ne vient pas s'ajouter au monde que nous connaissons, il le remplace.

C'est ainsi que nous avons choisi la subordination, la provincialisation et la colonisation. Nous avons lâché en trente ans près de mille ans d'histoire payés au prix du sang. Et cette Europe qui s'est éventrée – 700 000 victimes françaises et allemandes pour quelques centaines de mètres à Verdun en 1916 – a tout lâché en une flopée de clics.

Jadis, les criminels de guerre se disculpent en expliquant qu'ils n'avaient fait qu'obéir aux ordres. Quant à nous, nous voulions juste jouer à Candy Crush.

Nous sommes à cet instant le garde-manger, le minier numérique ou encore l'éventuel champ de bataille de ces trois empires. À l'instar de cette Afrique disputée par les puissances européennes du XIX<sup>e</sup> siècle, nous perdons dans ce dépeçage notre substance et notre esprit.

Et c'est d'autant plus tragique que le réseau est notre chance. Notre seule chance de surmonter les défis insensés du monde moderne ; notre seule chance de paix, de liberté et de prospérité.

Intervient ici ce qu'on appelle communément « l'intelligence artificielle ». Je retiens pour définition de l'intelligence : « ce qu'une machine ne peut pas faire » ; je suis donc mal à l'aise avec cette expression. Je lui préfère celle d'« *intelligence assistée* ». C'est toujours de l'IA, mais c'est plus réaliste.

La machine, certes, corrige ses erreurs et donc s'améliore par la comparaison entre ses résultats et la réalité, ce qui est remarquable, mais le processus n'en demeure pas moins une somme d'opérations stupides réalisées à grande vitesse.

Steve Jobs avait comparé l'ordinateur personnel à un vélo. Un formidable moyen d'aller plus vite, mais ce n'est pas le vélo qui va vite, c'est le cycliste. C'est le cycliste qui a le sens commun et la capacité de réagir à l'imprévu.

L'IA est une source immense de progrès : réduire l'incertitude que nous contrebalançons au XX<sup>e</sup> siècle par le gaspillage ; supprimer la routine qui a réduit à l'état de machines

précaires des générations d'êtres humains et fait perdre un temps considérable à tous. Les automates décisionnels vont nous soulagés d'un fardeau considérable. Et, c'est un champ d'innovations formidable qui s'ouvre à nous.

Mais, sans souveraineté numérique, c'est le processus le plus radical pour nous asservir et définitivement vider les meilleurs morceaux restants, tout autant que les dernières miettes du garde-manger numérique européen.

Pour nous sortir de cette nasse, deux moyens.

Il faut tout d'abord arrêter de parler de données personnelles. Une donnée personnelle ne renseigne que sur sa source. Or, aujourd'hui, les données se renseignent mutuellement, se déduisent, se corrélaient entre elles... En ce sens, définir des données par leur degré de confidentialité est bien hardi. Et puis, à qui appartient l'information sur un rendez-vous ? Et ce que j'appelle « mon carnet d'adresses » n'est pas autre chose que les adresses des autres, sur lesquelles je n'ai aucun droit, mais que des devoirs. Les données de chacun et des autres sont indissociables et chacun y conserve pourtant ses propres droits. Elles forment donc une totalité en multipropriété, c'est, en droit, une indivision. Et c'est, pour une nation, un bien commun souverain.

Un bien commun régit par nos lois, localisé sur notre territoire, chiffré par nos protocoles, transitant par des télécommunications sous nos lois, alimentant des algorithmes assujettis à nos règles et disposant, comme le dollar, de protections internationales, garanties par nos chiffrements souverains.

Cela vaut aussi pour les métadonnées, ces informations qui qualifient les données, comme la date ou le lieu d'une photo.

Les machines, les appareils, les capteurs, bref les intelligences numériques et leurs systèmes d'exploitation utilisés sur notre territoire intégreront un correctif obligatoire garantissant l'intégrité et les conditions d'usage de nos données, notre bien commun souverain. Il est probable que cette démarche suscitera des oppositions. Mais, ce n'est qu'une étape : les sociétés américaines opérant en Chine se sont conformées à des mesures analogues.

Avec les données de nos citoyennes et citoyens, nous faisons ainsi nation numérique et y appliquons les lois de la République.

Et n'oublions pas que les machines et services de nos amis américains sont soumis au *Patriot Act* qui

donne à leurs agences de renseignement un accès sans mandat à toutes les données transitant, traitées ou stockées par des sociétés américaines et leurs filiales, quel que soit leur territoire d'implantation. S'y est ajouté récemment le *Cloud Act* qui étend cette faculté aux institutions judiciaires et policières américaines. Nous voilà, *de facto*, sous droit américain.

Bien des nations européennes s'en inquiètent, notamment en France et en Allemagne et lancent des initiatives de télématique souveraine. En Allemagne, 96 % de la fonction publique dépend des suites Microsoft Office et 69 % des services de l'administration stockent leurs données sur les serveurs de cette belle entreprise.

Le secteur privé n'est pas en reste : 80 % des principales entreprises du CAC 40 en France et du DAX allemand utilisent l'excellent Amazon Web Services.

Cette subordination, volontaire ou par défaut, est incompatible avec notre souveraineté numérique.

Elle est illégale, dans les conditions actuelles, dès lors que les données deviennent par la loi un bien commun souverain.

Les composants, les logiciels, les serveurs, les routeurs et échangeurs qui traitent nos données et par lesquels transite notre trafic doivent également échapper à toute tutelle étrangère.

Cela ne signifie aucunement perdre les services et les appareils que nous apprécions tant. Ils sont bienvenus. Ils fonctionneront simplement dans notre cadre juridique.

Certains disent que nous avons perdu les compétences, que l'avance technologique américaine est telle qu'il est désormais impossible de contester cette situation et plus encore, pourquoi pas, de vouloir se lancer dans des initiatives autonomes. En fait, il est aberrant de s'être mis dans cette situation. Et il est irrationnel de ne pas se donner les moyens d'en sortir.

Le premier point était donc le nouveau statut juridique des données dont la prise en compte de l'organisation en réseau est capitale.

Le second point a trait à la compréhension de l'économie numérique : il faut passer d'une vision d'économie traditionnelle, digne du bac Sciences économiques et sociales, à une économie de guerre cyber. Dans cette économie, les données sont la monnaie première et la monnaie fiduciaire est secondaire. Ainsi, un réseau social peut brûler un milliard de dollars avant d'avoir

un plan d'affaires, car il vaut bien plus par ses enjeux de renseignement.

Lorsqu'en 1935 le radar est développé en Grande-Bretagne par Robert Watson-Watt, il est probable que s'il lui avait été demandé ses perspectives de rentabilité, il serait resté coi. Dès lors, les aviateurs allemands, leurs chasseurs et bombardiers, indétectables faute de radar, auraient gagné, en 40 et 41, la bataille d'Angleterre.

Nous devons quitter l'écume libérale qui nous est présentée comme motrice de cette mutation numérique et comprendre qu'elle est portée par de colossaux investissements d'État, tout à la fois en provenance de l'armée et du renseignement.

L'État français, quant à lui, s'est engagé à mobiliser un milliard et demi d'euros pour l'IA de 2018 jusqu'en 2022. C'est une prise de conscience, un premier pas et un encouragement à l'investissement privé. Cela nous place encore dans la course, mais loin derrière, les États-Unis, la Grande-Bretagne, la Chine ou le Canada. C'est probablement un dixième de l'investissement déclaré, américain ou chinois sur la même période.

C'est sur trois ans, 16 % du budget annuel 2017 de Facebook en recherche et développement et 8 % de celui d'Alphabet, la maison mère de Google. C'est certainement pourquoi, pour peser plus, la France inscrit l'IA dans l'agenda européen.

Espérons cependant que pour entraîner nos algorithmes apprenants, il nous soit permis d'emprunter nos propres données stockées à l'étranger...

Souhaitons aussi que ces belles initiatives sachent retenir nos talents naturellement tentés de mener cette course ailleurs pour la mener en tête.

Autre défi : l'informatique quantique. Cette technologie est l'application numérique du « *en même temps* » puisque les bits peuvent simultanément prendre les valeurs 0 et 1. Ce qui démultiplie leur puissance. Ces ordinateurs, qui réalisent

en quelques minutes des opérations qui auraient pris des milliers d'années à un supercalculateur traditionnel, vont, eux aussi, bouleverser les rapports de force. En effet, par exemple, la résistance de nos chiffrements classiques est proportionnelle au temps nécessaire pour les déchiffrer.

C'est donc avec le quantique, le risque d'une vulnérabilité presque absolue.

Pour bien faire, un plan pour l'informatique quantique va être lancé au niveau national, s'ajoutant à l'initiative européenne de soutien engagée en 2018.

Nous voyons, ici encore, cette bonne volonté publique utilisant tous les leviers à sa disposition pour agir. Régulièrement, les observateurs soulignent cependant la difficulté à passer de la recherche au marché. Ce qui a pour conséquence l'échec, trop souvent, de nos efforts. Probablement parce que l'on oublie que, dans

le numérique, la passerelle entre le laboratoire et le commerce, ce ne sont pas les fonds d'investissement, qui interviennent plus tard et sur des critères économiques, ce sont les financements et les besoins de l'armée comme du renseignement.

Dès les années 1930, le creuset innovant d'ingénieurs en électronique proches de l'université de Stanford, cerveau de la Silicon Valley, fut propulsé par les commandes de guerre en radars et en dispositifs pour l'aéronautique. Puis, au début des années 1960, la course à l'espace et l'invention du transistor en relancèrent l'expansion : Silicon Valley est la réponse à Spoutnik. L'investissement indistinctement public et militaire est le père nourricier depuis 90 ans de tout l'écosystème électronique puis numérique américain. Il n'y a pas de Silicon Valley, hier comme aujourd'hui, sans l'apport considérable de l'armée américaine et de ses dérivés en recherche, ressources et carnets de commandes.

Plus récemment, le CyberSpark, ouvert à Beersheba en 2014 en Israël, est un campus hybride qui rassemble entreprises et centres de recherche dédiés à la cybersécurité : il a pour moteur initial et continu l'investissement et l'expertise militaires.

CERTAINS DISENT QUE NOUS AVONS PERDU LES COMPÉTENCES, QUE L'AVANCE TECHNOLOGIQUE AMÉRICAINE EST TELLE QU'IL EST DÉSORMAIS IMPOSSIBLE DE CONTESTER CETTE SITUATION ET PLUS ENCORE, POURQUOI PAS, DEVOULOIR SE LANCER DANS DES INITIATIVES AUTONOMES. EN FAIT, IL EST ABERRANT DE S'ÊTRE MIS DANS CETTE SITUATION. ET IL EST IRRATIONNEL DE NE PAS SE DONNER LES MOYENS D'EN SORTIR.

La dynamique et l'attraction de cette pépinière créative soutenues par plusieurs milliards de dollars d'investissement combinés sont telles qu'Israël reçoit 20 % des financements privés mondiaux consacrés à la cybersécurité et se place ainsi au second rang mondial derrière les États-Unis. L'armée est le catalyseur et le réacteur de ce succès.

Dans le monde numérique, la distinction entre le civil et le militaire n'est pas pertinente. Le réseau est une zone de guerre et chaque terminal est à la fois arme contre nous ou avec nous, selon qui le contrôle. Le réseau est civil et militaire tout à la fois. Il est « civilitaire ». Les trois cyber-empires russes, chinois et américains ne fonctionnent pas autrement. Seuls les écosystèmes civilitaires sont compétitifs.

Il est probable qu'un nouveau champ de compétition confirmera encore cette alliance : le *new space*, le nouvel âge spatial, c'est-à-dire l'ouverture de l'espace aux acteurs du marché, comme Space X et Blue Origin, mais aussi à de nouveaux États aux ambitions spatiales tels que l'Inde, le Brésil ou la Malaisie... Et les dimensions militaires et civiles seront ici aussi inséparables. La Norvège lance deux satellites pour l'Arctique, ils seront dotés de capacité défensive. Et les grandes nations, y compris la France, se préparent à la militarisation de l'espace.

La catégorisation des données est une fiction puisqu'elles se déduisent les unes des autres. Une information collectée par une appli de jogging sur le parcours d'un sportif, lorsque c'est un militaire, est une information militaire.

De la même manière, croire qu'un collecteur de données ne les réserve qu'à son usage est au-delà du naïf. Les données circulent comme l'argent.

Toute donnée collectée par un opérateur privé est à la disposition de son État d'origine, de même toute information recueillie par un agent public, ou sous contrat, est communiquée aux entreprises de sa nation en compétition à l'étranger. Les mêmes circuits qui servent à la capture d'un terroriste sont employés pour récupérer des plans de turbine ou la configuration d'une molécule. S'y intercalent d'ailleurs officines grises et hybridations en tout genre. Le renseignement d'État et l'intelligence économique sont indissociables et consubstantiels l'un de l'autre.

La pire situation dans cette guerre numérique est de se croire en paix et de continuer à raisonner exclusivement en intérêt économique alors que la compétition, aux apparences trompeuses de pures entreprises, s'appuie en fait sur des ressources illimitées. C'est le pays qui est en jeu et pas le rendement des capitaux. Quand on se bat, on ne compte pas.

Il faut fonctionner avec trois monnaies. Une monnaie de long terme : la sécurité nationale commanditée par l'armée ; une monnaie immédiate, la donnée, financée par le renseignement. Et enfin le marché, qui s'intercale utilement entre les deux, avec ses ambitions de retour sur investissement à moyen terme et avec pour monnaie l'euro, mais qui, on le constate, ne peut être seul à porter la nation entière.

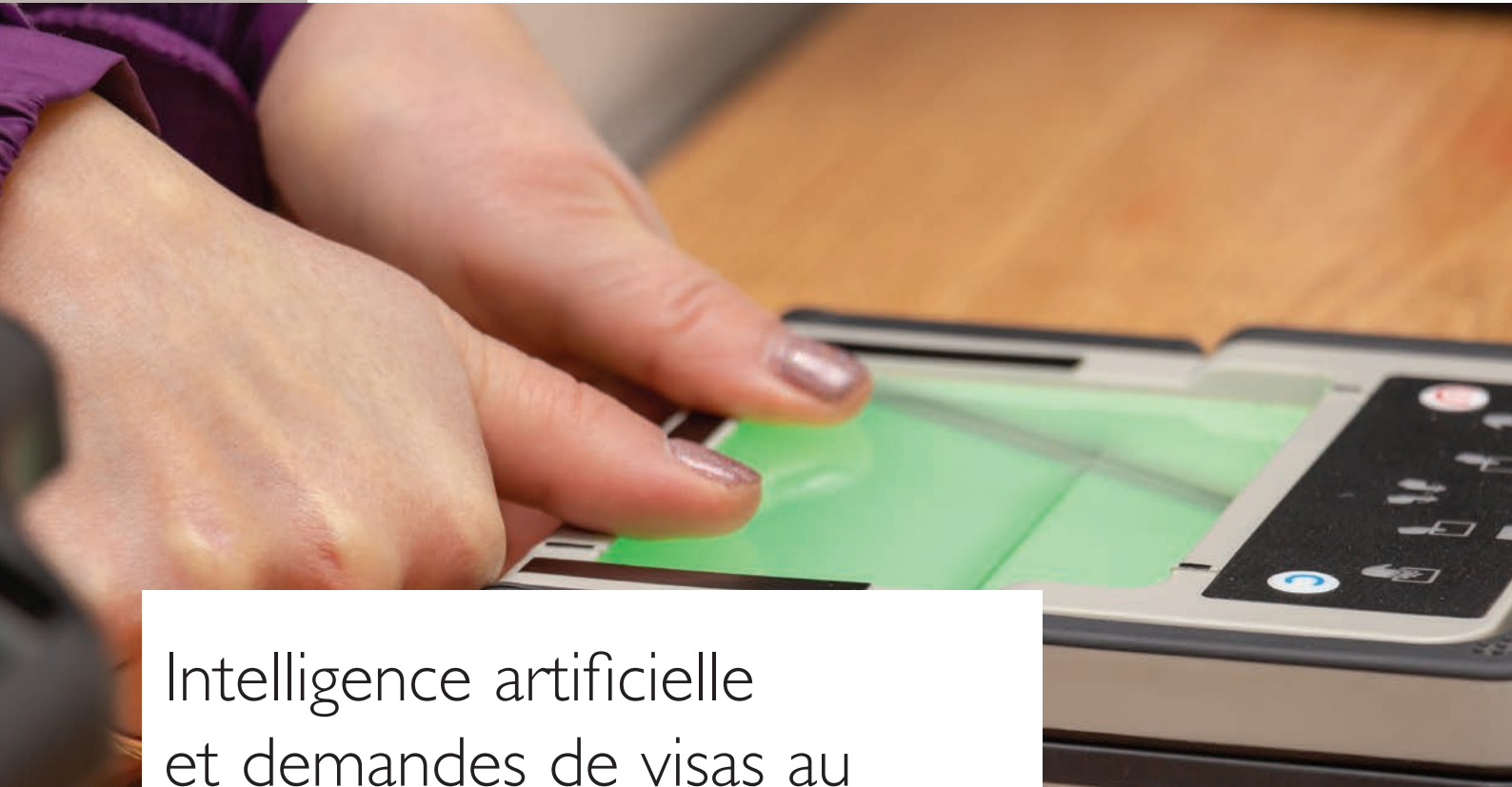
Nous n'avons aucune chance si nous continuons à être unidimensionnels dans notre calcul de valeur alors que notre compétition est tridimensionnelle.

C'est la raison de l'absence de géant de l'Internet européen.

Pourquoi cette naïveté de notre part ? Nous sommes les peuples des Machiavel, Talleyrand et Bismarck... Pourquoi sommes-nous à présent les Petit Nicolas de l'Internet ?

J'ironise pour alerter. Je sais les engagements, les talents qui œuvrent au quotidien et certainement j'ignore bien des développements en cours. Je les salue ici avec respect et reconnaissance.

Cependant, c'est pour mieux encore valoriser et faire effet de levier sur ces initiatives qu'il faut placer notre investissement collectif sur l'IA dans ce contexte de guerre cyber. Il ne nous sera laissée aucune place, aucune chance, aucun espace qui n'aura été conquis ou défendu. Comme jadis et toujours, seule notre volonté fait face à l'adversité ■



# Intelligence artificielle et demandes de visas au Quai d'Orsay

Olivier POUDADE

## L'expérimentation d'IA consulaire AVIS

**H**éritière des métiers du Chiffre, promotrice du développement de la micro-informatique dans l'Administration, la Direction des systèmes d'information (DSI) du ministère de l'Europe et des Affaires étrangères (MEAE) évolue dans un environnement technologique en constante mutation. Elle expérimente aujourd'hui l'utilisation de l'Intelligence artificielle (IA) concernant les Demandes de visas (DV) de type court-séjour (DVCS), aussi appelées « Schengen », « de type C », « 3/6 » ou encore « non-immigrant » chez les Anglo-Saxons.

Première destination touristique au monde en 2018, la France est confrontée à une augmentation volumétrique mécanique des DVCS (+255 000 en 2016) colinéaire à l'expansion démographique mondiale, dans un contexte administratif budgétaire contraint. Sur la base de la cible 2020 des indicateurs des objectifs fixés au MEAE par le ministère de l'Action et des Comptes publics dans le Projet de loi de finances (PLF) 2018 du programme 151, un système d'attribution de DVCS par Voie rapide (VR) nommé AVIS (*Accelerated visa information system*) a été expérimenté – dans les consulats de Tunis, Hô-Chi-Minh Ville et Kiev – en avril 2018 pour une période d'un an, prédisant l'opportunité d'accélérer 132 091 DVCS à la suite d'un apprentissage fondé sur 23 millions de DVCS du Réseau mondial visa (RMV).

Cette expérimentation a validé que l'efficacité qualitative (prédiction de signalements

*a posteriori*) d'AVIS est de 6 à 10 fois plus forte, selon le poste, que le système en vigueur et sa rapidité (efficacité quantitative), instantanée, dépasse les objectifs chiffrés du PLF pour 2020, dans le respect des obligations légales (PIA<sup>1</sup> du GDPR<sup>2</sup>, loi informatique et liberté de la CNIL<sup>3</sup>, traçabilité de la CADA<sup>4</sup>, sécurité du modèle PIMS<sup>5</sup> de l'ANSSI<sup>6</sup>) et des recommandations éthiques (anonymisation des champs nominatifs, lieu de naissance et photo du CERFA de demande de Visa Schengen N° 14076).

Néanmoins, le système AVIS émet seulement un avis consultatif sur l'opportunité d'accélérer le traitement d'une DVCS – l'exclusivité de l'attribution d'un visa demeurant la prérogative formelle de l'agent instructeur d'un consulat. Deux études juridiques interministérielles indépendantes l'ont d'ailleurs qualifié de système de discrimination positive.

Mais au-delà de l'emploi de l'IA au MEAE et dans l'Administration en général, ce progrès soulève plusieurs questions de fond.

Cette monopolisation de la communication autour du thème de l'IA – la peur qui en résulte légitimement – parasite et retarde une réflexion rassérénée en France et spécifiquement dans l'Administration publique. Surtout, la thématique exclusivement à la mode des méga-données ou de la « science des données » ne représente en réalité qu'environ 3 % du domaine de l'IA auquel elle appartient et de sa vraie appellation « Sciences cognitives et informatique avancée » (SCIA). Or, les SCIA n'ont pas évolué techniquement depuis l'apparition des premiers ordinateurs personnels grand public ; seule la loi de Moore (ratio capacité/prix des stockages et traitements) a démultiplié les capacités du sous-domaine des méga-données, déjà exploité à l'échelle industrielle depuis 1989 (notamment dans le tri postal).

L'aphonie de trente ans, à laquelle le rapport Villani a mis fin, n'est pas tant une spécificité française de la période « Minitel », qu'un manque de volontarisme par rapport au monde anglo-saxon.

## Les raisons de la résistance au changement en matière d'IA en France

## L'éthique de l'IA et la reconnaissance de la valeur de l'humain

Olivier POUDADE



Olivier Poudade est chargé de mission auprès du directeur des Systèmes d'information

au ministère de l'Europe et des Affaires étrangères. Ingénieur informatique spécialisé en Sciences cognitives et informatique avancée, il a participé à la conception du Réseau Mondial Visa (RMV) du ministère des Affaires étrangères en France, mais aussi à la conception de systèmes d'agents intelligents pour Dassault Systèmes, Honda Japon et la NASA, avant de travailler en génie génétique en Amérique du Nord.

L'anxiété sociologique sur l'IA s'explique en grande partie par une communication prenant la forme d'effets d'annonce spectaculaires dans les médias. Ses sources sont : les GAFA<sup>7</sup> premièrement, dont le modèle économique reposait déjà exclusivement sur l'exploitation des données utilisateur originellement (indépendamment de l'IA) ; les milieux universitaires ensuite, poussés régulièrement aux publications fracassantes dans un contexte global de baisse de renouvellements de crédits attribués à la recherche scientifique (*publish or perish*).

À la suite de la volonté récemment affichée de la Commission européenne d'instaurer la confiance dans l'IA et devant la difficulté de statuer sur les contours flous évoqués précédemment, le gouvernement pourrait, en écho à la saisie américaine du *National institute of standards and technology* (NIST) motivée par une normalisation propice à la clarification, demander à son tour une classification plus granulaire à l'homologue français AFNOR, avant de se prononcer sur l'éthique dans l'IA.

(1) Protection des données personnelles (PIA).

(2) Règlement général sur la protection des données (*General Data Protection Regulation*)

(3) Commission nationale de l'informatique et des libertés.

(4) Commission d'accès aux documents administratifs.

(5) Système de management de la protection de la vie privée (PIMS).

(6) Agence nationale de la sécurité des systèmes d'information.

(7) Google, Apple, Facebook, Amazon.



En l'attente d'éventuelles nouvelles directives interministérielles sur l'éthique dans l'IA, au sein du ministère de l'Europe et des Affaires étrangères, l'éthique a historiquement été la prérogative du Comité d'éthique des affaires étrangères (décret du 27 décembre 2007). En application de la loi du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires et du décret du 10 avril 2017 relatif au référent déontologue dans la fonction publique, cette prérogative se voit confiée aujourd'hui au référent déontologue du Département, rattaché directement au Secrétariat général du MEAE.

Se pencher sans attente sur l'étymologie de l'IA autorise d'en deviner les contours éthiques. La partie « informatique avancée » des SCIA a trait au domaine des algorithmes, dont l'analyse numérique exclue *a priori* la notion d'éthique puisqu'elle est absente par nature des mathématiques appliquées. La partie « sciences cognitives », en revanche, en sanctionne l'inspiration initiale neurophysiologique s'arrêtant aux portes philosophiques de la conscience collective, considérée du domaine réservé des sciences sociales. Néanmoins, en pratique, l'éthique en IA portant sur les méga-données serait donc celle des personnes ayant traité antérieurement ces mêmes données, nécessaires pour l'apprentissage par machine. Dans le cas spécifique de l'Administration publique, ces personnes représentent les agents de la fonction publique, répondant par ailleurs déjà de facto à l'ensemble du corpus des exigences légales déontologiques.

Par expérience, l'IA induit paradoxalement la correction d'injustices aux processus existants issus du cloisonnement des tâches auxquelles il se substitue. Par exemple, dans l'expérimentation AVIS, quatre dysfonctionnements importants ont été analysés puis corrigés, au bénéfice de l'ensemble des usagers consulaires concernant l'attribution présentielle de visas, le cheminement cyclique des signalements, le rétro-marquage dans les bases de données relationnelles et la cohérence globale de ces dernières face à certains types de signalements singuliers.

Il demeure enfin une résistance au changement de l'IA résultant de l'incompréhension de sa finalité et du sentiment de dévalorisation du travail, en relation avec l'éthique, portant sur l'usage des algorithmes et l'effacement d'humanisme. Là encore, l'IA dans la fonction publique s'attache, dans le respect des critères dictés par le projet de loi de finances, à déplacer un savoir-faire reconnu des agents, sur un travail moins quantitatif et plus qualitatif qu'auparavant en se départant des traitements les plus triviaux et répétitifs automatisables, signe d'une reconnaissance *a contrario* de la valeur réelle et irremplaçable de leur travail ■



## La cybersécurité dans le rétroviseur

### L'émergence d'une politique européenne (1997-2017)

Pierre BERTHELET

« Les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars. » Ces propos de la Commission européenne, tenus par Jean-Claude Juncker dans son discours sur l'état de l'Union, le 13 septembre 2017, illustrent les préoccupations actuelles à l'égard des cybermenaces<sup>1</sup>.

Largement confidentielle il y a quelques années, la cybersécurité constitue actuellement l'objet d'une politique en plein essor. La stratégie du 13 septembre

2017, qui constitue en droit positif, le document directeur de cette politique, précise que « la cybersécurité est essentielle tant pour notre prospérité que pour notre sécurité. Plus nos vies quotidiennes et nos économies deviennent dépendantes des technologies numériques, plus nous sommes vulnérables. Les incidents de cybersécurité se diversifient, en ce qui concerne aussi bien leurs auteurs que leurs objectifs<sup>2</sup> ». Il faut dire que l'Union fait de la cybersécurité une priorité majeure, la communication et l'information constituant un facteur clé du développement économique et sociétal<sup>3</sup>.

Cette stratégie de septembre 2017 s'inquiète de l'exposition des risques. Les

Pierre BERTHELET



Pierre Berthelet est Docteur en droit, chercheur associé au Centre d'études sur

la sécurité internationale et les coopérations européennes - CESICE (Univ. Grenoble)/ Centre de recherche de l'École des officiers de la gendarmerie nationale - CREOGN (Gendarmerie nationale).

(1) Disponible à l'adresse : [http://europa.eu/rapid/press-release\\_SPEECH-17-3165\\_fr.htm?locale=FR](http://europa.eu/rapid/press-release_SPEECH-17-3165_fr.htm?locale=FR)

(2) Communication conjointe de la Commission européenne et du haut représentant intitulée « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide » [JOIN(2017)450].

(3) P. 1 de la communication de la Commission du 6 juin 2001 sur la sécurité des réseaux et de l'information : proposition pour une approche politique européenne [COM(2001)298].

cyberattaques sont fréquentes, les serveurs d'installations sensibles sont la cible de *hackers*<sup>4</sup>. La cybercriminalité est en hausse notable<sup>5</sup>. Ce risque va croissant, parallèlement à la transformation numérique. Des dizaines de milliards de dispositifs reliés à l'« Internet des objets » devraient être connectés à l'Internet d'ici à 2020, mais la cybersécurité n'est pas encore une priorité dans leur conception<sup>6</sup>.

Comme beaucoup, la politique de l'Union propre à la cybersécurité est de nature horizontale, au sens où il ne s'agit pas d'une politique sectorielle répertoriée dans la troisième partie du traité FUE. Il est d'ailleurs remarquable que cette question ne figure dans aucune disposition du droit primaire, qu'il s'agisse du traité sur l'Union européenne (TUE) ou du traité sur le fonctionnement de l'Union européenne (TFUE).

Il est vrai que l'intérêt est tardif. À la lecture du droit dérivé, le terme de « cybersécurité » n'apparaît qu'au cours des années 2000. La formule de « sécurité des réseaux électroniques » (ou encore « sécurité des réseaux et de l'information » et « sécurité des réseaux et des systèmes d'information ») lui était préférée. Les cyberattaques contre l'Estonie en 2007 font office d'élément déclencheur pour les institutions européennes et pour les États membres, en leur faisant prendre conscience que l'Union reste trop vulnérable face aux menaces cybernétiques transfrontalières<sup>7</sup>.

L'objectif de cet article est d'analyser le processus de la politique européenne de cybersécurité.

Le processus de maturation de cette politique peut être séquencé en trois étapes : une phase de fécondation, où il n'est pas encore question de cybersécurité, mais de sécurité des réseaux électroniques, une phase de « gestation<sup>8</sup> », où dans un contexte de lutte antiterroriste,

le traitement des problématiques dites « CBRN<sup>9</sup> » conduit à la mise en place d'un dispositif européen de protection des « infrastructures critiques » qui, lui-même, débouche sur la protection des « infrastructures d'information critiques », et enfin une phase de mise au monde au sens où la politique européenne de cybersécurité naît d'un document directeur, la stratégie sur la cybersécurité. Une stratégie approuvée en 2013 permet de structurer l'action de l'Union dans ce domaine.

## La fécondation : la problématique de sécurité des réseaux électroniques

Avant d'aborder les prémisses de l'action de l'Union européenne en matière de cybersécurité, il importe d'apporter un ensemble de précisions concernant ce thème.

### La cybersécurité, considérations générales

Comme le note Myriam Dunn Cavelty, la cybersécurité est largement façonnée par la pensée stratégique américaine<sup>10</sup> : la crainte des cybermenaces naît à la fin des années 1980 dans l'atmosphère de la fin du conflit Est-Ouest<sup>11</sup>. Cela étant, elle émerge au moment de la montée dites « des nouvelles menaces » : la typologie classique des conflits évolue en devenant plus large, en englobant des menaces asymétriques (terrorisme, crime organisé, cybermenaces, etc.). À partir des années 1990, Internet est perçu comme un champ de bataille<sup>12</sup>. Or, les nouvelles technologies permettent cette asymétrie entre belligérants<sup>13</sup>. Elles favorisent les stratégies du faible au

(4) Le rapport de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) dénommé *Annual Incident Reports* pour l'année 2015, et consacré au secteur des télécommunications, fait état de 138 incidents majeurs, impliquant dix-neuf États membres et deux États de l'AELE. Le rapport annuel d'activité pour l'année 2016 de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) mentionne ainsi le rançongiciel Locky, chiffrant l'ensemble des disques et lecteurs des ordinateurs par partages réseaux, se propageant en France et en Allemagne, ou bien encore des attaques en déni de service distribué de grande ampleur menés à partir de centaines de milliers d'objets connectés (p. 14 du rapport de l'ANSSI).

(5) Voir à ce sujet les rapports iOCTA (*Threat Internet Crime organised Assessment*) élaborés par l'agence Europol.

(6) Comme le rappelle une résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense [p. 8\_TA-PROV (2018) 0258].

(7) Boin (A.), Ekengren (M.), Rhinard (M.), 2013, *The European Union as crisis manager. Problems and Prospects*, Cambridge, Cambridge University Press, p. 122.

(8) Cammilleri (A.), 2015, « Cybersécurité et cyberdéfense européennes... What else ? », in Collectif, *Entre ordres juridiques. Mélanges François Hervoët*, Paris, LGDJ, p. 54.

(9) Nucléaire, radiologique, biologique et chimique (NRBC) ou CRBN en anglais.

(10) Dunn Cavelty (M.), 2010, « Cyber-Security », in Dunn Cavelty (M.), Mauer (V.) (dir.), *The Routledge handbook of new security studies*, Londres, Routledge, p. 181.

(11) Pour une lecture de référence, voir Ronfeldt (D. F.), Arquilla (J.), 1997, *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Rand.

(12) Yagil (L.), 2002, *La cyberguerre, Terroristes et Internet*, Montréal, Trait d'union, p. 56.

(13) Hanson (E. C.), 2008, *The information revolution and world politics*, Lanham, Rowman and Littlefield Publishers, 269 p. 119.

fort, un individu (ou un groupe d'individu) étant capable, avec peu de moyens, de mettre hors fonction certaines infrastructures, notamment des infrastructures critiques, telles des centrales nucléaires, des usines d'alimentation en eau potable ou des routeurs internet<sup>14</sup>.

Les années 2000 correspondent à une période de montée en puissance des discours étatiques sur la dangerosité du cyberspace<sup>15</sup>. La prolifération des cybermenaces, sur fond de sentiment d'insécurité globale, met en danger l'État et la nation. La militarisation du cyberspace s'accompagne par la promotion de la cybersécurité comme moyen de contrer ces cybermenaces qui présentent les caractères des « nouvelles menaces » : asymétrie, ubiquité et hybridité notamment. Cela étant, la cybersécurité s'insère dans le contexte d'une reformulation de la défense autour de la sécurité qui voit son périmètre élargi<sup>16</sup>. La sécurité est, depuis les années 1980, un concept englobant destiné à dépasser les différents cloisonnements. La cybersécurité entend, elle aussi, surmonter les frontières traditionnelles existant notamment entre la sécurité intérieure, la sécurité extérieure et la défense<sup>17</sup>. Elle s'insère dès lors dans la perspective des thèses relatives à la sécurité globale<sup>18</sup>. En vertu de cette thèse, les évolutions géostratégiques et les mutations des menaces appellent à un « retour de l'État » comme ultime rempart protecteur. En effet, cette montée en puissance des discours étatiques sur la dangerosité du cyberspace légitime un « retour en force<sup>19</sup> » des États dans le cyberspace au nom de la préservation de leurs prérogatives régaliennes menacées par la prolifération incontrôlée des cybermenaces.

Cependant, la mondialisation de l'économie et l'apparition de nouveaux acteurs l'amènent à composer

avec ces États. La sécurité globale est donc, certes, un processus transversal, c'est-à-dire permettant de dépasser ces différents cloisonnements, mais un moyen de placer chacun d'eux au cœur d'un processus collaboratif, destiné à favoriser une action de concert efficace de tous les acteurs concernés.

En France, la prise de conscience de la sécurité des systèmes d'information naît en 2005 avec la publication du rapport parlementaire Laborde<sup>20</sup>. Rapidement, les choses s'accroissent<sup>21</sup>. La cybersécurité est incluse dans le *Livre blanc* de 2008 pour qui le cyberspace est un enjeu de souveraineté<sup>22</sup>. Opérant une révolution conceptuelle, ce livre blanc a mis en évidence le fait que la sécurité des systèmes d'information constitue un élément de la souveraineté française et c'est dans cette optique qu'une politique dans ce domaine est formulée, avec comme cheville ouvrière, une structure dont les origines remontent à 1986, en l'occurrence, la création du service central de la Sécurité des systèmes d'information, lui-même remplacé en 2001 par la direction centrale de la Sécurité des systèmes d'information (DCSS<sup>23</sup>). Cette cheville ouvrière de la sécurité des systèmes d'information qui sera par la suite l'Agence nationale de la sécurité des systèmes d'information (AnSSI). Cette agence sera mise en place un an après l'adoption du *Livre blanc*, soit la même année que l'adoption de la loi de programmation militaire 2009-2014 faisant des cybermenaces une priorité de premier plan<sup>24</sup>. Quant au *Livre blanc* de 2013, il précise que les menaces identifiées en 2008, en particulier les cybermenaces, se sont amplifiées. C'est la raison pour laquelle différentes mesures sont prises, en particulier la loi de programmation militaire 2014-2019 du 18 décembre 2013. Celle-ci impose une série de

(14) Bonnaure (P.), 2012, « Infrastructures stratégiques et cyberguerre », *Futuribles*, n° 384, avril, p. 21-33.

(15) Desforges (A.), 2014, « Les représentations du cyberspace : un outil géopolitique », *Hérodote*, n° 152-153, 1<sup>er</sup>-2<sup>e</sup> trimestre, p. 78. Et pour prolonger cette analyse du cyberspace comme discours, voir dans le même numéro Nieto Gomez (R.), « Cybergéopolitique de l'utilité des cybermenaces », p. 98-116.

(16) Ronfeldt (D. F.), Arquilla (J.) (dir.), 2001, *Networks and Netwars. The Future of Terror, Crime, and Militancy*, Santa Monica, Rand. Comme le note Benoît Dupont, « on assiste cependant depuis quelques années à une évolution de la doctrine militaire. La militarisation de l'internet reflète l'évolution de la doctrine militaire, qui fait du contrôle de l'Internet non seulement un enjeu de sécurité intérieure, mais aussi de sécurité nationale avec une multiplication des ressources consacrées au développement de capacités défensives et offensives », 2013, « The proliferation of cyber security strategies and their implications for privacy », in Benyekhlef (K.), Mitjans (E.) (dir.), *Circulation internationale de l'information et sécurité*, Montréal, Les Éditions Thémis, p.67-80 (p. 16 du doc. pdf publié dans <http://benoitdupont.openum.ca>).

(17) Elle s'insère dans la perspective d'une approche globale fondée sur une approche partenariale articulée autour d'un pilier d'un « justicier » (justice, police, gendarmerie, douanes), d'un pilier du « guerrier » et d'un pilier « pompier » (le(s) autorité(s) nationale(s) en matière de sécurité des réseaux), Watin-Augouard (M.), 2012, « La cybersécurité », *Revue de la Gendarmerie nationale*, n° 244, 4<sup>e</sup> trimestre, p. 35.

(18) Voir à ce propos Roche (J.-J.), 2008, « Écologie et sécurité globale », *Cahiers de la sécurité*, n° 3, janvier-mars, p. 99-105.

(19) Douzet (F.), 2014, « La géopolitique pour comprendre le cyberspace », *Hérodote*, n° 152-153, 1<sup>er</sup>-2<sup>e</sup> trimestre, p. 10.

(20) Perrine (S.), 2006, « La sécurité des systèmes d'information. De la prise de conscience collective à la mobilisation politique », *Cahiers de la sécurité*, n° 6, octobre-décembre, p. 107-112.

(21) Baumard (P.), 2017, *Cybersecurity in France*, Berlin, Springer, p. 52-65.

(22) Et ce, en écho au rapport du sénateur Romani (voir à ce propos Romani (R.), 2006, « Cyberdéfense : un nouvel enjeu de la défense nationale », *Cahiers de la sécurité*, n° 6, octobre-décembre, p. 113-121).

(23) Mongin (D.), 2013, « Les cyberattaques, armes de guerre en temps de paix », n° 1, janvier, p. 40.

(24) Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » (NOR : PRMD0914748D).

prescriptions aux opérateurs d'information vitales<sup>25</sup>. Une telle loi rappelle également que la responsabilité d'assurer une sécurité suffisante des systèmes critiques de ces opérateurs incombe à l'État.

Cette date coïncide avec l'adoption d'une stratégie européenne en matière de sécurité promouvant, elle aussi, une approche globale. L'Union s'implique en effet dans cet effort de régulation du cyberspace et son implication va croissant<sup>26</sup>. Il est possible de remarquer également la diffusion au sein de l'Union, de l'idée d'un brouillage des menaces et de la nécessité d'une approche horizontale de sécurité<sup>27</sup>. Cependant, cette diffusion est progressive et la stratégie de 2017 en matière de cybersécurité, qui prône une telle approche horizontale à l'ère des insécurités globales, est en réalité le point d'aboutissement d'une évolution entamée il y a deux décennies.

## Les prémisses de l'action de l'Union européenne

Les années 2000 constituent le temps des premières mesures. À l'époque, il n'était pas encore question de cybersécurité, mais plutôt de sécurité des réseaux et de l'information (ci-après la sécurité des réseaux). Celle-ci peut se définir comme « *la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes* »<sup>28</sup>. L'action de l'Union en la matière apparaît comme le prolongement des efforts fournis dans le cadre de la société d'information. Elle a trait à des sujets aussi variés que la stimulation du commerce électronique, le développement de transports intelligents ou l'administration en ligne<sup>29</sup>.

La problématique de sécurité des réseaux électroniques était, à l'époque, une question, importante, mais accessoire

à la création d'une société de l'information en Europe. Autrement dit, il n'existait pas, en tant que tel, d'agenda institutionnel spécifique dans ce domaine. La sécurité des réseaux constituait un volet du projet de société numérique, entendue comme processus de digitalisation du marché intérieur.

Ce dernier peut apparaître comme la matrice de cette sécurité des réseaux électroniques, au nom du besoin de la confiance numérique. Très rapidement, la sécurité des réseaux s'élargit à d'autres problématiques, en particulier l'espace pénal européen. Les violations commises, par exemple les intrusions dans les systèmes d'information, nécessitent d'être sanctionnées et, du fait même de la nature transfrontière des comportements incriminés, un rapprochement des législations pénales nationales apparaît nécessaire.

La protection des systèmes d'information est entreprise à la fin des années 1990<sup>30</sup>. Elle s'inscrit dans le cadre du plan d'action global « eEurope 2002 » approuvé par le Conseil européen de Feira des 19 et 20 juin 2000<sup>31</sup>. Ce plan d'action est destiné à promouvoir une société de l'information en Europe. Les entreprises, comme les ménages, sont davantage connectées. Le plan d'action dénommé « eEurope » est destiné à favoriser l'émergence de cette société de l'information en Europe. Il s'agit d'un programme lancé en décembre 1999, visant à concrétiser les objectifs de la stratégie de Lisbonne de 2000. Il ambitionne de faire de l'Union européenne l'économie de la connaissance la plus compétitive au monde. Or, parmi les mesures de ce plan figure le développement de l'Internet à haut débit.

Dans une communication publiée l'année suivante, en 2001 donc, la Commission aborde la question de la protection des réseaux. Elle y met en exergue la nécessité de sécuriser ceux-ci. Pour elle en effet, la nécessité d'une

(25) Art. 22 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

(26) Wessels (R. A.), *op. cit.*, p. 424.

(27) La stratégie de 2017 consacrée à la cybersécurité énonce cette situation : « *les cybermenaces sont le fait d'acteurs aussi bien étatiques que non étatiques ; elles sont souvent criminelles, motivées par l'appât du gain, mais elles peuvent aussi être politiques et stratégiques. La menace criminelle est accentuée par l'effacement progressif de la frontière entre cybercriminalité et criminalité « traditionnelle », les criminels utilisant l'Internet à la fois pour étendre leurs activités et pour y puiser de nouvelles méthodes et de nouveaux outils en vue de commettre des délits. Or, dans la grande majorité des cas, les chances de localiser les criminels sont minimes, et la probabilité de pouvoir les poursuivre en justice est encore plus faible. Simultanément, certains acteurs étatiques poursuivent de plus en plus souvent leurs objectifs géopolitiques en employant non seulement les méthodes traditionnelles telles que la force militaire, mais aussi des outils informatiques plus discrets, y compris en interférant dans les processus démocratiques nationaux. De nos jours, l'utilisation du cyberspace comme une zone de guerre soit exclusivement, soit dans le cadre d'approches hybrides, est de notoriété publique* » (p. 2 de la communication conjointe précitée).

(28) Définition donnée figurant à l'art. 4.c du règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JOUE L 77 du 13.3.2004, p. 1).

(29) Pour approfondir ce sujet, voir Degryse (C.), 2007, *Dictionnaire de l'Union européenne*, Bruxelles, De Boeck/Larcier, 3<sup>e</sup> éd., p. 866-869.

(30) Esterle (A.), 2005, « National and European information security policies », in Esterle (A.), Ranck (H.), Schmitt (B.) (dir.), *Information security. A new challenge for the EU*, Paris, Institut d'études de sécurité (ISS), Chailot Papers, n° 76, mars, p. 39.

(31) Point 22 des conclusions du Conseil européen.

action dans ce domaine est devenue plus évidente<sup>32</sup>. Elle note que la société de l'information a encore évolué considérablement en Europe. La sécurité fait partie intégrante des mesures préconisées dans ce texte de 2001. Constatant les attaques par déni de service et les actes de sabotage de grande envergure, notamment la propagation du virus *I Love You*, elle préconise des mesures supplémentaires allant au-delà de celles mises en place dans le cadre de la communication de 2000<sup>33</sup>. Cette communication présente les premières actions dans ce domaine : lancement d'un financement public visant à soutenir la recherche et le développement dans le domaine des technologies de sécurité, rapprochement des législations nationales en matière pénale destinées à réprimer la criminalité utilisant de hautes technologies et enfin instauration d'un forum de l'UE (Forum européen sur la cybersécurité et la cybercriminalité<sup>34</sup>).

Toujours dans cette communication de 2001, la Commission estime qu'il importe d'aller plus loin. Elle observe un décalage entre le caractère urgent de l'action à mener, et la lenteur des progrès effectués, liée notamment à la structure décentralisée d'Internet. Répondant à ce souhait d'une action renforcée, le Conseil européen de Stockholm des 23 et 24 mars 2001 demande à la Commission, ainsi qu'au Conseil, de mettre en place une stratégie dans ce domaine<sup>35</sup>. Pour la première fois, l'idée d'un plan spécifique consacré à la sécurité des réseaux est évoquée.

En réponse à cette demande, la Commission propose, dans une autre communication, publiée quant à elle le 6 juin 2001<sup>36</sup>, une série de mesures comme une meilleure organisation des actions des équipes d'intervention en cas d'urgence informatique, les CSIRT (*Computer Emergency Response Teams* ou *Computer Security and Incident Response Team*). En particulier, elle suggère de renforcer les compétences des CSIRT existantes<sup>37</sup>, notamment les cyberattaques, et de les mettre en réseau avec celles du monde entier. De son côté, le Conseil approuve deux résolutions, l'une le 28 janvier 2002<sup>38</sup>, et l'autre le 18 février 2003<sup>39</sup>, lançant plusieurs pistes, comme la mise en place d'un groupe de travail sur la cybersécurité ou l'étude de formes de collaboration entre États membres concernant l'échange d'informations dans ce domaine.

En parallèle, une agence est mise en place afin de renforcer la sécurité des réseaux. Le Conseil adopte à ce sujet une décision le 17 novembre 2003 établissant un programme financier, le programme Monidis<sup>40</sup>. Celui-ci vise notamment à concourir à l'instauration de l'ENISA<sup>41</sup>. Cette agence, située à Heraklion, est fondée sur un règlement du Conseil et du Parlement européen du 10 mars 2004<sup>42</sup>. Opérationnelle depuis le 14 mars 2004, elle constitue un centre d'expertise ayant pour tâche de rassembler les informations sur les risques actuels et émergents relatifs à la sécurité des réseaux, de les analyser et de les diffuser<sup>43</sup>. Le règlement l'instituant mentionne à titre liminaire que les réseaux de communication et les systèmes d'information sont devenus un facteur clé

(32) Point 3.7 de la communication de la Commission du 13 mars 2001 intitulée « eEurope 2002 : Impacts et priorités », communication en vue du Conseil européen de Stockholm, 23-24 mars 2001 » (COM(2001)140).

(33) Communication de la Commission intitulée « Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité » (COM(2001)140).

(34) Il s'agit d'une plate-forme destinée à rassembler des acteurs du secteur public (services de police, autorités chargées de la protection des données), et du secteur privé, qu'ils soient issus du monde de l'entreprise (fournisseurs de services internet, entreprises de télécommunications) ou du milieu associatif (organisations de défense des libertés publiques, associations de consommateurs). Ce forum de l'UE vise à promouvoir le dialogue entre eux, de même que la sensibilisation du public face aux risques sur Internet.

(35) § 36 des conclusions du 24 mars 2001 indiquant que « le Conseil, en concertation avec la Commission, mettra au point une vaste stratégie en matière de sécurité des réseaux électroniques, prévoyant des mesures de mise en œuvre pratique. Cette stratégie devrait être prête à temps pour le Conseil européen de Göteborg ».

(36) Communication de la Commission du 6 juin 2001 sur la sécurité des réseaux et de l'information : proposition pour une approche politique européenne (COM(2001)298).

(37) Qui sont des structures permanentes destinées à centraliser et à résoudre les incidents informatiques, et plus généralement à gérer les risques pour la sécurité des réseaux. Celles-ci ont notamment pour mission d'assurer l'analyse des risques et incidents, l'activation du mécanisme d'alerte précoce et la diffusion de messages d'alerte en cas d'incident, l'intervention et le suivi.

(38) Résolution du Conseil du 28 janvier 2002 relative à une « approche commune et à des actions spécifiques dans le domaine de la sécurité des réseaux et de l'information » (JOUE C 43 du 16.2.2002, p. 2).

(39) Résolution du Conseil du 18 février 2003 relative à « une approche européenne axée sur une culture de la sécurité des réseaux et de l'information » (JOUE C 48 du 28.2.2003, p. 1).

(40) Décision n° 2256/2003/CE du Parlement européen et du Conseil du 17 novembre 2003 relative à l'adoption d'un programme pluriannuel (2003-2005) portant sur le suivi du plan d'action eEurope 2005, la diffusion des bonnes pratiques et l'amélioration de la sécurité des réseaux et de l'information (Modinis) (JOUE L 336 du 23.12.2003, p. 1).

(41) Art. 1.d de la décision.

(42) Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JOUE L 77 du 13.3.2004, p. 1).

(43) Degryse (C.), 2007, *Dictionnaire de l'Union européenne*, Bruxelles, De Boeck/Larcier, 3<sup>e</sup> éd., p. 23.

du développement de l'économie et de la société. Leur sécurité est donc un élément indispensable à l'essor de la société numérique. Quant aux violations à la sécurité, elles portent atteinte à la confiance des opérateurs. Il importe dès lors, à travers les mesures prises, de restaurer cette confiance jugée indispensable et cette agence nouvellement créée est un moyen d'y parvenir.

Cela étant, les mesures prises au cours de cette période posent les jalons d'une politique européenne en matière de cybersécurité qui s'esquisse, à savoir un document de programmation, une enveloppe financière et le développement de capacités propres à l'Union. À ce stade, cette politique demeure embryonnaire, ne serait-ce que par les moyens limités dont dispose l'agence. Il n'empêche, ces trois éléments – la stratégie en 2001, l'établissement d'un programme financier en 2003 et la création en 2004 de cette agence européenne spécifique, l'ENISA –, constituent une ébauche de ce qui va être une politique européenne en matière de cybersécurité. La protection des « infrastructures critiques » va, quant à elle, constituer un environnement placentaire au sein duquel celle-ci va se développer.

## La gestation : des programmes « CBRN » à la protection des « infrastructures d'information critiques »

Le processus de gestation de la politique européenne en matière de cybersécurité va s'opérer dans le cadre des efforts menés par l'Union européenne en matière de protection des infrastructures critiques. Pour comprendre ce processus, il importe de revenir sur les programmes dits « CBRN » (chimique-radiologique-biologique-nucléaire), puisque ceux-ci vont favoriser la mise en place, au niveau européen, d'un processus de protection des infrastructures critiques. Par effet de cascade, les travaux en matière CBRN vont déboucher sur ce processus de protection des infrastructures critiques, qui lui-même va amener l'Union à s'intéresser à la protection des « infrastructures d'information critiques ».

## Des programmes dits « CBRN » à la protection des « infrastructures critiques »

Les prémisses d'une politique européenne en matière de cybersécurité correspondent au besoin, à l'échelle de l'Union, d'une protection des infrastructures critiques. La sécurité des réseaux tend à être appréhendée de plus en plus sous l'angle de la protection des infrastructures critiques<sup>44</sup>. En effet, les processus d'uniformisation et d'interdépendance des systèmes les rendent vulnérables aux attaques. La lutte antiterroriste ne constitue pas le moteur de ce processus. Elle se trouve plutôt en toile de fond de la dynamique générée, en impulsant indirectement cette politique européenne en matière de cybersécurité, à travers les efforts menés en matière de protection des infrastructures critiques qui ont englobé, à la fin des années 2000, les infrastructures d'information critiques.



À cet égard, aucun des attentats, qu'il s'agisse de ceux de New York de 2001, ou de ceux de Madrid de 2004 et de Londres de 2005, n'a véritablement mis en évidence la thématique de la menace terroriste comme risque pour la sécurité des réseaux. En effet, ni les conclusions de Conseil du 21 décembre 2001, ni la stratégie antiterroriste de décembre 2005<sup>45</sup>, qui constituent les deux documents directeurs de l'action de l'Union, n'évoquent une telle thématique. Néanmoins, le silence des textes, n'implique pas le désintérêt de l'Union pour ce sujet. La sécurité des réseaux et de la protection des systèmes d'information, qui va déboucher sur la création d'une politique européenne en matière de cybersécurité, se déroule de manière indirecte, par le truchement de la protection des infrastructures critiques.

Les conclusions du Conseil européen des 17 et 18 juin 2004 approuvées dans la foulée des attaques de Madrid entament la jonction entre ces deux sujets, terrorisme d'un côté, sécurité des réseaux de l'autre, à travers la question de la protection des infrastructures critiques. Elles précisent que « le Conseil et la Commission sont invités à évaluer les moyens dont disposent les États membres tant pour prévenir les attentats terroristes de tous types que pour faire face à leurs conséquences, à recenser les meilleures pratiques et à proposer les mesures nécessaires. [...] D'ici à la fin de l'année, le Conseil est invité à préparer, sur la base d'une approche coordonnée du secrétaire général/haut représentant et de la Commission, une stratégie globale visant à renforcer la protection des infrastructures critiques<sup>46</sup> ».

(44) Voir à ce sujet : Jeanson (É.), 2013, « La cybersécurité des infrastructures vitales : un enjeu de sécurité nationale », *Revue de la gendarmerie nationale*, n° 248, 4<sup>e</sup> trimestre, p. 79-84.

(45) Doc. du Conseil du 30 décembre 2005, n° 14469/4/05.

(46) Point 17 des conclusions du Conseil européen (doc. du Conseil du 18 juin 2004, n° 10679/1/04, CONCL 2).


 LE PROCESSUS DE GESTATION DE LA POLITIQUE EUROPÉENNE EN MATIÈRE DE CYBERSÉCURITÉ VA S'OPÉRER DANS LE CADRE DES EFFORTS MENÉS PAR L'UNION EUROPÉENNE EN MATIÈRE DE PROTECTION DES INFRASTRUCTURES CRITIQUES. POUR COMPRENDRE CE PROCESSUS, IL IMPORTE DE REVENIR SUR LES PROGRAMMES DITS « CBRN » (CHIMIQUE-RADIOLOGIQUE-BIOLOGIQUE-NUCLÉAIRE), PUISQUE CEUX-CI VONT FAVORISER LA MISE EN PLACE, AU NIVEAU EUROPÉEN, D'UN PROCESSUS DE PROTECTION DES INFRASTRUCTURES CRITIQUES. PAR EFFET DE CASCADE, LES TRAVAUX EN MATIÈRE CBRN VONT DÉBOUCHER SUR CE PROCESSUS DE PROTECTION DES INFRASTRUCTURES CRITIQUES, QUI LUI-MÊME VA AMENER L'UNION À S'INTÉRESSER À LA PROTECTION DES « INFRASTRUCTURES D'INFORMATION CRITIQUES »
 

Répondant aux invitations du Conseil européen, la Commission a présenté une stratégie globale visant à renforcer la protection des infrastructures critiques. Avant d'aller plus avant et de décrire cette stratégie globale, il importe de revenir un instant sur le substrat ayant favorisé l'émergence de l'action de l'Union dans le domaine de la protection des infrastructures critiques. Il s'agit en l'occurrence des programmes « CBRN ». Sur demande du Conseil européen de Gand du 19 octobre 2001, la Commission a présenté, le 28 novembre 2001, une communication dressant le panorama des capacités de réaction de l'Union en cas d'attaque terroriste<sup>47</sup>. Sur le fondement des éléments figurant dans cette communication, le Conseil a adopté, le 20 décembre 2002, le premier programme CBRN qui est mis à jour à la fin de l'année de 2004 au regard des conclusions du Conseil des 17 et 18 juin 2004. Ce programme de 2004,

dit « programme CBRN révisé/élargi » a pour objectif « d'accroître l'efficacité des mesures prises au niveau des pays et de l'UE en vue de prévenir et de limiter les conséquences des menaces et des attentats terroristes [en particulier concernant] les infrastructures critiques<sup>48</sup> ». Constatant que la protection des infrastructures vitales relève des États membres au premier chef, il met en avant le respect du principe de subsidiarité énoncé dans le droit primaire, pour confier à la Commission le soin de procéder à l'évaluation des risques et à la mise au point de techniques de protection concernant la protection des infrastructures critiques de nature transnationales. Appelé de ses vœux, le programme européen de protection des infrastructures critiques (EPCIP) présenté par la Commission entend promouvoir une série de mesures organisationnelles horizontales nécessitant une coopération, une coordination, voire une harmonisation des législations nationales dans ce domaine. Sur la base d'un *Livre vert* publié le 17 novembre 2005<sup>49</sup>, et des conclusions du 2 décembre 2005<sup>50</sup>, ce programme, inséré dans une communication de la Commission du 12 décembre 2006, est destiné à créer un cadre communautaire pour la protection des infrastructures critiques<sup>51</sup>. Le principe central énoncé dans ce programme est l'approche multirisque. Même si la menace terroriste est jugée prioritaire, le dispositif de protection des infrastructures critiques entend faire face à différents types de risques, terroriste ou non. En effet, le critère porte avant tout sur le degré de vulnérabilité de ces infrastructures et sur le risque de perturbation de l'économie européenne avec, pour conséquence, une réduction de la compétitivité de l'UE à l'échelle mondiale. Le programme dissocie à cet effet les infrastructures critiques européennes (ICE) des infrastructures critiques nationales (ICN). Concernant ces dernières, l'Union fournit un soutien aux États membres sur leur demande. Le principe est que, conformément à ce principe de subsidiarité, la responsabilité de la protection des infrastructures critiques nationales relève de leurs propriétaires/exploitants et des États membres. Quant aux infrastructures critiques européennes, une procédure commune est menée afin de procéder à leur recensement. Une directive datant de 2008 a été adoptée visant à identifier les ICE et à soumettre celles-ci à un régime commun d'évaluation<sup>52</sup>. Le texte définit une infrastructure critique comme « un point, système ou partie de celui-ci, situé dans les États membres, qui est indispensable au

(47) Communication de la Commission au Conseil et au Parlement européen, du 28 novembre 2001, Protection civile - État d'alerte préventive contre les urgences éventuelles (COM (2001)707).

(48) Point 13 du doc. du Conseil du 18 novembre 2004, n° 4813/04.

(49) Livre vert sur un programme européen de protection des infrastructures critiques (COM(2005)576).

(50) Conclusions du Conseil du 2 décembre 2005 relatives à la prévention, la préparation et la réaction en cas d'attentats terroristes (doc. du Conseil n° 14390/05 (presse 296)).

(51) COM (2006)786.

(52) Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JOUE L 345 du 23.12.2008, p. 75).



*maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif dans un État membre du fait de la défaillance de ces fonctions* » et une ICE comme « *une infrastructure critique située dans les États membres dont l'arrêt ou la destruction aurait un impact considérable sur deux États membres au moins. L'importance de cet impact est évaluée en termes de critères intersectoriels. Cela inclut les effets résultant des dépendances intersectorielles par rapport à d'autres types d'infrastructures* ». L'annexe I ne mentionne pas la sécurité des réseaux. Cette omission est volontaire dans la mesure où il est indiqué explicitement que ce texte devra être réexaminé en vue d'inclure le cas échéant d'autres secteurs dans son champ d'application, en particulier le secteur des technologies de l'information et de la communication (TIC). Un nouveau texte est présenté rapidement en ce sens, puisqu'une communication du 30 mars 2009 entend remédier à la lacune identifiée dans cette directive de 2008.

### **De la protection des « infrastructures critiques » à la protection des « infrastructures d'information critiques »**

L'inclusion des systèmes d'information dans le champ de la protection des « infrastructures critiques » résulte des incidents rencontrés au milieu des années 2000. Deux événements marquants conduisent l'Union à favoriser la protection des « infrastructures d'information critiques ». Il s'agit des cyberattaques majeures rencontrées en 2007 par l'Estonie et de la perturbation des communications en 2008, par la rupture en Méditerranée de trois câbles sous-marins transcontinentaux. Cette communication du 30 mars 2009 entend dès lors assurer la sécurité d'infrastructures d'information dont la perturbation ou la destruction aurait des incidences considérables sur le

fonctionnement de l'économie et de la vie sociale. La communication part d'un double constat : le secteur des TIC est présent dans l'ensemble des segments de la société. Elle favorise la croissance économique et elle constitue un moteur de l'innovation en favorisant des gains de productivité. En parallèle, les cyberattaques ont atteint un degré de complexité sans précédent. Or, citant le Forum économique mondial, elle souligne qu'une défaillance des TIC aurait un coût de 250 milliards de dollars, tandis que la probabilité d'une défaillance grave au cours des dix prochaines années est estimée à 10 à 20 %. Face à la gravité du danger, ce texte de 2009 présente une série de mesures dans le domaine de prévention, de la préparation, de la résilience et de la sensibilisation.

Il est vrai que les efforts institutionnels menés trouvent leurs racines dans une communication de 2001 consacrée à la sécurité des infrastructures de l'information<sup>53</sup>. À l'époque, les mesures préconisées se cantonnaient à la sécurisation des éléments essentiels de l'infrastructure grâce, notamment, au développement de protocoles de sécurité, à la sécurisation des environnements à l'aide de logiciels antivirus et des systèmes de cryptage, ou encore des procédés d'authentification des utilisateurs autorisés. Néanmoins, l'idée d'une approche qui ne soit pas juste réactive était amorcée avec une logique préventive du risque (c'est-à-dire la prise en compte de la sécurité au moment de la conception des systèmes).

Quant à la communication du 30 mars 2009, elle va bien plus loin en envisageant un modèle européen de gouvernance pour les infrastructures d'information critiques<sup>54</sup>. Parmi les mesures se trouvant dans le plan d'action, figurent la définition commune de normes minimales pour la mise en place de CERT nationales et l'établissement du partenariat public privé européen pour la résilience (EP3R<sup>55</sup>). Il s'agit d'améliorer le

(53) Communication de la Commission du 26 janvier 2001 intitulée « Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité - eEurope 2002 » (COM(2000)890).

(54) Communication de la Commission relative à la protection des infrastructures d'information critiques - « Protéger l'Europe des cyberattaques et des perturbations de grande envergure : améliorer l'état de préparation, la sécurité et la résilience » (COM(2009)149).

(55) La communication du 31 mars 2011 relative à la protection des infrastructures d'information critiques indique que l'EP3R a pour mission « d'encourager la coopération entre le secteur public et le secteur privé sur des questions stratégiques de politique de l'UE en matière de sécurité et de résilience. L'ENISA a fait office de facilitateur pour les activités de l'EP3R et, conformément à la proposition de la Commission de 2010 relative à la modernisation de l'ENISA, elle fournira un cadre durable à long terme pour l'EP3R. L'EP3R constituera aussi une plateforme de portée mondiale pour les questions relatives à la politique publique, à l'économie et aux marchés à examiner sous l'angle de la sécurité et de la résilience, notamment pour renforcer la gestion mondiale des risques dans le domaine des infrastructures [relatives aux technologies de l'information et de la communication] » [communication de la Commission du 31 mars 2011 relative à la protection des infrastructures d'information critiques : « Réalisations et prochaines étapes : vers une cybersécurité mondiale » (COM(2011)163), p. 5]. Elle ajoute que « ses futures activités continueront à bénéficier du soutien de l'ENISA et porteront sur la coopération entre les équipes d'intervention en cas d'urgence informatique (CERT) nationales/gouvernementales, la définition de mesures incitatives, de nature économique et réglementaire, en faveur de la sécurité et de la résilience (dans le respect des règles applicables dans le domaine de la concurrence et des aides d'État), l'évaluation de la situation de la cybersécurité en Europe, l'organisation d'exercices paneuropéens ainsi que l'examen des priorités à aborder dans un cadre international en matière de sécurité et de résilience » (idem, p. 5-6).

Concrètement, l'EP3R, dont l'ENISA assure le secrétariat, a pour objectif de fournir un ensemble d'éléments concernant, notamment, les besoins minimums pour la résilience des infrastructures critiques, ou la coopération en cas de panne des systèmes à large échelle.

dialogue entre le secteur public et le secteur privé, de fournir une plate-forme d'échange d'informations et de bonnes pratiques, de discussions des priorités politiques et d'identification des lignes directrices en matière de sécurité et de résilience<sup>56</sup>. La résilience, ou récupération, correspond, à cet égard, à la capacité pour un système d'absorber un choc et de retrouver rapidement son état antérieur<sup>57</sup>.

Sont mentionnés également dans la communication de 2009, l'idée d'une planification en situation d'urgence et l'accomplissement d'exercices à l'échelon national en cas d'incident de grande envergure affectant la sécurité des réseaux. La Commission apporte son soutien financier aux exercices paneuropéens. Or, « *qui dit plans d'urgence dit exercices afin de tester ceux-ci*<sup>58</sup> ». À ce sujet, le premier exercice paneuropéen intitulé « Cyber Europe 2010 » se tient le 4 novembre 2010<sup>59</sup>. Cet exercice, qui a été lancé en avril 2009 suite à la conférence ministérielle de Tallinn, est régulièrement renouvelé, le but étant d'évaluer l'état de préparation et la capacité de résilience des systèmes d'information face à une série d'incidents.

Enfin, le plan d'action figurant dans la communication de 2009 prévoit la création d'un système européen de partage d'information et d'alerte (SEPIA). Il s'agit de mettre en place un dispositif européen de partage d'informations et d'alerte destiné au grand public (citoyens et PME). Le SEPIA est opérationnel en 2012 et il repose sur le réseau de CERT nationales<sup>60</sup>. Ce plan d'action est suivi par la publication d'une communication du 31 mars 2011, dans laquelle la Commission récapitule les résultats obtenus. En

outre, elle décrit les prochaines étapes prévues au niveau européen pour chaque action, comme l'établissement d'un plan d'urgence européen en cas d'incident informatique, l'organisation d'exercices paneuropéens réguliers, ainsi que la création de partenariats stratégiques, avec, notamment, des exercices et des mesures de coopération entre les CERT des États membres en collaboration avec les CERT de certains pays tiers<sup>61</sup>.

Là encore, les événements conduisent l'Union à prendre de nouvelles mesures en faveur de la protection des infrastructures d'information critiques. Il s'agit en l'occurrence de la propagation du ver informatique stuxnet. Destiné à s'attaquer aux centrifugeuses iraniennes, ce logiciel malveillant, capable de saboter des systèmes industriels, a infecté en 2010, plusieurs infrastructures critiques dans le monde. Cette communication du 31 mars 2011 reprend et approfondit la démarche de la sécurisation des réseaux sous l'angle de la protection de ce type d'infrastructures. En les classant sous l'angle de la finalité et non sous leur nature, elle distingue les menaces exploitant les réseaux, telles que l'espionnage économique ou le vol d'identité, les menaces perturbant les réseaux comme les attaques au moyen d'ordinateurs zombies et enfin, les menaces ayant pour finalité la destruction de ces réseaux<sup>62</sup>. Ce peut être le cas du cyberterrorisme<sup>63</sup>.

En écho à cette communication, le Conseil approuve des conclusions le 27 mai 2011 dans lesquelles il déclare que la protection durable des infrastructures d'information critiques européennes revêt une importance stratégique. C'est pourquoi il insiste sur un approfondissement de la

(56) Irion (K.), 2012, «The governance of network and information security in the European Public-Private Partnership for Resilience (EP3ER)», in Krüger (J.), Bertram (N.), Gaycken (S.) (dir.), *The secure information society: Ethical, legal and political challenges*, New York, Springer, p. 97-98.

Sur la question plus générale du partenariat public-privé en matière de protection des infrastructures critiques, voir Andresson (J.J.), Malm (A.), 2006, «public-private partnership and the challenge of critical infrastructure protection», in Dunn (M.), Mauer (V.) (dir.), *International CIIP handbook 2006*, vol. 2, Zurich, Center for Security Studies, p. 139-166.

(57) Brunner (E.), Giroux (J.), 2009, «Resilience: A tool for preparing and managing emergencies». Zurich, Center for Security Studies, CSS Analyses in Security Policy, n° 60, p. 1.

Ce système peut en effet « rebondir » (*bounce back*) après un événement (Boin (A.), Smith (D.), 2006, «Terrorism and critical infrastructures: Implications for public-private crisis management», *Public money and management*, vol. 26, n° 5, novembre, p. 301). La résilience relève de l'idée que ce système peut maintenir une certaine stabilité en dépit de la variabilité de l'environnement (voir à ce sujet Hollnagel (E.), Pariès (J.), Woods (D. D.), Wreathall (J.) (dir.), 2011, *Resilience Engineering in Practice. A Guidebook*, Londres, Ashgate, coll. Ashgate Studies in Resilience Engineering).

(58) Lavaux (S.), 2010, « La politique européenne en matière de lutte contre le terrorisme CBRN », *Cahiers de droit européen*, vol. 46, n° 3-4, p. 366.

(59) Doc. du Conseil du 17 janvier 2011, n° 15893/1/10, p. 10. La communication précitée du 31 mars 2011 indique que la coopération européenne s'est développée de façon notable depuis 2009 et que les résultats obtenus sont encourageants, en particulier dans le cadre de l'exercice Cyber Europe 2010 (op. cit., p. 9).

(60) Communication de la Commission du 31 mars 2011 relative à la protection des infrastructures d'information critiques : « Réalisations et prochaines étapes : vers une cybersécurité mondiale » (COM (2011)163), p. 6.

(61) Liste complète p. 11 à 18 de la communication précitée du 31 mars 2011.

(62) Pour une description, voir Castets-Renard (C.), 2012, *Droit de l'internet : droit français et européen*, Paris, Montchrestien, p. 443.

(63) La Commission indique que « ce scénario ne s'est pas encore concrétisé mais, compte tenu de l'utilisation de plus en plus généralisée des [technologies de l'information et de la communication] dans les infrastructures critiques (réseaux électriques et systèmes d'alimentation en eau intelligents, par exemple), il ne peut pas être exclu à l'avenir » (p. 4 de la communication de 2011).

coopération entre les États membres en mettant au point des mécanismes de coopération entre les États membres en matière d'incidents informatiques, en élaborant des exercices à l'échelle paneuropéenne, et en améliorant le dialogue dans le domaine de la sécurité des réseaux. Quant à l'ENISA, l'agence est conviée à apporter un soutien aux États membres concernant le renforcement de leurs capacités respectives et l'amélioration de la coopération entre eux<sup>64</sup>. Enfin et surtout, ces conclusions du Conseil estiment qu'il est important de mettre en place, outre les équipes nationales d'intervention en cas d'urgence informatique, et les exercices nationaux dans le domaine de la cybersécurité, une stratégie nationale en matière de cybersécurité ainsi que des plans d'urgence nationaux en cas d'incident informatique. Ce faisant, le Conseil de l'Union entrevoit l'étape suivante, à savoir l'établissement d'une approche globale et cohérente en matière de cybersécurité. Qu'il s'agisse de la communication ou des conclusions, le terme de « cybersécurité » trouve désormais droit de cité.

## La mise au monde : la stratégie cybersécurité de 2013

La communication précitée de 2009, complétée par celle de 2011, reflète la prise de conscience de structurer l'action de l'Union pour faire face aux défis existant en matière de sécurité<sup>65</sup>. Elle ouvre la voie à l'élaboration d'une stratégie destinée à structurer l'intervention européenne dans ce domaine, en définissant les principes d'action et en organisant les rapports entre elle et les États membres.

Répondant à l'invitation du Parlement européen de présenter « une stratégie détaillée en matière de sécurité de

*l'internet pour l'Union* » qui prenne « comme point de référence principal les travaux réalisés dans le domaine de la protection des infrastructures d'information critiques et viser une approche globale et systématique de la cybersécurité », le haut représentant et la Commission européenne le 7 février 2013 présentent un texte qui vient prendre le relais du plan d'action de 2009<sup>66</sup>. Il permet à l'Union d'établir une action cohérente, à la fois en faisant la synthèse des actions réalisées précédemment, et en dressant les axes d'action à venir (même si le volet « cyberdéfense » est insuffisamment présent, ceci au motif que l'Union demeure un acteur mineur sur la défense<sup>67</sup>).

S'intitulant « un cyberspace ouvert, sûr et sécurisé », ce document s'apparente à une « stratégie parapluie<sup>68</sup> », au sens où il englobe des mesures de gestion de risque, des procédures destinées à faire face aux incidents, des moyens d'assurer une protection des infrastructures critiques et des méthodes pour améliorer la cyber-résilience. Il reflète la préoccupation de l'Union et des États membres pour cette question en présentant une vision globale de l'Union européenne dans ce domaine<sup>69</sup>, qui s'organise autour de cinq priorités<sup>70</sup>. Une telle stratégie, imprégnée de la logique de la gestion de risques, vise, d'une part, à détecter et réduire les vulnérabilités et, d'autre part, à anticiper la crise, à limiter son impact et à favoriser un retour à la normale. Elle consiste à prévenir la crise en vue de faire du cyberspace un espace sûr. Parmi les mesures prévues figurent l'identification par Europol des tendances émergentes en matière de cybercriminalité, le développement d'outils numériques en matière médico-légale, ainsi qu'une meilleure coopération entre l'ENISA, le Centre européen de lutte contre la cybercriminalité (EC3) d'Europol et l'Agence européenne de défense.

Toujours dans cette perspective de faire du cyberspace un espace sûr, la stratégie est accompagnée d'une proposition de directive présentée le même jour<sup>71</sup>. Cette dernière

(64) P. 3 du doc. du Conseil du 19 mai 2011, n° 10299/11, TELECOM 71, DATAPROTECT 55, JAI 332, PROCIV 66.

(65) Cammilleri (A.), *op. cit.*, p. 54.

(66) En ce sens, la stratégie fait écho à la volonté exprimée dans un rapport de Sénat de 2012 considérant que « l'Union européenne a un rôle important à jouer en matière de protection des systèmes d'information, car une grande partie des règles dans ce domaine relève de ses compétences. Or, l'Union européenne n'a pas encore pris réellement la mesure des enjeux liés à la protection des systèmes d'information. Avant toute chose, il semble indispensable que l'Union européenne se dote d'une véritable stratégie européenne qui englobe l'ensemble des questions liées au cyberspace » (Sénat, rapport d'information de J.-M. Bockel, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, n° 681, 18 juillet 2012, p. 113).

(67) Joubert (V.), Samaan (J.-L.), *op. cit.*, p. 271-272.

(68) Irion (K.), *op. cit.*, p. 92. : « concernant l'Union, l'EP3R constitue un ensemble organisationnel susceptible de fournir un cadre à une gouvernance à l'échelle européenne, destiné à améliorer la cybersécurité » (*idem*, p. 110) (nous traduisons).

(69) Communication conjointe de la Commission et du haut représentant du 7 février 2013 : « Stratégie de cybersécurité de l'Union européenne : un cyberspace ouvert, sûr et sécurisé » (JOIN (2013)1).

(70) À savoir, parvenir à la cyber-résilience, faire reculer la cybercriminalité, développer une politique et des moyens de cyberdéfense en liaison avec la politique de sécurité et de défense commune (PSDC), développer les ressources industrielles et technologiques en matière de cybersécurité, et instaurer une politique internationale de l'Union européenne cohérente en matière de cyberspace.

(71) Proposition de directive du 7 février 2013 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (COM(2013)48).

entend harmoniser, de par son caractère contraignant, le niveau de sécurité des réseaux et des infrastructures dans l'Union<sup>72</sup>. Formant le bras armé de la stratégie, cette directive dite « SRI » ou « NIS » (*Network and Information Security*), qui sera adoptée le 6 juillet 2016, instaure une série d'obligations à l'égard des États membres, parmi lesquelles celle de désigner des autorités nationales en matière de sécurité des réseaux, celle d'établir une « stratégie nationale en matière de sécurité des réseaux et des systèmes d'information » (SNCS) ou encore celle de doter les CSIRT en ressources suffisantes. Constatant que le nombre d'incidents ne cesse d'augmenter, la proposition suggère un ensemble de mesures parmi lesquelles l'adoption d'une stratégie nationale au regard du cadre fixé dans la directive. Un tel texte est de nature horizontale, au sens où il constitue la première législation de l'Union européenne qui s'efforce de répondre aux divers défis relatifs à la cybersécurité. S'efforçant de dépasser les cloisonnements sectoriels, il prévoit l'établissement d'un réseau rassemblant les services nationaux compétents et la Commission européenne, auquel participe l'ENISA, en matière de gestion de risques et d'incidents touchant les réseaux et systèmes informatiques. Surtout, la directive NIS se fonde sur le modèle de l'US-CERT préconisant une plus grande transparence de la part du secteur privé, en premier lieu concernant le signalement des incidents parmi les principaux acteurs économiques<sup>73</sup>. Il s'agit en effet pour ces acteurs économiques, en dépit de leur réticence à faire état de cyberattaques de nature à ternir leur image, de signaler aux autorités tout incident.

Dressant un premier bilan de la transposition de la directive SRI, la Commission juge celle-ci satisfaisant, quel que soit l'objectif, à savoir le renforcement des capacités nationales en matière de cybersécurité, la coopération menée à l'échelle de l'Union et la promotion d'une culture de la gestion des risques et du signalement des incidents<sup>74</sup>. Toutefois, elle suggère, dans ce rapport du 4 octobre 2017, d'étendre les obligations prévues

dans la directive à des domaines qui ne sont pas couverts. Concrètement, l'obligation de notification s'applique aux opérateurs de services essentiels (OSE). La Commission suggère d'inclure dans le champ de la directive certaines administrations publiques telles que le secteur postal, le secteur de la sécurité alimentaire, l'industrie chimique et nucléaire ainsi que la protection civile. Dans le même registre, elle envisage d'étendre les compétences des CSIRT au-delà des secteurs couverts par cette directive. En ce sens, la directive SRI apparaît comme un premier pas qui en appelle d'autres. Elle s'inscrit désormais dans le volet « cyber-résilience » de la nouvelle stratégie européenne en matière de cybersécurité.

## Conclusion

La stratégie de cybersécurité de 2013 promeut une vision globale et ce, au nom d'une sécurité devenue multisectorielle et multiniveaux. Elle s'inscrit dans la perspective d'une gouvernance et d'un processus de pilotage de la sécurité de l'information<sup>75</sup>. Cependant, il ne s'agit que d'une ébauche. La Stratégie nationale pour la sécurité du numérique de 2015 avait déclaré que « l'Europe, qui a adopté en 2013 une stratégie de cybersécurité, peine toutefois à oser une autonomie stratégique numérique et à se doter des outils nécessaires à un rééquilibrage du cyberspace en sa faveur<sup>76</sup> ». La stratégie de 2017 entend effectuer ce rééquilibrage, du moins, il s'agit d'un effort en ce sens. Présenté peu après les attaques des ransomware Wannycry et Petya, la nouvelle stratégie européenne en matière de cybersécurité met à jour le programme de 2013. Elle entend approfondir les efforts déployés en 2017 en remédiant aux imperfections constatées ■

(72) Quémener (M.), 2016, « La directive NIS, un texte majeur en matière de cybersécurité », *Sécurité et stratégie*, vol 23, n° 3, p. 52.

(73) Elle entend imposer aux opérateurs d'infrastructures critiques de signaler les incidents graves aux autorités nationales compétentes, ce que ne prévoit pas le programme européen de protection des infrastructures critiques (EPCIP). Il faut dire que les opérateurs de ces infrastructures ont tendance à minimiser les risques (Ranck (H.), Schmitt (B.), « Threat assesment », in Esterle (A.), Ranck (H.), Schmitt (B.) (dir.), *op. cit.*, p. 27).

(74) Commission européenne, communication du 4 octobre 2017 intitulée « Exploiter tout le potentiel de la directive SRI – Vers la mise en œuvre effective de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union » (COM(2017)476).

(75) Quémener (M.), 2016, « La directive NIS, un texte majeur en matière de cybersécurité », *Sécurité et stratégie*, vol 23, n° 3, p. 50.

(76) Premier ministre, *Stratégie nationale pour la sécurité du numérique*, 2015, p. 38.

# Intelligence artificielle et *Big Data* : du risque cyber à l'opportunité pour les services de sécurité et de défense étatiques

Amandine LÉVÊQUE

Le développement par certains États des technologies intelligentes amplifie les risques d'intrusion dans les systèmes informatiques et de manipulation de la population à grande échelle. Les défis : élever et homogénéiser le niveau de cybersécurité ; optimiser le processus de gestion des incidents ; renforcer les coopérations internationales pour la stabilité du cyberspace. À l'inverse, les solutions intelligentes sont porteuses d'opportunités pour les services de sécurité et de défense, tant au niveau opérationnel qu'administratif. Le manque de régulation visant l'usage de ces solutions conduit cependant à des situations d'atteinte aux libertés publiques et aux droits fondamentaux.

## Intelligence artificielle et *Big Data* : la difficile maîtrise du cyberspace

### La cybersécurité à l'épreuve de l'intelligence artificielle

### L'intensification des risques cyber

Il existe deux types de risques d'origine cybernétique : le *risque d'infiltration* des réseaux de communication à des fins d'espionnage, d'altération des données

ou de prise de contrôle et le *risque d'orientation* de l'opinion publique par le biais de campagnes d'influence sur internet<sup>1</sup>.

L'usage de l'IA intensifie le risque d'intrusion des systèmes informatiques en permettant aux cyberattaquants de frapper plus rapidement, avec plus d'efficacité et à moindre coût. D'abord, la technologie peut reconnaître des systèmes d'information ciblés et apprendre à les cartographier dans le but d'identifier les vulnérabilités et de pouvoir les exploiter<sup>2</sup>, ce qui réduit le temps habituellement long de l'attaque. Par exemple, les attaques par hameçonnage – via une boîte mail – deviendraient plus aisées grâce à la faculté de reconnaissance

### Amandine LÉVÊQUE



Amandine Léveque est actuellement en Master 2 Geopolitique, risques et Défense

à l'Institut Français de Geopolitique. Auparavant, elle a obtenu un Master 2 Management du Risque à l'Université Paris-Nanterre au cours duquel elle a rédigé un mémoire sur le thème « Intelligence artificielle et Big data : du risque cyber à l'opportunité pour les services de sécurité et de défense étatiques ».

(1) Vie-publique, 2019, « Cybersécurité : quelles réponses aux menaces nouvelles ? ».

(2) Baraer (F.), 2018, « Cybersécurité : comment l'intelligence artificielle peut se retourner contre vous », *Journaldunet*.



de messages habituels par la machine, puis de pièges envoyés aux utilisateurs<sup>3</sup>. Ensuite, l'interconnectivité croissante de ces systèmes intelligents est susceptible d'entraîner la propagation du virus à l'ensemble du système informatique. Enfin, les ressources engagées pour une cyberguerre sont bien moindres comparées aux moyens conventionnels nécessaires à une guerre ouverte. Pourtant, des cyberattaques peuvent engendrer des dégâts similaires. Rappelons-le, les cyberattaques augmentées par les capacités de l'IA ne sont l'apanage que de quelques États ou potentiellement d'*hacktivists* soutenus par ceux-ci.

Les systèmes d'IA peuvent également être détournés. Un cyberattaquant pourrait prendre le *contrôle* de systèmes d'IA embarqués, par exemple sur un drone. *Influencer* la machine pendant sa phase d'apprentissage ; une technique parvenue à dérouter « Tay » l'IA de Microsoft avec du contenu raciste sur Twitter<sup>4</sup>. Jouer sur le défaut de *perception* de la machine en provoquant une illusion d'optique au moyen d'un autocollant<sup>5</sup>. Les objets intelligents et

connectés ou encore les *Clouds* sont pris pour cible, car reliés à des sources importantes de données ; dont le potentiel stratégique n'est plus à démontrer. En effet, si elles apportent un avantage commercial considérable aux géants du Web, elles peuvent également donner un avantage économique ou encore militaire à l'État qui les possède. Il est donc impérativement nécessaire que la sécurité informatique soit pensée dès la phase de conception de ces systèmes<sup>6</sup>.

Enfin, l'utilisation de l'IA peut conduire à des campagnes de désinformation massives influençant la population. Sur les réseaux sociaux sont apparues les « *deep fakes* », ces vidéos déformant le discours de personnalités politiques, lesquelles vont agir sur une partie de la population et conduire à alimenter les thèses complotistes<sup>7</sup>. Les *social boats* ou encore les *trolls* sont utilisés pour orienter la population en amont d'un vote ou encore d'un soulèvement social. Les *social boats* ciblent des individus spécifiques et les influencent via du contenu auquel

(3) Chinaski (W.), 2018, « Intelligence artificielle : amie ou ennemie de la sécurité informatique ? », *Data analytics post*.

(4) Lecun (Y.), 2017, « Apprendre aux machines à penser : un défi majeur pour l'économie ? Un progrès pour l'humanité ? », *Défis*, n° 8, p. 13.

(5) Reynaud (M.), 2018, « Intelligence artificielle : un "game changer" en matière de cybersécurité », *observatoire fic*.

(6) Secrétariat général de la Défense et de la Sécurité nationale, 2018, *Revue stratégie de cybersécurité*, p. 100.

(7) Jeangène Vilmer (J.), Escorcía (A.), Guillaume (M.), Herrera (J.), 2018, *Les Manipulations de l'information : un défi pour nos démocraties*, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, p. 153.

ils sont susceptibles d'être sensibles ; un mécanisme utilisé par la société Cambridge Analytica pour servir la campagne présidentielle de Donald Trump en 2016. Pour cette même campagne, il apparaîtrait que le pouvoir russe se serait appuyé sur l'usage de *trolls* – des comptes fictifs particulièrement actifs en politique<sup>8</sup>.

### Protéger les systèmes informatiques et s'organiser face à la menace

La loi de programmation militaire de 2013 a imposé des mesures visant à élever le niveau de sécurité informatique des opérateurs d'importance vitale (OIV). L'Agence nationale de sécurité des systèmes d'information (ANSSI) est chargée d'y veiller en accompagnant les structures. Cependant, le niveau de sécurité informatique demeure inégal entre les secteurs d'activité pour des raisons matérielles et financières. Certaines règles de sécurité informatique ne sont pas appliquées, des failles sont donc exploitables par des cyberattaquants de faible niveau<sup>9</sup>. Les collectivités et de nombreuses entreprises échappent à ces mesures. Leur niveau de cybersécurité est souvent insuffisant alors qu'elles représentent des cibles de choix pour les cyberattaquants. À titre d'exemple, en 2017 le virus NotPetya s'est propagé en Ukraine, puis dans le reste du monde via un logiciel de comptabilité utilisé par de nombreuses entreprises<sup>10</sup>.

Plusieurs solutions renforcent le niveau de sécurité informatique. D'abord, la protection des systèmes d'information tout au long de leur cycle de vie avec un renouvellement permanent pour éviter leur obsolescence<sup>11</sup>. Ensuite, la mise en place d'un *Security Operation Center* (SOC) surveillant les systèmes d'information, alimenté par un *Security information and event management* (SIEM), lequel détecte les anomalies. Des États et de grandes entreprises se sont également dotés de *Computer Emergency Response Team* (CERT) pour répondre aux incidents. Les attaques étant de plus en plus sophistiquées, les solutions anti-virus ou pare-feux classiques sont désormais incapables de maintenir un seuil élevé de cybersécurité. En ce sens, des solutions cyber intelligentes visant à donner plus d'intelligence aux SIEM voient le jour<sup>12</sup>. Les sondes de détection de l'équipementier Thalès par exemple sont capables – grâce à la technologie

de l'IA – d'apprendre le comportement des utilisateurs et de détecter les incidents de *logging* ou des flux anormaux. Le système est également en mesure de traiter l'incident en plaçant en quarantaine un fichier infecté afin d'éviter la généralisation du problème à l'ensemble du système informatique<sup>13</sup>. Quelle que soit l'entité, un plan continuité activité (PCA) doit être pensé pour maintenir le système informatique suite à un incident.

En cas de survenance d'une cyberattaque visant les intérêts nationaux, le Centre interministériel de crise (CIC) est activé. Le plan Piranet prévoit que l'ANSSI pilote la Cellule de coordination cyber (CCC). L'ANSSI – concourant à la lutte informatique défense (LID) – procède également à l'analyse et au traitement des causes de l'incident ou de l'origine de l'attaque. En cas d'incident intervenant sur le périmètre du ministère des Armées, le Commandement de cyberdéfense (COMCYBER) remplit ce rôle en étroite collaboration avec l'ANSSI. Le COMCYBER contribue également à la lutte informatique offensive (LIO<sup>14</sup>). Les services de renseignement agissent contre l'ingérence étrangère et veillent au recueil de renseignement d'origine cyber. Différents services de la gendarmerie et de la police couvrent le périmètre de la cybercriminalité.

### Lutter contre la porosité d'un cyberspace

Le cyberspace ne possède pas de frontières. En cas de cyberattaque, l'interconnectivité croissante des systèmes peut engendrer des conséquences systémiques et toucher une partie du monde. Comment les États s'organisent-ils face à cette menace croissante ?

D'abord, le réseau des CERT européens a créé l'European government computer security incident response teams (EGC) afin de développer des moyens conjoints et plus performants de réponse aux incidents cyber de grande ampleur et de faciliter le partage d'informations. L'European network and information security Agency (ENISA) produit des réflexions sur les cyberattaques frappant l'Europe afin d'améliorer la capacité de réponse aux incidents cyber, l'échange d'informations entre les acteurs et l'établissement de partenariat public-privé.

(8) Longueueau (F.), 2018, « Les manipulations de l'information : analyse d'un rapport attendu », *Centre de Réflexion sur la guerre économique*.

(9) Secrétariat général de la Défense et de la Sécurité nationale, *op.cit.*, p.60-63.

(10) Espanol (I.), 2019, « L'Ukraine, cible préférée des hackers russes », *Le Monde*.

(11) Secrétariat général de la Défense et de la Sécurité nationale, 2018, *op.cit.*, p.33.

(12) Reynaud (M.), 2019, « Intelligence artificielle : un "game changer" en matière de cyberdéfense », *op.cit.*

(13) Leroy (P.), 2019, *Cyberattaques : détection et réaction*, Chaires Cyber Interarmées.

(14) Agence nationale de sécurité des systèmes d'information, « Le centre de cyberdéfense ».

Le *Livre blanc de la défense et de la sécurité nationale* juge indispensable de renforcer son efficacité et la coopération opérationnelle au sein de l'Union européenne (UE<sup>15</sup>). Il existe également un réseau international des CERT.

Ensuite, la Politique de sécurité et de défense commune (PDSC) tente de promouvoir une politique de cyberdéfense commune. Cependant, certains États concentrent davantage leurs forces au sein de l'Organisation de l'Atlantique nord (OTAN), laquelle développe sa capacité de cyberdéfense depuis longtemps<sup>16</sup>.

Enfin, les agences Europol, Euromed et Interpol favorisent l'échange d'informations concernant des activités cybercriminelles et facilitent les opérations des forces de l'ordre. Cependant l'échange d'informations reste compliqué, les États craignent que les informations transmises ne facilitent des opérations de cyberespionnage sur leurs propres systèmes<sup>17</sup>.

Les États doivent accroître les coopérations avec les acteurs privés notamment les géants du Web, lesquels possèdent une plus grande maîtrise du cyberspace. Suite à la tuerie de Christchurch diffusée en *live* sur les réseaux sociaux, des discussions étaient notamment en cours avec Facebook pour accélérer le processus de suppression des contenus violents<sup>18</sup>. Les opérateurs d'Internet sont également susceptibles de fournir un certain nombre de données sur des fraudes ou encore des cyberattaques, à l'image du partenariat entre Orange et Europol<sup>19</sup>.

## Encadrer l'usage du cyberspace

### Les options françaises en cas de cyberattaque visant les intérêts nationaux

En cas de survenance d'une cyberattaque visant les intérêts français, deux possibilités : la voie judiciaire ou la riposte.

La voie judiciaire vise essentiellement les *hackers* non affiliés à un État. La loi Godfrain a posé le cadre des poursuites contre les cyberattaquants, puis cinq lois sont

venues successivement alourdir les peines. Les atteintes aux systèmes informatisés de données sont désormais sanctionnées aux articles 323-1 à 323-7 du Code pénal. Cependant, la porosité du cyberspace rend difficile la recherche de la preuve, *de facto* les peines prononcées par les juges sont relativement légères. Toutefois, viser l'État, voler des données et agir en bande organisée constituent des circonstances aggravantes<sup>20</sup>.

Cela a été vu précédemment, l'usage de l'intelligence artificielle à des fins de déstabilisation n'est l'apanage que de certains États. Dès lors qu'un État vise les intérêts souverains en ingérant dans les affaires intérieures, l'État français se réserve le droit de riposter par des moyens diplomatiques ou des contre-mesures tels que l'y autorise l'article 2 alinéa 4 de la Charte des Nations unies. En cas d'agression armée – d'atteinte humaine, physique ou économique grave – la France se réserve le droit de se munir du principe de légitime défense afin de riposter par des moyens conventionnels ou cybers. Le principe de proportionnalité s'applique, cependant l'État français se fonde sur les conséquences de l'attaque et non les armes employées pour en apprécier. En temps de guerre, le droit international humanitaire s'applique aux cyberopérations venant en complément des moyens conventionnels. La technologie ne permettant pas, pour l'instant, que des cyber-opérations seules atteignent le même seuil de violence. Est considérée comme une attaque : toute action entraînant des conséquences physiques ou rendant inopérant les systèmes informatiques militaires (article 49 du PA I aux conventions de Genève<sup>21</sup>).

### L'échec de l'adoption de normes internationales contraignantes garantissant la stabilité du cyberspace

Il apparaît nécessaire de réguler l'usage du cyberspace afin d'éviter une escalade des tensions et l'apparition de cyberguerres. La Convention de Budapest lancée par le Conseil de l'Europe est le principal instrument de lutte contre la cybercriminalité. Elle tente de préserver la sécurité des réseaux informatiques face aux menaces cybers (accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système,

(15) Sénat, *Cyberdéfense : un nouvel enjeu de sécurité nationale*, Sénat.

(16) Mazzucchi (N.), 2018, « 2018, année charnière pour l'Europe dans le cyber ? », Fondation pour la recherche stratégique.

(17) Duarte de Jesus (C.), 2017, « Le cyberspace : quelle coopération au sein de l'Union Européenne », *eyes on europe*.

(18) Haski (P.), 2019, « La tuerie de christchurch en direct sur facebook : l'échec des géants numériques », [podcast], *France-inter*, géopolitique.

(19) Quemener (M.), 2018, « Pour une lutte plus efficace contre la cybercriminalité », *Sécurité globale*, vol. 15, n° 3, p. 15.

(20) Doutriaux (C.), 2019, « Cyberattaques : détection et réaction », *Chaires cyber interarmées*.

(21) Ministère des armées, 2019, *Droit international appliqué aux opérations dans le cyberspace*, ministère des Armées, p. 7-13.



falsification informatique, fraude informatique, etc.<sup>22</sup>). Ce traité, bien que lancé par le Conseil de l'Europe a une dimension internationale, mais souffre de l'absence de ratification par la Russie et la Chine ; des acteurs de premier plan dans le cyberspace. La Commission pour la prévention du crime et de la justice pénale a constitué un groupe d'experts gouvernementaux en 2011 afin d'adopter des normes internationales communes, cependant la majorité des États s'est exprimée en faveur de l'utilisation de la Convention de Budapest.

Depuis 2004 des groupes d'experts gouvernementaux de l'ONU sur la cybersécurité (GGE) se réunissent afin d'établir des principes communs régissant l'usage du cyberspace. Le groupe a reconnu l'applicabilité du droit international et notamment de la Charte des Nations unies aux activités menées dans le cyberspace et s'est entendu sur des principes communs non contraignants de bonne conduite. Lors du dernier GGE de 2017, aucun consensus n'a été trouvé pour réguler le cyberspace. En effet, les États possèdent des interprétations différentes du principe de légitime défense, des formes de menaces et des stratégies à adopter<sup>23</sup>. Il apparaît donc opportun de s'entendre au sein de groupes restreints comme l'Organisation de coopération de Shanghai (OCS) ou encore l'Association des Nations de l'Asie du sud-est (ASEAN).

## Allier sécurité, innovation et respect des droits et libertés

### L'IA au service des acteurs de la sécurité et de la défense

#### L'accroissement de l'efficacité des services

Ces solutions intelligentes vont agir à différents niveaux. D'abord, elles permettent d'*anticiper* afin de mieux gérer des incidents et les crises. Il s'agit des algorithmes ciblant des comportements suspects en sources ouvertes ; les algorithmes se basant sur les chiffres passés de la délinquance pour cibler des lieux à risques et les caméras intelligentes capables de détecter des comportements



IL APPARAÎT NÉCESSAIRE DE RÉGULER L'USAGE DU CYBERSPACE AFIN D'ÉVITER UNE ESCALADE DES TENSIONS ET L'APPARITION DE CYBERGUERRES. LA CONVENTION DE BUDAPEST LANCÉE PAR LE CONSEIL DE L'EUROPE EST LE PRINCIPAL INSTRUMENT DE LUTTE CONTRE LA CYBERCRIMINALITÉ. ELLE TENTE DE PRÉSERVER LA SÉCURITÉ DES RÉSEAUX INFORMATIQUES FACE AUX MENACES CYBER



violents<sup>24</sup>. Le but est de faciliter la prise de décision stratégique afin de déployer de la meilleure façon possible les forces opérationnelles.

Ensuite, des solutions intelligentes – grâce à leur puissance de calcul – permettent d'*accélérer* le cycle de renseignement ou encore de l'enquête en traitant un nombre d'informations considérables dans des bases de données. Par exemple, dans le cadre d'une affaire de pédopornographie, la technologie analyse toutes les images d'un disque dur en vue de trouver des images à caractère pédopornographique.

Enfin, l'IA porte *assistance* aux services de sécurité et de défense en opération avec des systèmes qui informent sur l'état du matériel<sup>25</sup> ou encore des robots capables d'aller chercher des soldats blessés. L'assistance concerne également les tâches administratives comme la retranscription d'un interrogatoire, ce qui entraînera à terme une refonte de l'organisation des services.

Cependant, la technologie possède ses limites. En effet, l'IA est dépourvue d'émotions, de conscience ou encore d'instinct, ce qui pourrait s'avérer dramatique sur le terrain<sup>26</sup>. C'est pourquoi, l'homme doit prendre la décision en dernier ressort. L'IA ne possède pas les capacités de perception humaine et peut facilement être trompée<sup>27</sup>. Enfin, la technologie est soumise aux erreurs de programmation humaines, lesquelles faussent les résultats de l'étude.

(22) Quemener (M.), 2018, « Pour une lutte plus efficace contre la cybercriminalité », *op.cit.*, p. 12

(23) *Sécurité et Défense magazine*, 2018 « La diplomatie du numérique ».

(24) Mines-paristech, « Police prédictive : étude d'une controverse ».

(25) Noël (J.), 2018, *Intelligence artificielle : vers une nouvelle révolution militaire*, Institut français des relations-internationales, p. 29.

(26) Devillers (L.), 2017, « L'empathie des robots », *Défis*, n° 8, p. 73.

(27) Nouyrgat (V.), 2018, « I.A : la faille inattendue », *Science & vie*.

## Conserver le principe d'autonomie stratégique

L'urgence post-attentat de 2015 avait conduit la Direction générale de la Sécurité intérieure (DGSI) à utiliser la technologie de la société américaine « Palantir », laquelle est en lien avec la Central intelligence agency (CIA) et le Président américain Donald Trump. À l'époque, cette technologie des plus puissantes au monde, capable de récolter un volume important de données et de les traiter au moyen de puissants algorithmes, ne trouvait pas son pareil en France.

Suite à l'émoi suscité par ces révélations, des industriels français se sont associés au sein du Groupement des industries de défense et de sécurité terrestres et aéroterrestres (GICAT) afin de proposer aux services de renseignement des solutions françaises capables de concurrencer Palantir<sup>28</sup>. De la même façon, la communauté du Renseignement s'est lancée à la recherche de solutions françaises innovantes, à l'image de la Direction du Renseignement militaire et de son *intelligence-campus*<sup>29</sup>. En effet, seul le développement de partenariats civilo-militaires et public-privé-recherches permettra de garantir l'autonomie stratégique de la France.

La coopération et les projets de recherche avec les partenaires européens est souhaitable pour concurrencer les géants américains, chinois ou encore israéliens.

## La difficile régulation de l'usage de l'IA

### Un cadre juridique national balbutiant

Les solutions intelligentes utilisées à des fins de sécurité intérieure sont susceptibles de nuire aux libertés publiques et aux droits fondamentaux. Par exemple, les codes sources des algorithmes d'IA peuvent se révéler discriminants et ne viser qu'une partie de la population<sup>30</sup>. Les caméras intelligentes peuvent entacher le droit à la vie privée ; la liberté de manifester et de s'exprimer dans les cas d'utilisation lors de rassemblements<sup>31</sup>. La mise en

service par la Chine du dispositif céleste – des milliers de caméras utilisées pour la reconnaissance faciale<sup>32</sup> – et le développement de *smart cities* pouvant servir à des fins de surveillance permanente de la population sont préoccupants<sup>33</sup>. D'autant que l'arsenal juridique est incomplet et crée parfois quelques exceptions.

Il n'existe aucune loi régissant la création des codes sources des algorithmes et les entreprises refusent d'être transparentes en la matière en invoquant le secret industriel. La CNIL n'a pas de droit de regard sur la création des codes sources. Le rapport sur l'intelligence artificielle du député de l'Essonne, Cédric Villani, propose donc d'adopter des principes de loyauté – l'algorithme est dévolu à une tâche précise – et de vigilance – le contrôle de la machine dont le travail peut évoluer en fonction des données qu'elle rencontre<sup>34</sup>.

En revanche, sous l'impulsion du Règlement général européen sur la protection des données (RGPD), le législateur français a modifié en mars 2018 la « loi caméras » du 21 mars 2007 afin d'y introduire la notion de « caméra de surveillance intelligente ». Celle-ci n'autorise que les caméras non reliées aux données personnelles des citoyens, ainsi que les caméras de reconnaissance de plaques d'immatriculation dans la mesure où le fichier contenant les données personnelles est conforme à la législation sur la vie privée<sup>35</sup>.

La loi informatique et libertés de 1978 confère plusieurs droits aux personnes dont les données sont collectées et des obligations à l'égard de ceux qui les collectent. Le règlement européen de 2012 qui instaure un droit à l'oubli sur Internet<sup>36</sup> a été complété par le Règlement général sur la protection des données (RGPD) instaurant notamment un droit à la portabilité des données et visant à mettre en place une réelle protection de l'utilisateur<sup>37</sup>.

Cependant, depuis les attentats de 2015 la législation évolue difficilement. Si la loi de renseignement de 2015 clarifie les activités des services de renseignement, il n'en reste pas moins qu'elle leur donne officiellement le droit de recueillir des données à caractère personnel

(28) Monin (J.), 2018, « Palantir : l'œil américain du renseignement français » [podcast], *France-inter*, « Secret d'info ».

(29) Lagneau (L.), 2018, « Face à l'inflation des données, la direction du Renseignement militaire mise sur l'intelligence artificielle », *opex 360*.

(30) Mines-paristech, « Police prédictive : étude d'une controverse », *op.cit.*

(31) Hérard (P.), 2018, « Surveillance : le réseau français intelligent d'identification par caméras arrive », *TV5 Monde*.

(32) Schaeffer (F.), 2018, « En Chine, 1,4 milliard de suspects sous surveillance », *Les échos*.

(33) *Influenca*, 2017, « Regard critique sur la smart-city ».

(34) Georges (B.), 2017, « Intelligence artificielle : faut-il une loi ? » [en ligne], *Les Échos*.

(35) Ibz Sécurité & prévention, 2018, « Modification de la législation sur les caméras : quels changements pour vous ? », *besafe*.

(36) *Tendance droit*, « Les enjeux juridiques du Big data », *Tendance droit*.

(37) Commission nationale de l'informatique et des libertés, 2018, « Règlement européen pour la protection des données : ce qui change pour les professionnels », CNIL.

grâce à des boîtes noires installées chez les fournisseurs d'Internet<sup>38</sup>. Le Premier ministre autorise les opérations de renseignement après avis de la Commission nationale du contrôle des techniques de renseignement (CNCTR) qui contrôle la durée de conservation des données et la légalité de la démarche<sup>39</sup>. La Commission informatique et libertés (CNIL) peut opérer un contrôle sur le mode de collecte des données, et s'informer sur la personne visée, en revanche elle ne sait ce qu'il advient de ces données par la suite et n'a aucun droit de regard sur leur contenu<sup>40</sup>.

### L'échec des négociations internationales sur la régulation de l'IA

Les solutions intelligentes peuvent nuire aux droits fondamentaux et aux libertés publiques des individus. À l'échelle des États, la puissance de cette technologie est susceptible d'entraîner l'escalade des tensions. Or, il est très difficile de réguler l'usage de l'IA sans porter atteinte à l'innovation. À l'échelle européenne et internationale, les États doivent-ils adopter des normes juridiquement contraignantes encadrant la conception et l'utilisation de l'IA ?

L'Europe aspire à devenir un *leader* en la matière, les instances ont donc opté pour l'adoption de principes éthiques communs régissant la création des IA tels que la sécurisation des algorithmes, le respect des droits de l'homme, etc.<sup>41</sup>.

Au niveau international, la norme ISO/IEC 23894 *Artificial intelligence – Risk management* devrait prochainement permettre de renforcer la sécurité des systèmes d'IA en



LES SOLUTIONS INTELLIGENTES PEUVENT NUIRE AUX DROITS FONDAMENTAUX ET AUX LIBERTÉS PUBLIQUES DES INDIVIDUS. À L'ÉCHELLE DES ÉTATS, LA PUISSANCE DE CETTE TECHNOLOGIE EST SUSCEPTIBLE D'ENTRAÎNER L'ESCALADE DES TENSIONS. OR, IL EST TRÈS DIFFICILE DE RÉGULER L'USAGE DE L'IA SANS PORTER ATTEINTE À L'INNOVATION. À L'ÉCHELLE EUROPÉENNE ET INTERNATIONALE, LES ÉTATS DOIVENT-ILS ADOPTER DES NORMES JURIDIQUEMENT CONTRAIGNANTES ENCADRANT LA CONCEPTION ET L'UTILISATION DE L'IA ?



analysant et en évaluant les risques qui en découlent. Pour ce qui est de la sécurité des objets, le groupe d'experts gouvernement (GGE) sur les systèmes d'armes létaux autonomes (SALA) n'est pas parvenu à l'adoption d'un accord juridiquement contraignant. Le groupe a adopté dix principes non contraignants dont le maintien de l'intervention de la responsabilité de l'homme dans le processus de décision propre à l'utilisation des systèmes d'armes<sup>42</sup>. Les États agissant pour leurs intérêts propres et ne souhaitant pas freiner l'innovation, les compromis sont difficiles à trouver ■

## Bibliographie

### Littérature grise

JEANGÈNE VILMER (J.), ESCORCIA (A.), GUILLAUME (M.), HERRERA (J.), 2018, *Les Manipulations de l'information : un défi pour nos démocraties* [en ligne], rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, <https://www.diplomatie.gouv.fr/>. Consulté le 19/08/19.

Ministère des Armées, 2019, *Droit international appliqué aux opérations dans le cyberspace* [en ligne], Ministère des Armées, <https://www.defense.gouv.fr/>, Consulté le 19/09/19.

NOËL (J.), 2018, *Intelligence artificielle : vers une nouvelle révolution militaire* [en ligne], Institut français des relations internationales, <https://www.ifri.org/>, Consulté le 05/06/19.

(38) Combiér (E.), 2015 « L'article à lire pour comprendre le projet de loi sur le renseignement », *Franceinfo*.

(39) Secrétariat général de la Défense et de la Sécurité nationale, *op.cit.*, p. 53.

(40) Cuny (D.), 2015, « Loi renseignement : la CNIL doit pouvoir contrôler les fichiers », *La Tribune*.

(41) Ravel d'Escalpon, (T. de), 2019, « Intelligence artificielle : nouvelle résolution du Parlement européen », *Dalloz actualité*.

(42) Garreau (M.), 2018, « Toujours pas d'accord international pour encadrer les robots tueurs », *L'Usine nouvelle*.

Secrétariat général de la Défense et de la Sécurité nationale, 2018, *Revue stratégie de cyberdéfense* [en ligne], SGDSN, <http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/>, Consulté le 03/02/19.

Sénat, *Cyberdéfense : un nouvel enjeu de sécurité nationale* [en ligne], Sénat, <https://www.senat.fr/rap/r07-449/r07-4495.html> Consulté le 16/07/19.

### Articles de périodiques

DEVILLERS (L.), 2017, « L'empathie des robots », *Défis*, n° 8, p. 73-77.

QUÉMÉNER (M.), 2018, « Pour une lutte plus efficace contre la cybercriminalité » [en ligne], *Sécurité globale*, vol. 15, n° 3, p. 5-16, <https://www.cairn.info/revue-securite-globale-2018-3-page-5.htm> Consulté le 05/06/19.

LECUN (Y.), 2017, « Apprendre aux machines à penser : un défi majeur pour l'économie ? Un progrès pour l'humanité ? », *Défis*, n° 8, p. 9-14.

### Articles de presse

BARAER (F.), 2018, « Cybersécurité : comment l'intelligence artificielle peut se retourner contre vous » [en ligne], *Journaldunet*, <https://www.journaldunet.com/solutions/expert/70239/cybersecurite--comment-l-intelligence-artificielle-peut-se-retourner-contre-vous.shtml> Consulté le 20/06/19.

comment-l-intelligence-artificielle-peut-se-retourner-contre-vous.shtml Consulté le 20/06/19.

CHINASKI (W.), 2018, « Intelligence artificielle : amie ou ennemie de la sécurité informatique ? » [En ligne], *Dataanalyticspost*, <https://dataanalyticspost.com/intelligence-artificielle-amie-ou-ennemie-de-la-securite-informatique/> Consulté le 08/07/19.

COMBIER (E.), 2015 « L'article à lire pour comprendre le projet de loi sur le renseignement » [en ligne], *Franceinfo*, [https://www.francetvinfo.fr/politique/loi-sur-le-renseignement/larticle-a-lire-pour-comprendre-le-projet-de-loi-sur-le-renseignement\\_875623.html](https://www.francetvinfo.fr/politique/loi-sur-le-renseignement/larticle-a-lire-pour-comprendre-le-projet-de-loi-sur-le-renseignement_875623.html) Consulté le 07/12/18.

CUNY (D.), 2015, « Loi renseignement : la CNIL doit pouvoir contrôler les fichiers » [en ligne], *La Tribune*, <https://www.latribune.fr/technos-medias/internet/loi-renseignement-la-cnil-doit-pouvoir-controller-les-fichiers-469523.html> Consulté le 23/11/18.

ESPANOL (I.), 2019, « L'Ukraine, cible préférée des hackers russes » [en ligne], *Le Monde*, [https://www.lemonde.fr/international/article/2019/04/04/l-ukraine-cible-preferee-des-hackers-russes\\_5445462\\_3210.html](https://www.lemonde.fr/international/article/2019/04/04/l-ukraine-cible-preferee-des-hackers-russes_5445462_3210.html) Consulté le 11/08/19.

GARREAU (M.), 2018, « Toujours pas d'accord international pour encadrer les robots tueurs » [en ligne], *L'Usine nouvelle*, <https://www.usinenouvelle.com/editorial/les-robots-tueurs-divisent-aux-nations-unies-les-associations-engagees-contre-se-mobilisent.N736794> Consulté le 02/08/19.

GEORGES (B.), 2017, « Intelligence artificielle : faut-il une loi ? » [en ligne], *Les Échos*, <https://www.lesechos.fr/2017/12/intelligence-artificielle-faut-il-une-loi-190154> Consulté le 06/06/19.

HÉRARD (P.), 2018, « Surveillance : le réseau français intelligent d'identification par caméras arrive » [en ligne], *TV5 Monde*, <https://information.tv5monde.com/info/surveillance-le-reseau-francais-intelligent-didentification-par-cameras-arrive-242520> consulté le 05/12/18.

NOUYRIGAT (V.), 2018, « I.A : la faille inattendue » [en ligne], *Science & vie*, <https://www.science-etvie.com/archives/i.a.-la-faille-inattendue-41754> Consulté le 20/07/19.

RAVEL D'ESCALPON (I. de), 2019, « Intelligence artificielle : nouvelle résolution du Parlement européen » [en ligne], *Dalloz actualité*, <https://www.dalloz-actualite.fr/flash/intelligence-artificielle-nouvelles-resolution-du-parlement-europeen>, Consulté le 02/08/19.

SCHAEFFER (F.), 2018, « En Chine, 1,4 milliard de suspects sous surveillance » [en ligne], *Les échos*, <https://www.lesechos.fr/2018/06/en-chine-14-milliard-de-suspects-sous-surveillance-991913>, Consulté le 03/12/18.

*Sécurité et Défense magazine*, 2018 « La diplomatie du numérique » [en ligne], *SD magazine*, <https://sd-magazine.com/securite-numerique-cybersecurite/la-diplomatie-du-numerique> Consulté le 01/08/19.

### Sites internet

Agence nationale de sécurité des systèmes d'information, « Le centre de cyberdéfense », ANSSI, <https://www.ssi.gouv.fr/agence/organisation/les-sous-directions/centre-operationnel-de-la-securite-des-systemes-d-information-rossi/le-centre-de-cyberdefense/> Consulté le 06/06/19.

Commission nationale de l'informatique et des libertés, 2018, « Règlement européen pour la protection des données : ce qui change pour les professionnels » [en ligne], CNIL. <https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels>, Consulté le 05/12/18.

DUARTE DE JESUS (C.), 2017, « Le cyberspace : quelle coopération au sein de l'Union européenne », [en ligne], *eyes on europe*, <https://eyes-oneurope.eu/cyberspace-cooperation-sein-de-lunion-europeenne/> Consulté le 03/09/19.

Ibz Sécurité & prévention, 2018, « Modification de la législation sur les caméras : quels changements pour vous ? » [en ligne], *besafe*, <https://www.besafe.be/fr/actualit%C3%A9s/modification-de-la-legislation-surles-cameras-quels-changements-pour-vous>, Consulté le 27/11/18.

Influenca, 2017, « Regard critique sur la smart-city » [en ligne], *Influenca*. [http://www.influenca.net/fr/actualites/media-com\\_etudes\\_regard-critique-sur-smart-city\\_7255.html](http://www.influenca.net/fr/actualites/media-com_etudes_regard-critique-sur-smart-city_7255.html), Consulté le 23/11/18.

LAGNEAU (L.), 2018, « Face à l'inflation des données, la direction du Renseignement militaire mise sur l'intelligence artificielle » [en ligne], *opex 360*, <http://www.opex360.com/2018/02/06/face-a-linflation-donnees-direction-renseignement-militaire-mise-lintelligence-artificielle/>, Consulté le 04/06/19

LONGUETEAU (F.), 2018, « Les manipulations de l'information : analyse d'un rapport attendu » [en ligne], Centre de réflexion sur la guerre économique, [https://infoguerre.fr/2018/10/manipulations-delinformation-analyse-dun-rapport-attendu/#\\_edn3](https://infoguerre.fr/2018/10/manipulations-delinformation-analyse-dun-rapport-attendu/#_edn3) Consulté le 16/08/19.

MAZZUCCHI (N.), 2018, « 2018, année charnière pour l'Europe dans le cyber ? » [en ligne], Fondation pour la recherche stratégique, <https://www.frstrategie.org/publications/notes/2018-annee-charnierepour-l-europe-dans-le-cyber-01-2018> Consulté le 28/07/19.

Mines-paristech, « Police prédictive : étude d'une controverse » [en ligne], *Mines-paristech*, [http://controverses.mines-paristech.fr/public/promo16/promo16\\_G16/www.controversesminesparistech-4.fr/\\_groupe16/index.html](http://controverses.mines-paristech.fr/public/promo16/promo16_G16/www.controversesminesparistech-4.fr/_groupe16/index.html), Consulté le 20/11/19.

REYNAUD (M.), 2018, « Intelligence artificielle : un "game changer" en matière de cyberdéfense » [en ligne], *observatoire fic*, <https://observatoire-fic.com/intelligence-artificielle-un-game-changer-en-matiere-de-cyberdefense/> Consulté le 05/04/19.

Tendance droit, « Les enjeux juridiques du Big data » [en ligne], *Tendance droit*.

<http://www.tendancedroit.fr/focus-sur-les-enjeux-juridiques-du-big-data/> Consulté le 05/12/18.

Vie-publique, 2019. « Cybersécurité : quelles réponses aux menaces nouvelles » [en ligne], *vie-publique*, <https://www.vie-publique.fr/actualite/dossier/cybersecurite/cybersecurite-queelles-reponses-auxmenaces-nouvelles.html> Consulté le 13/07/19.

### Autres

Chaires Cyber interarmées, 2019, *Cyberattaques : détection et réaction*, Chaires Cyber Interarmées.

HASKI (P.), 2019, « La tuerie de christchurch en direct sur Facebook : l'échec des géants numériques » [podcast], *France-inter*, géopolitique.

MONIN (J.), 2018, « Palantir : l'œil américain du renseignement français » [podcast], *France-inter*, « Secret d'info ».



© Samir Lebcher

## La causalité est morte : vive la corrélation !

*Vers une criminologie du lieu augmentée par l'intelligence artificielle*

Jean-Luc BESSON

### Jean-Luc BESSON



Chargé d'étude géostatistique à l'Observatoire national de la délinquance et des réponses pénales

(ONDRP). Il a auparavant été le directeur de la prévention, des relations police - justice, du service médiation sociale et directeur de la police municipale de la ville de Roubaix. Diplômé en journalisme, diplômé en victimologie (American University), formé en analyse criminelle et information géographique dans le cadre du *Crime Mapping & Analysis Center Program (CMAP)*, il est l'auteur de l'ouvrage *Les cartes du crime* (PUF 2005). Il développe un partenariat avec *Rutgers University Center on Public Security* sur les recherches de modélisation des lieux d'événements criminels et des études sur les lieux d'homicides à partir de données médico-légales. Il est membre de l'équipe de recherche de l'INHESJ sur le Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT).

L'intelligence artificielle (IA) est-elle la nouvelle ressource qui va permettre à la doctrine de sécurité publique de passer du stade de la réaction à celui de l'anticipation ? Pour Alain Bensoussan, avocat, spécialiste du droit des technologies avancées<sup>2</sup>, lorsque l'intelligence artificielle aura suffisamment appris pour réduire l'incertitude du résultat des algorithmes prédictifs de la criminalité à une quasi-certitude, les performances du policier ne seront plus jugées sur le nombre

d'interpellations ou d'affaires élucidées, mais sur le nombre de faits qu'il n'aura pas su éviter<sup>3</sup>. Car dans cet autre monde caractérisé par la perfection, une interpellation signifiera un échec. Un échec de la prédiction donc un échec du système et de ses agents. Le moindre crime ou délit sera considéré comme la révélation d'un biais, ou pire, d'une faute.

L'introduction de nouvelles technologies au sein de la police ne s'est pas seulement réduite à l'apport de nouveaux outils dans une panoplie déjà fournie. Elle a toujours modifié les doctrines de surveillance et de maintien de l'ordre [Kennedy, Caplan, Piza,

- (1) Cette image issue du réseau social Twitter, illustre la permanence géographique d'un phénomène délictuel pourtant bien identifié. Depuis au moins les années 1960, le secteur de la station de métro Barbès est un repère pour les trafics illégaux en tout genre, dont le trafic de cigarettes à la sauvette. « *Pluie, neige, contrôles de police à répétition, rien ne peut dissuader les buralistes du métro Barbès-Rochechouart de vendre leurs Marlboro. Il était temps d'officialiser leur profession* », revendique Omerta Project.
- (2) Alain Bensoussan dirige le cabinet Lexing Alain Bensoussan Avocats. Il a participé à l'élaboration de la loi de 1985 sur la protection du logiciel et se fait le chantre de la personnalité robot dans le droit [Bensoussan, 2019].
- (3) Intervention au pôle judiciaire de la Gendarmerie nationale, colloque organisé par l'Observatoire national des sciences et technologies de la sécurité (ONSTS) : intelligence artificielle et lutte contre la délinquance (février 2019).

2018]. Dans les années 1970, les patrouilles automobiles ont remplacé les patrouilles à pied, afin de créer une impression d'ubiquité. Aux États-Unis, la mise en place du 911 a priorisé une doctrine fondée sur les interventions rapides sur incident et la combinaison 911/patrouilles mécanisées/interventions rapides grâce à ces « nouvelles technologies » pour l'époque, a déterminé ce qu'est encore le *design* des services de police dans de nombreux cas [Mastrofski, Willis, 2011].

L'apparition de l'IA parmi les nouveaux outils des forces de l'ordre va probablement modifier fondamentalement une doctrine de sécurité publique toujours fondée sur l'intervention et donc la réactivité. La prévention/prédiction aura remplacé l'intervention/interpellation [Lum, Koper, Telep, 2011]. Dans cette ère gérée par l'intelligence artificielle, le policier contraint de courir après le voleur relèvera de la nostalgie.

S'il est vrai que les dernières années ont vu les progrès technologiques et l'IA commencer à s'introduire dans le quotidien de la sécurité, par exemple, les systèmes de surveillance et d'identification, ces outils sont encore globalement loin d'en être à un stade d'utilisation industrialisée. Mais il ne fait guère de doute qu'à terme, dans l'ensemble les acteurs de la prévention de la délinquance, la police, la justice, l'administration pénitentiaire, utiliseront massivement cette innovation dite « de rupture » [Christensen, Raynor, 2013] si, dans le contexte de raréfaction budgétaire, elle aboutit à des gains de sécurité en respectant le cadre établi des libertés fondamentales.

Ce qui incite à dégager cette perspective, c'est la capacité affichée de l'IA à réduire l'incertitude des décisions par un calcul probabiliste dont le résultat sera d'autant plus certain qu'il sera basé sur des quantités volumineuses de données (*Big Data*) et des analyses multicritère. Traduite à un échelon opérationnel, cette incertitude s'illustre par des questions simples telles que :

- où et quand dois-je positionner cette patrouille pour obtenir un résultat tangible contre les cambriolages ?
- dois-je décider d'éloigner ce conjoint en raison des risques de réitération de violences ? Sur quels critères ? Quel est son *scoring* de risque ?

– quelle priorité dois-je adresser à ce territoire pour cette semaine la nuit ?

– vais-je prendre la décision de refuser la visite à ce détenu en raison du profil de risque du visiteur ?

La complexité des décisions à prendre et leurs conséquences dans la vie de ceux à qui elles vont s'appliquer semblent plaider pour offrir une assistance technique aux décideurs. Sébastien Gallois<sup>4</sup> ne dit pas autre chose lorsqu'il évoque les 120 critères qui entrent en ligne avant de décider une interdiction d'approche dans le cadre d'un conjoint violent. Déjà en 2007, Anne Milgram, alors procureur général du New Jersey (USA), expliquait pourquoi les statistiques sont des éléments clés dans la lutte contre la criminalité. « *Lorsque j'étais assistante du procureur puis quand j'étais procureur général, je regardais les affaires en face de moi, et je prenais généralement des décisions fondées sur mon instinct et mon expérience* », disait-elle. Et elle ajoutait : « *Ce que j'ai appris très rapidement c'est que nous ne faisons pas du bon travail. Donc j'ai voulu faire les choses différemment. Je voulais introduire des données et des analyses, des analyses statistiques rigoureuses de notre travail. En clair, je voulais faire du Moneyball en justice pénale* » [Milgram, 2014].

## On ne regrettera pas le passé

Ce bouleversement n'est pas encore là. Mais il s'approche à grands pas, probablement aussi rapidement que la croissance de la puissance de calcul nécessaire à entrainer les algorithmes de l'IA<sup>5</sup>. Il n'est pour cela pas nécessaire d'être un *Précog*<sup>6</sup> pour anticiper qu'avec l'IA, l'approche actuelle de la lutte contre la criminalité basée sur un mélange d'analyses relativement sommaires du passé criminel d'un lieu, des auteurs connus qui s'y rapportent, d'influences contextuelles et d'expériences professionnelles personnelles, a sans doute vécu.

Certes on se méfie d'un futur où une IA surpuissante supplanterait les décisions humaines dans les domaines courants de la vie et aussi dans les champs de la police et de la justice. Le rapport Villani est très prudent en la matière [Villani *et al.*, 2018]. Des chercheurs les plus éminents ont lancé des initiatives destinées à mettre en garde la population contre une dérive des IA dans le cadre de la

(4) Sébastien Gallois, chef du service de l'expertise et de la modernisation au secrétariat général ministère de la Justice, colloque Sécurité et Justice, le défi de l'intelligence artificielle (INHESJ, novembre 2019).

(5) Selon OpenAI, la puissance de calcul a été multipliée par 300 000 en sept ans et actuellement elle double tous les 3,4 mois, in Futura Tech, Céline Deluzarche (novembre 2019).

(6) Les *Précogs* sont des êtres doués de précognition dans le film de Steven Spielberg *Minority Report*.



MESURÉE DEPUIS 1996 EN FRANCE  
MÉTROPOLITAINE PAR LES DIX INDICATEURS  
STATISTIQUES LES PLUS COURANTS DÉCRIVANT LES  
PRINCIPALES FAMILLES D'ATTEINTES  
ET D'INFRACTIONS, L'ÉVOLUTION DES CRIMES  
ET DÉLITS RENVOIE LE PLUS SOUVENT UNE  
IMAGE D'AGGRAVATION QUI DOIT INTERROGER  
CHACUN SUR LES DOCTRINES, MÉTHODOLOGIES,  
TECHNIQUES, STRATÉGIES UTILISÉES JUSQU'ALORS  
POUR LUTTER CONTRE LA DÉLINQUANCE  
ET LA CRIMINALITÉ.



mise en œuvre de systèmes d'armes létales autonomes (SALA) ou robots tueurs<sup>7</sup>. Mais on ne regrettera peut-être pas un passé marqué factuellement par une relative impuissance des politiques publiques à réduire l'insécurité. Mesurée depuis 1996<sup>8</sup> en France métropolitaine par les dix indicateurs statistiques les plus courants décrivant les principales familles d'atteintes et d'infractions, l'évolution des crimes et délits renvoie le plus souvent une image d'aggravation qui doit interroger chacun sur les doctrines, méthodologies, techniques, stratégies utilisées jusqu'alors pour lutter contre la délinquance et la criminalité.

Le nombre d'homicides intentionnels a baissé. Cette tendance se retrouve dans la plupart des études menées en France à partir de diverses sources<sup>9</sup>. En revanche les tentatives sont en hausse. Un paradoxe qui peut par hypothèse s'expliquer par la rapidité des interventions et l'accroissement de la qualité des soins d'urgence en matière de violences [Harris, 2002]. Un sujet d'étude.

Selon les statistiques policières, les coups et blessures, c'est-à-dire les violences interpersonnelles hors des faits intervenant dans le ménage et celles qui concernent les couples et ex. conjoints ont progressé significativement passant d'un taux de 1,3 pour 1 000 habitants à 3,3 en l'espace de 22 ans. Le système statistique du ministère de l'Intérieur agrégeant les motifs de violences, il est

difficile de déterminer si tous les motifs de violences ont progressé ensemble au sein cet indicateur, ou si l'un d'eux a pris le pas sur l'autre.

Ce que l'on apprend en revanche à partir des enquêtes de victimation c'est que le nombre de personnes se déclarant victimes de violences physiques hors du ménage a plutôt diminué sur la période 2006–2018. Il en est de même pour les violences physiques et sexuelles commises sur des victimes cohabitantes [Insee-ONDRP-SSMSI, 2019]. Cette divergence des résultats tendrait à indiquer que le phénomène des violences est mieux rapporté et qu'il serait plutôt globalement en baisse sur la période des treize dernières années.

Les violences sexuelles, qu'elles visent les mineurs ou les majeurs, ont connu une forte progression au cours des vingt dernières années, notamment les faits commis contre les majeurs : + 140 %, si l'on compare le niveau des faits enregistrés de 2017 à celui de 1996. L'effet #MeToo, en France comme dans la plupart des pays, a probablement entraîné un effet statistique, comme l'a souligné le ministère de l'Intérieur dans son bilan statistique de janvier 2018 [Interstat, 2018]. Mais on ne peut s'empêcher de remarquer qu'à partir de 2010 pour les majeurs et 2011 pour les mineurs, les chiffres ne cessent d'augmenter. L'affaire Weinstein semble avoir été un accélérateur de la hausse plus qu'une source.

Le nombre de cambriolages oscille depuis 1996 entre un plus bas en 2007 (150 491 faits) et un plus haut en 2013 (229 365 faits), pour finalement produire une courbe sans signification statistique. Un haut responsable de la police parisienne s'interrogeait encore récemment en privé sur les facteurs de ces variations et sur sa capacité à peser sur ce phénomène dont il se considérait plutôt comme un spectateur<sup>10</sup>, car démuné d'outil de compréhension lui permettant de réagir à bon escient.

La courbe des vols d'automobiles est la statistique la plus encourageante. Elle indique un reflux significatif de ce type de vol sur la période, le taux passant de 6 à 1,5 pour 1 000 habitants. Cette tendance est la même constatée par Eurostat pour les voisins de la France et pour l'ensemble des pays de l'UE : - 36 % entre 2008 et 2016

(7) <https://futureoflife.org/autonomous-weapons-open-letter-2017/?cn-reloaded=1> ;  
<https://www.stopkillerrobots.org/>  
<https://www.declarationmontreal-iaresponsable.com/la-declaration>

(8) 1996 est l'année de référence pour la continuité statistique, car le contexte légal, la nomenclature et les modes de recueil de l'information ont peu varié.

(9) Voir : Besson (J.-L.), 2015, « Les homicides volontaire diagnostiqués par l'IML de Paris de 1994 à 2013 », *Focus*, ONDRP, n° 9 ; Mucchielli (L.), 2008, *L'évolution des homicides depuis les années 1970 : analyse statistique et tendance générale*, CESDIP.

(10) Entretien avec l'auteur (2017).



[Eurostat, 2018]. L'explication la plus souvent avancée tient au fait que les constructeurs ont pris des mesures efficaces pour mieux protéger les produits [Tremblay, Cusson, Clermont, 1992]. S'y ajoutent probablement la diminution des facteurs de risque par la vidéosurveillance de la voie publique et la multiplication des infrastructures de stationnement privées et gardiennées [Besson, 2019].

Le nombre de vols simples et de vols avec violences augmente significativement au cours des vingt dernières années, et notamment celui des vols simples (+ 51 %). Il faut rappeler qu'ils constituent l'infraction la plus massive et aussi la plus banale au sein des délits : 20 % en moyenne sur la période d'observation. Les vols simples sont particulièrement concentrés dans l'espace et leur distribution spatiale est liée à la forme de l'organisation urbaine et au flux de population [Besson, 2019].

Les infractions aux stupéfiants sont des faits révélés par l'initiative des forces de l'ordre. Que ce soit la lutte contre le trafic ou l'usage, la hausse des faits est significative sur la période. Le taux d'infraction pour l'usage simple passe ainsi de 1,1 à 2,7 pour 1 000 habitants, ce qui peut traduire une hausse du nombre de consommateurs, ou le temps toujours plus grand consacré par la police à lutter contre l'usage de stupéfiants. Ou les deux.

La justice n'est pas en reste. Lors de l'audience solennelle de rentrée de janvier 2018, la procureure du TGI de Bobigny a lancé ce qui a été entendu comme un appel au secours face à l'aggravation de la délinquance en Seine-Saint-Denis et au défaut de moyens pour mettre en œuvre des réponses pénales adaptées. Elle a rappelé à cette occasion que 170 000 affaires avaient été traitées par seulement 56 magistrats l'année précédente.

## Veiller à ce que les victimes d'actes criminels reçoivent le service auquel elles s'attendent

Les questions de moyens, d'organisation, de méthode, de mode de procédures ont des effets pervers qui s'étendent au-delà de la sphère de la police et de la justice. La congestion, la lenteur de la procédure, des décisions et de leur exécution renvoient à la problématique de la confiance de la victime dans le système pénal et aboutit *in fine* à distendre les liens police/population, justice/victimes. Car l'une des raisons majeures avancées par les victimes pour justifier de leur absence de déplacement pour signaler le fait dont elles ont été victimes est que

« ça ne sert à rien ». C'est notamment ce qui ressort de l'enquête de victimation de 2019 pour les violences au sein du couple dont 59 % ont estimé ce déplacement inutile alors qu'elles n'étaient « que » 23 % à ne pas avoir signalé les violences par crainte de représailles [ONDRP, 2019].

L'enquête nationale de victimation dont les résultats ont été publiés en 2018 [ONDRP, 2018] révèle que seulement 41 % des victimes de vols avec violences et 32 % des victimes de vols simples sur 10 se déplacent auprès des autorités. Lorsque le fait est une violence hors du contexte du ménage, 24 % des victimes portent plainte et elles ne sont plus que 14 % dans le cas des violences commises au sein du couple, 12 % pour des violences sexuelles subies hors du ménage, 9 % pour des violences commises au sein du ménage (hors violences entre conjoints). Mis à part les vols d'automobiles pour lesquels 92 % des victimes portent plainte [ONDRP, 2018] et dans une moindre mesure les cambriolages dont 74 % des victimes portent plainte [ONDRP, 2018], les autorités n'ont qu'une connaissance très partielle des autres atteintes à travers les données de signalements des victimes.

Avec la naissance du *Data Driven Policing* (DDP), il y a nécessité d'augmenter les flux de données relatifs aux signalements des victimes pour augmenter le volume de la réalité connue [Kearns, Muir, 2019]. À l'instar de l'apprentissage de l'IA qui a besoin d'ingérer des quantités très importantes d'informations pour réduire l'incertitude du résultat, les autorités auraient également besoin, par symétrie, d'augmenter la quantité de déclarations et de plaintes pour mieux cerner les phénomènes criminels auxquels elles ont à faire face. Pour cela, la France pourrait élaborer une solution inspirée par les nouvelles règles générales d'enregistrement du système national d'enregistrement du Home Office. Elles obligerait la police à enregistrer initialement, sous la forme d'un rapport d'incident, tout signalement émanant d'une victime, d'un témoin ou d'une partie autre. La qualification pénale (ou pas) de l'incident interviendrait après. Dans ce système la personne signalante est garantie que sa parole est enregistrée et traitée [Home Office, 2019]. Les objectifs sont clairement énoncés dans les instructions du système. On lit notamment : « veiller à ce que les victimes d'actes criminels reçoivent le service auquel elles s'attendent et qu'elles méritent ; informer le public de l'ampleur, de la portée et du risque de criminalité dans leurs localités ; éclairer l'élaboration de la politique gouvernementale visant à réduire la criminalité et à déterminer si ces politiques sont efficaces ».

## 10 000 suspects en 100 millisecondes

Techniquement, le bouleversement qui allie le DDP et l'IA a commencé. Il a débuté en Chine, en Estonie, en Grande-Bretagne, aux États-Unis, aux Émirats arabes unis, en Russie et en France. L'IA va s'insérer dans les outils d'anticipation (lieu des faits), de surveillance (caméras), de contrôle (lunettes), de traitement (procédure). Déjà présente dans les navigateurs internet, les véhicules autonomes, la santé, l'IA va s'introduire dans le champ de la police et de la justice à plus ou moins court terme selon l'état d'avancement de la recherche des expérimentations et selon aussi la liberté autorisée par la réglementation. Quelques exemples d'expérimentations menées çà et là dans le monde permettent de s'en convaincre.

L'Estonie, poursuivant son objectif de construction d'un e.État, expérimente l'IA dans nombre de secteurs. L'un de ses projets les plus disruptifs est sans doute l'introduction d'une justice digitalisée pour les affaires de litiges de moins de 7 000 euros. Cette justice devrait être rendue par un « juge robot » et susceptible d'appel devant une cour humaine. L'objectif est ici de résorber un contentieux de masse de faible gravité, mais qui encombre les tribunaux et submerge juges et greffiers [Rohaidi, 2019].

Pour améliorer l'accueil, la police de Dubaï expérimente une version modifiée du robot Reem de chez Pal Robotics. Ce robot est capable de comprendre neuf langues, transmettre les plaintes, surveiller par vidéo et utiliser de la reconnaissance faciale. Dubaï s'est fixé l'objectif de composer un quart de sa police par des robots à l'horizon 2030 [Page, 2017].

L'augmentation des flux de personnes sur la voie publique, dans les espaces de transports, sur les points de rassemblement (stades, salles de concerts...) réclame une augmentation des capacités de surveillance et le contrôle qui ne peuvent être assumés uniquement par les moyens humains. La vidéosurveillance se généralise<sup>11</sup> donc en milieu urbain [BOVP, 2019]. Son efficacité se heurte cependant aux limites des capacités des opérateurs. L'œil ne peut détecter une situation atypique au-delà de huit flux vidéo simultanés et l'attention décline au bout de 2 heures [ministère Intérieur, 2006]. En termes de recherches post-

événement, la somme d'images à consulter contraint à des heures de visionnage. L'afflux d'image augmente les besoins en capacité de traitement, d'où l'apparition d'assistances logicielles, par exemple pour éliminer les séquences sans mouvement ou retrouver une forme, voire un visage si la réglementation le permet<sup>12</sup>, sur de longues durées d'enregistrement.

Une réglementation restrictive des libertés fondamentales n'est pas un obstacle en Chine. Pour juger des performances des systèmes de surveillance déjà en place, un test mené par un journaliste de la BBC a prouvé qu'il pouvait être localisé en 7 minutes n'importe où sur le territoire grâce au dispositif de 170 millions de caméras équipées d'intelligence artificielle [Sudworth, 2017] – 400 millions de caméras sont prévues pour 2020, elles pourront identifier les plaques d'immatriculation, les visages, déterminer les âges.

La société chinoise LLVision a, de son côté, développé une technologie de reconnaissance faciale montée sur des lunettes portées par les policiers, capable de balayer une base de données de 10 000 suspects en 100 millisecondes et de faire correspondre les visages captés à cette base. Sept personnes recherchées ont ainsi pu être identifiées par ce système utilisé par la police ferroviaire de la gare de Zhengzhou et 26 usurpateurs d'identité ont été interpellés [Yan, 2018].

## Apprendre des comportements qui ne peuvent être détectés par l'œil humain

Surveiller ne dissuade pas toujours les passages à l'acte délictueux ou criminels. Identifier est un objectif premier de l'enquête mais c'est un processus réactif. Il consacre l'échec de la prévention. Ce qu'Alain Bensoussan entrevoit pour l'avenir, c'est une société sans crime et délit parce que chacun d'eux aura pu être anticipé, prévenu, empêché. C'est une voie dans laquelle se sont engagés ceux qui pensent avoir la capacité de prévoir l'avenir, fût-ce au prix du renoncement aux principes généraux qui fondent la démocratie. C'est un peu le cas pour la police de Fresno (Californie) et la société Hitachi.

(11) 1 400 caméras de surveillance sont implantées à Paris, 2 145 à Nice, 6 000 communes possèdent un système de vidéoprotection (ministère de l'Intérieur).

(12) Table ronde Hicham Aloui Fdili, Sécurité, Justice : le défi de l'intelligence artificielle, jeudi 7 novembre 2019, bâtiment Ségur/Auditorium Marceau Long.

La police de Fresno s'est équipée en 2015 d'un centre de contrôle en temps réel qui surveille la ville 24 heures sur 24 [Appleton, 2015]. Ses opérateurs ont accès à 1 000 flux vidéo différents et comptaient y ajouter les 400 flux individuels issus des caméras portées par les policiers. Les opérateurs ont aussi la capacité de fouiller une base de données privée de 2 milliards de données d'analyses de plaques d'immatriculation, mais aussi les réseaux sociaux et même les sons de la ville à travers un outil qui triangule le bruit d'éventuelles détonations dues à des armes à feu. Quelque chose de classique désormais pour les villes nord-américaines.

Plus original, le centre a expérimenté une voie plutôt inattendue pour prévenir les crimes : il a imaginé un dispositif de *scoring* des menaces présentées par les individus à Fresno. Pour cela, un logiciel parcourt « des milliards de points de données, notamment des rapports d'arrestation, des dossiers de propriété, des bases de données commerciales, des recherches approfondies sur le Web et les publications sur les réseaux sociaux », rapporte le *Washington Post* dans son édition locale de janvier 2016 [Jouvenal, 2016]. Ceci permet à l'opérateur du centre opérationnel d'établir un score de niveau de menace d'un individu et d'anticiper une éventuelle activité criminelle de sa part.

Une des justifications avancées par le chef de la police était que le *scoring* permettait une sécurisation des interventions par une évaluation précise de la menace. Ce système a été stoppé à la suite des préoccupations qu'il avait fait naître parmi la population et le conseil municipal de Fresno, notamment à cause d'exemples de mauvaises interprétations des données traitées faisant peser le risque de prises de décisions erronées par la police.

À travers son système *Visualization Predictive Crime Analytics* (PCA) piloté par l'intelligence artificielle, la société Hitachi a conçu un outil qui serait capable de prédire les actes criminels avant qu'ils ne se produisent grâce à une plateforme de traitement<sup>13</sup>. Celle-ci serait capable de produire une carte de zones de chaleur résultant de données d'événements en temps réel captées à partir de systèmes de sécurité publique et de capteurs puis combinées à des données historiques et contextuelles sur la criminalité, des médias sociaux et autres sources ouvertes. Selon le communiqué de presse, Hitachi se disait

capable d'exploiter une intelligence artificielle « capable d'apprendre des comportements qui ne peuvent être détectés par l'œil humain ». Ces algorithmes peuvent également être utilisés pour créer des prédictions extrêmement précises de niveau de menace afin d'anticiper où des crimes sont susceptibles de se produire et où des ressources supplémentaires sont susceptibles d'être nécessaires [Nicora, 2015].

En Corée du Sud, le district de Seocho à Seoul et l'Institut de Recherche sur les Télécommunications Electroniques (IRTE), vont installer en 2020 des caméras couplées à de l'IA pour analyser l'emplacement, l'heure et les comportements des citoyens afin de déterminer la probabilité qu'un crime se produise. L'analyse sera affinée par l'apprentissage automatique à partir de jugements et de descriptions de séquences d'actes criminels pour déterminer des « situations à risque » par comparaison. « It will work like Déjà Vu », a dit le porte parole d'IRTE (Mu-Hyun, 2020).

En Europe, il n'apparaît pas raisonnable de penser comme cela. Notamment pas selon le groupe d'experts de haut niveau<sup>14</sup> placé auprès de la Commission européenne pour réfléchir sur l'éthique de l'IA. Il vient de passer en phase test les sept principes pour une IA éthique après avoir publié, début 2019, ses directives d'éthique pour une IA digne de confiance [High-Level Expert Group on Artificial Intelligence, 2019]. La Commission européenne pour l'efficacité de la justice du Conseil de l'Europe avait déjà adopté la Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement en décembre 2018 [CEPEJ, 2018].

Mais avant les aspects éthiques de l'IA, la protection des données personnelles est un sujet qui en Europe a débouché sur la mise en place du règlement général sur la protection des données (RGPD). Ce règlement européen en vigueur depuis le 25 mai 2018 pour les pays de l'Union européenne, a pour objectif de responsabiliser les collecteurs de données et instaure, de fait par ses effets sur les échanges de données, une nouvelle norme mondiale en la matière. Si les fichiers de sûreté de l'État et de la défense nationale sont exclus du champ d'application, en revanche certains traitements « mis en œuvre dans le cadre d'activités qui ne relèvent pas spécifiquement de la sphère pénale mais qui se rapportent à des activités de police effectuées en amont de

(13) Hitachi Visualization Suite (HVS).

(14) The AI HLEG is an independent expert group that was set up by the European Commission in June 2018. Madame Françoise Soulie-Fogelman, professeur d'IA et consultant en Data Mining & Artificial Intelligence, qui est intervenue dans le colloque organisé par l'INHESJ le 7 novembre 2019 sur le défi de l'IA appliqué à la sécurité et à la justice, est membre de ce groupe d'experts indépendants.

(15) <https://www.cnil.fr/directive-police-justice-de-quoi-parler>

(16) Google, Apple, Facebook, Amazon, Microsoft.

(17) Baidu, Alibaba, Tencent et Xiaomi.

la commission d'une infraction pénale », entrent dans le champ de la directive Police Justice qui complète le RGPD, indique la Commission nationale de l'informatique et des libertés (CNIL) sur son site Web<sup>15</sup>.

On peut s'interroger sur le niveau réel d'acceptabilité de la population envers la collecte de ses propres données lorsque l'on observe les comportements des utilisateurs de réseaux sociaux et des principaux outils mis en ligne par les GAFAM<sup>16</sup> et autres BATX<sup>17</sup>. C'est-à-dire nous tous. Mais de plus en plus de voix se font entendre qui visent à rendre conscient l'utilisation de ces outils basés sur le *Big Data*.

## Les boucles de rétroaction, un biais inhérent à la compilation des données ?

Mais qu'est-ce que l'IA ? Le groupe d'experts indépendants donne la définition suivante : « *Les systèmes d'intelligence artificielle (IA) sont des systèmes logiciels (et éventuellement matériels) conçus par des êtres humains et qui, ayant reçu un objectif complexe, agissent dans le monde réel ou numérique en percevant leur environnement par l'acquisition de données, en interprétant les données structurées ou non structurées collectées, en appliquant un raisonnement aux connaissances, ou en traitant les informations, dérivées de ces données et en décidant de la/ des meilleure (s) action (s) à prendre pour atteindre l'objectif donné*<sup>18</sup> ».

Née en 1956<sup>19</sup>, c'est un système qui génère de la connaissance à partir des données volumineuses, ce que George Uzbelger nomme « *l'ère Cognitive* » qui résulte de la convergence de quatre technologies : l'informatique, les nanotechnologies, la biotechnologie et les sciences cognitives [Uzbelger, 2019]. Au départ, il existe un besoin et des données relatives à ce besoin. La solution est d'abord conceptualisée puis modélisée par les algorithmes, ce qui aboutit à un résultat qui sera traduit par une visualisation. Les données sont comme du pétrole brut qui est raffiné par les algorithmes qui en révèlent des caractères qu'un être humain est incapable de déceler en raison du volume à ingérer. Plus le volume de données sera élevé, plus la solution sera pertinente et le résultat certain. C'est ce qui conduit les concepteurs de logiciels prédictifs basés sur ces données à vouloir intégrer le plus de sources possible.

En matière de police, l'objectif de la plupart des logiciels prédictifs est bien celui-là : anticiper les lieux où les faits vont se produire à partir de l'étude du passé criminel des lieux. Plus les informations sur le passé seront nombreuses, plus le résultat sera pertinent et plus la gestion des policiers sur le terrain sera précise et optimisée.

Cette approche de la criminalité à partir des données semble plus objective que celle fondée uniquement sur l'expérience des agents, comme pour le *Moneyball*, car l'observation des agents est subjective par définition et elle ne concerne que le territoire sur lequel ils agissent. Pour les faits qui ne sont pas révélés uniquement par l'action de la police (infractions à la législation sur les stupéfiants, port d'arme prohibé, travail clandestin...), l'alimentation des bases de données peut être considérée comme objective. Elle ne dépend que de la propension de la victime à déposer plainte. Elle n'est cependant pas dénuée de biais.

Le premier, et c'est ce qui constitue la faiblesse principale des logiciels de prédictivité en matière de police, consiste à confondre les faits connus des autorités avec la criminalité réelle. Or, ces données ne reflètent finalement que l'activité d'enregistrement des services à partir des paroles des victimes qui, comme on l'a mentionné plus haut, auront bien voulu se déplacer. On sait, par les enquêtes de victimation, que le taux de plainte est très variable en fonction des types d'infractions, du sexe et de l'âge des victimes. Il est le plus élevé pour les vols d'automobiles et le plus faible pour les violences commises au sein du ménage [Insee-ONDRP-SSMSI, 2019]. Les données criminelles relatives au passé des lieux ne fournissent parfois qu'une image très partielle du phénomène et font douter légitimement de la pertinence du résultat de l'analyse.

Un second biais réside dans ce que Cathy O'Neil appelle les « *boucles de rétroaction* ». Cette théorie fonctionne ainsi. Lorsque les signalements de nuisances et d'infractions générés par la population aboutissent à envoyer plus de policiers sur un secteur, cette augmentation de personnel (logique d'affecter le personnel là où se produisent les incidents) amène mécaniquement une hausse des constatations (si ce personnel ne ramène pas d'affaires, il sera mal noté) qui entraîne à nouveau mécaniquement une augmentation du personnel. « *Le maintien de l'ordre génère par lui-même de nouvelles données qui justifient en retour son renforcement dans certaines zones [...] Même si un modèle se montre indifférent à la couleur de peau, il en va tout autrement*

[18] La définition complète en suivant ce lien : <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>

[19] Conférence de Dartmouth, été 1956, qui instaure l'intelligence artificielle comme domaine de recherche autonome.

du résultat obtenu. Aux États-Unis, où les villes sont fortement marquées par la ségrégation, la localisation géographique se substitue très efficacement aux données raciales » [O'Neil, 2016].

La question des données est donc centrale. La meilleure IA en théorie pourra s'avérer défailante jusqu'à provoquer des effets secondaires indésirables si les données sont elles-mêmes biaisées par leur imperfection : valeurs manquantes, absence de leur mise à jour, erreurs... Car l'une des croyances largement répandues est qu'il suffit de mettre au point un système qui fonctionne pour considérer qu'il fonctionnera *ad vitam aeternam*. Notamment en matière de criminalité, les données évoluent constamment. Ce qui constitue théoriquement la force d'une approche *Data* est paradoxalement aussi sa principale faiblesse, car contrairement à ce qui est médiatisé actuellement, l'IA n'a d'intelligence que le nom. Il s'agit, au stade des développements actuels, d'un système de calculs très élaborés capable de traiter des quantités immenses d'informations variées et hétérogènes, d'y trouver des corrélations et de proposer des résultats avec une probabilité élevée de certitude. Mais il n'est pas intelligent. Il permet juste de proposer des règles de décision au sein d'une masse d'informations. L'intelligence, c'est une activité volontaire et réfléchie qui s'oppose à l'instinct [Bar-Hen, 2018]. Il lui manque le sens commun et la conscience, des états que la recherche échoue aujourd'hui à modéliser [Uzbelger, 2018].

Faut-il tout jeter pour autant ? On l'a vu, le bilan de l'action publique contre la criminalité n'est pas satisfaisant. À de rares exceptions près, la réponse est quantitative. Les maires réclament toujours plus de policiers ou de gendarmes sur leur territoire. Le ministère de l'Intérieur communique sur le nombre de forces de l'ordre alignées pour contrôler tel ou tel événement. La population se sent rassurée lorsqu'elle apprend l'affectation de policiers dans le commissariat de sa ville. Depuis des dizaines d'années, la réponse à l'insécurité semble se focaliser sur ces dix ou vingt policiers qui manquent localement dans les effectifs. Et ce serait une cause de la hausse de l'insécurité, si tant est qu'il existe une hausse réelle et une cause principale.

La pression budgétaire introduite par la Révision générale des politiques publiques (RGPP) a conduit à réduire le nombre de policiers et de gendarmes de plus de 9 000 entre 2009 et 2012 [Placé, 2012]. Même si depuis leur nombre a augmenté, la France cherche, comme la plupart des pays, à rationaliser sa dépense publique et augmenter sa performance. Ceci vaut aussi pour l'utilisation des forces de l'ordre contre la criminalité. L'analyse de la rationalité géographique de la criminalité est un angle d'attaque connu pour avoir obtenu des résultats au cours depuis les années 1990 [Willis, Mastofski, Weisburd, 2007].



LA MEILLEURE IA EN THÉORIE POURRA S'AVÉRER DÉFAILANTE JUSQU'À PROVOQUER DES EFFETS SECONDAIRES INDÉSIRABLES SI LES DONNÉES SONT ELLES-MÊMES BIAISÉES PAR LEUR IMPERFECTION : VALEURS MANQUANTES, ABSENCE DE LEUR MISE À JOUR, ERREURS... CAR L'UNE DES CROYANCES LARGEMENT RÉPANDUES EST QU'IL SUFFIT DE METTRE AU POINT UN SYSTÈME QUI FONCTIONNE POUR CONSIDÉRER QU'IL FONCTIONNERA AD VITAM AETERNAM. NOTAMMENT EN MATIÈRE DE CRIMINALITÉ, LES DONNÉES ÉVOLUENT CONSTAMMENT. CE QUI CONSTITUE THÉORIQUEMENT LA FORCE D'UNE APPROCHE DATA EST PARADOXALEMENT AUSSI SA PRINCIPALE FAIBLESSE, CAR CONTRAIREMENT À CE QUI EST MÉDIATISÉ ACTUELLEMENT, L'IA N'A D'INTELLIGENCE QUE LE NOM.



## Organiser la distribution des forces de police à partir de l'analyse statistique du terrain

Ce que l'on sait depuis quelques décennies à propos de la localisation des crimes, des délits, des nuisances, c'est que ces événements sont concentrés sur un territoire. Les premiers travaux, regroupés sous la bannière de l'école de Chicago, s'intéressent à la distribution spatiale de la criminalité à travers l'étude des lieux de résidence des auteurs d'infractions [Shaw, McKay, 1942]. Après la Seconde Guerre mondiale et jusqu'aux années 1970, la recherche a délaissé cette approche pour se consacrer à l'étude des auteurs et les causes des déviations en assumant par principe que les lieux de commission des faits étaient distribués uniformément sur le territoire [Weisburd, Eck, Braga, 2016]. Mais dans les années 1980, avec l'émergence de l'ordinateur personnel (PC), des données (*DATA*), des systèmes d'information géographique (SIG), et d'une nouvelle criminologie de l'environnement appuyée sur les travaux de la théorie du choix rationnel [Cornish, Clarke, 1986], la théorie des activités de routine [Cohen, Felson, 1979] et de l'influence du contexte géographique sur la fréquence de commission des faits criminels

[Brantingham & Brantingham, 1984], la criminologie du lieu renaît. Les travaux sur les micro-lieux, c'est-à-dire l'analyse du fait à son lieu exact de commission et non plus agrégé à une échelle territoriale supérieure (quartier, secteur, arrondissement, district...), permettent de mettre en exergue une caractéristique propre à la criminalité : la concentration sur des lieux restreints, autrement dit, les *hot spots* [Sherman, Gartin, Buerger, 1989].

Cette découverte va être largement exploitée par la suite par nombre services de polices de par le monde, à commencer par la plupart des villes américaines à travers la mise en œuvre du management par le COMPSTAT<sup>20</sup>. Ce système de management par objectifs chiffrés, organise la distribution des forces de police à partir de l'analyse statistique du terrain par les données remontées sur l'état-major central. Deux motivations à cela. La première est un constat à la fin des années 1980 d'une impuissance de la police et de la justice à réduire le niveau de la criminalité avec un traitement qui privilégie avant tout l'aspect social, à travers les programmes d'aide, de prévention, d'insertion et d'encadrement. On doit se rappeler qu'en 1990, New York enregistre 2 262 meurtres, 3 126 viols, 122 055 cambriolages, 100 280 vols avec violences, 44 122 agressions<sup>21</sup>.

La seconde raison est budgétaire. Après avoir traversé une période économique très difficile qui débute à la fin des années 1960 avec le désengagement de l'État fédéral d'un certain nombre de budgets et qui culmine le 13 juillet 1977 avec le black-out des 31 quartiers de la ville à la suite d'un orage, le changement de doctrine policière va s'illustrer sur deux axes : une rationalisation de la ressource policière en raison de la raréfaction des possibilités budgétaires ; une politique de résultats évalués en permanence. En 2018, la ville a enregistré 295 meurtres, 1 794 viols, 12 913 vols avec violences, 20 208 agressions, 11 687 cambriolages<sup>22</sup>. De nombreux débats portent sur les causes de cette baisse drastique des crimes et délits commis sur la période 1990-2018 et sur ses effets collatéraux [E.Zimring, 2011] ; [Gopnik, 2018]. Mais personne ne conteste factuellement les résultats de la mesure statistique.

## Causation is dead, correlation is king

Est-ce que cette situation est durable ? Si l'on prend pour hypothèse que l'un des éléments de la baisse a été

l'identification des *hot spots* et l'affectation de moyens dérogatoires sur ces lieux pour reconquérir le territoire, les autorités seront contraintes de maintenir une pression constante dans le temps. En effet, ces points chauds (concentrations criminelles sur peu de lieux) n'existent qu'en raison de conditions contextuelles favorables à leur émergence et leur pérennité [Lee, Eck, O, Martinez, 2017]. Identifier les *hot spots* sans pousser plus avant l'analyse pour déterminer les facteurs explicatifs qui produisent ces situations ne permet probablement pas de modifier le résultat dans le long terme.

C'est ici que revient l'intelligence artificielle. « *Causation is dead, correlation is king. Les nouveaux défis concernent simplement la gestion du volume, de la vitesse et de la variété des informations flexibles, relationnelles, affinées et indicielles qui deviennent de plus en plus disponibles* » [Kitchin, 2014]. Prédire l'émergence de points chauds à travers la modélisation de réseaux de neurones artificiels [Olligschlaeger, 1998] et d'autres techniques avancées de traitement des données de plus en plus volumineuses et variées a été entrepris à l'état expérimental depuis les années 2000. On citera les recherches destinées à améliorer la détection des *hot spots* par la mise en œuvre de l'analyse par densité de noyau (Kernel) en y adjoignant une analyse linguistique des tweets géolocalisés [Gerber, 2014]. Le volume des tweets géolocalisés est aussi utilisé dans l'expérience menée à San Francisco pour tenter de prédire l'activité criminelle d'une rue [Bendler, Brandt, Wagner, 2014].

Cette dernière expérience répond à une problématique que l'on rencontre couramment dans les études spatiales sur la criminalité, à savoir : comment estimer la population présente sur un territoire en fonction du moment pour estimer le niveau de risque relatif ? En effet, en raison de l'absence de disponibilité de données, les faits constatés sont rapportés au nombre d'habitants du territoire d'étude. Cependant, pour les infractions dépendantes des flux de population (la plupart de celles commises sur la voie publique), le nombre d'habitants comme donnée de standardisation est une donnée fautive. Elle aboutit à surexposer statistiquement artificiellement le territoire [Besson, 2007]. La captation des flux Twitter géolocalisés dans la zone peut permettre d'estimer la population présente réellement sur le territoire à l'heure de commission du fait [Malleison, Andressen, 2015].

Le centre de recherche sur la sécurité publique de l'université Rutgers (New Jersey) a voulu dépasser l'objectif d'identification du *hot spot* après avoir fait le constat que le

(20) Acronyme de *Computer Statistics*.

(21) Source NYPD COMPSTAT Unit, vol. 26 Number 45.

(22) *Idem*, 14

point chaud étant éliminé, il ressortait immanquablement ailleurs sur le territoire. Repartant des recherches sur le contexte du lieu du crime, la criminologie du lieu et des espaces à risque, ses chercheurs ont inventé une méthode devenue depuis une application en ligne, destinée à identifier les facteurs significatifs qui concourent à la création de ces points chauds.

Cette méthode dénommée «*Risk Terrain Modeling*» consiste, après avoir découpé le territoire en cellules (ex : 200 m), à désagréger tous les facteurs contextuels de risques géolocalisés dans l'environnement du lieu du fait, à tester leur influence sur le fait et à ne retenir que les facteurs significatifs qui sont alors empilés par le système<sup>23</sup> d'information géographique et visualisé dans une cartographie. Il s'agit d'une analyse de régression avec une sélection du « meilleur » modèle statistique. Le résultat propose une carte avec une échelle de risques déclinée par cellule qui a pour avantage de ne plus prendre seulement en compte l'historique criminel du lieu, mais également les conditions de son environnement qui, sur un plan statistique, sont les facteurs d'aggravation du risque, ceux qui provoquent les concentrations criminelles.

Cette approche fonctionne [Caplan, Kennedy, Piza, Barnum, 2019]. Mais les facteurs sont actuellement limités aux données physiques présentes dans les bases de données courantes des systèmes d'information géographique (restaurants, arrêts de bus, bouches de métro, écoles, gares, commerces...). L'analyse est encore limitée par la puissance de calcul de la machine et, si elle est reproductible, sa précision ne s'améliore pas à l'usage.

Y parvenir, c'est probablement passer du stade de la régression statistique à l'IA. L'intégration et le traitement de nouvelles données hétérogènes relatives au lieu produit par les déplacements, les réseaux sociaux, les flux vidéo, les fils d'informations, les rapports de police, le déploiement des forces de l'ordre sur le lieu, auraient toute leur place dans cette méthodologie RTM. Mais le moyen d'augmenter la précision du modèle passerait par l'utilisation d'une IA qui serait elle-même capable de choisir les meilleures variables et de combiner les facteurs de manière inattendue par l'auto-apprentissage, en réinjectant par exemple les faux positifs et les faux négatifs dans l'analyse.

## Vers une criminologie augmentée

L'augmentation de l'utilisation par la police de données autres que les plaintes, les mains courantes, les interpellations, les fichiers de recherche, devient peu à peu une réalité pour le maintien de l'ordre au quotidien. Les images des réseaux de vidéosurveillance et celles des caméras portées par les agents, les sons des systèmes de captation des détonations (GDS), les scanners viennent s'ajouter aux sources classiques de données [Fergusson, 2017]. Mais il s'agit de données d'activités qui, sous couvert de nouvelles technologies, maintiennent toujours l'action policière dans une doctrine réactive.

L'utilisation des nouvelles *Big Data*, composées notamment des flux des réseaux sociaux, ouvre de nouvelles perspectives en matière d'analyse qui potentiellement peuvent faire basculer la doctrine vers l'anticipation et la prévention. Le passage de l'approche sociologique à la science criminelle s'est opéré autour des années 2000 lorsque le *Big Data* a changé les pratiques des sciences sociales en passant de la recherche d'une causalité à l'identification de corrélations au travers de données variées, structurées, non structurées, volumineuses, changeantes [Chan & Bennett Moses, 2016]. Il ne s'agit pas maintenant de considérer que les données sont objectives parce que neutres par définition. Les données ne sont pas neutres. Elles sont produites et conçues par des hommes et des machines fabriquées par des hommes, dans un contexte particulier. Elles n'existent pas comme des éléments autonomes, ce que voudraient faire croire parfois certains scientifiques emportés sans doute par leur enthousiasme d'atteindre enfin un résultat avec une véritable objectivité. Les données ne parlent pas pour elles-mêmes. Elles reflètent le système qui les crée [O'Neil, 2016].

Pour autant, les moins de 24 ans savent qu'elles font partie de ce nouveau monde où ce qui n'est pas plateforme apparaît pour le moins daté. Les rejeter au nom d'un principe de précaution, d'un manque de cadre théorique et parce que quelques éléments de compréhension nous échappent encore, c'est probablement tourner le dos aux promesses d'une criminologie augmentée. Plaidons au moins pour la recherche et sa procédure du bac à sable<sup>24</sup> ■

(23) Gunshot Detection System (GDS). 50 % des juridictions de 1 million d'habitants sont équipées, 30 % des juridictions de 500 000 habitants, 28 % des juridictions de 250 000 habitants [Reaves, 2015].

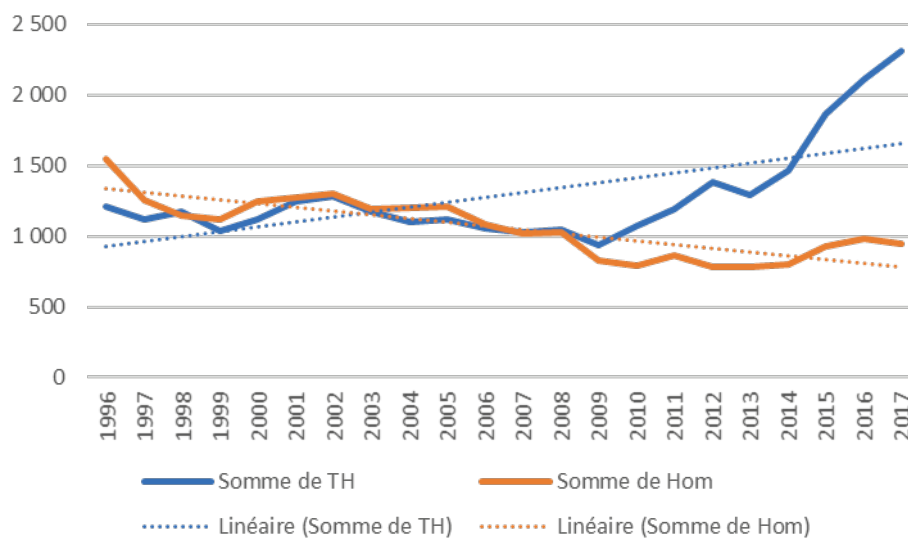
(24) *Sand Box* est une série de règles qui permet de tester une méthode dans un environnement réel sans avoir à suivre certaines contraintes juridiques faisant l'objet de restrictions. La méthode du bac à sable a récemment été retenue par le rapport Villani sur l'intelligence artificielle.

## Figures

1 - Homicides intentionnels et tentatives

Taux pour 100 000 habitants 1996 Homicides = 2,7 ; 2017 = 1,4 ; baisse significative sur la période.

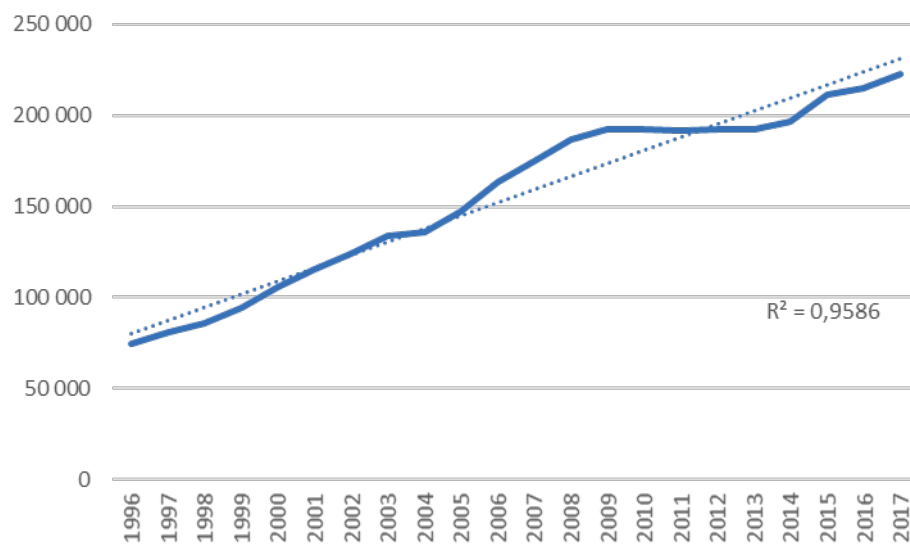
Taux pour 100 000 habitants 1996 Tentatives Homicides = 2,1 ; 2017 = 3,4 ; hausse significative sur la période.



Source : ministère de l'Intérieur, état 4001.

2 - Coups et blessures volontaires

Taux pour 1 000 habitants 1996 = 1,3 ; 2017 = 3,3 ; hausse significative sur la période.

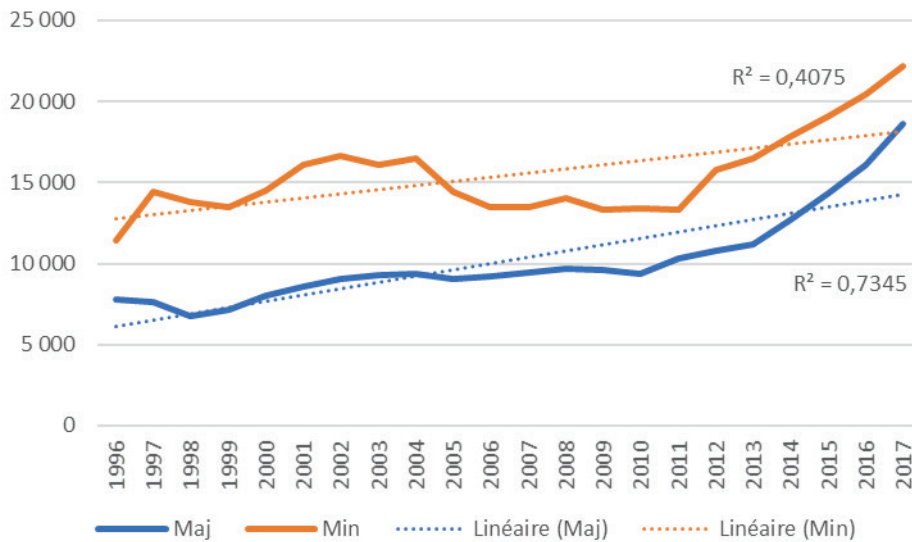


Source : ministère de l'Intérieur, état 4001.



### 3 - Viols et agressions sexuelles sur majeurs et mineurs

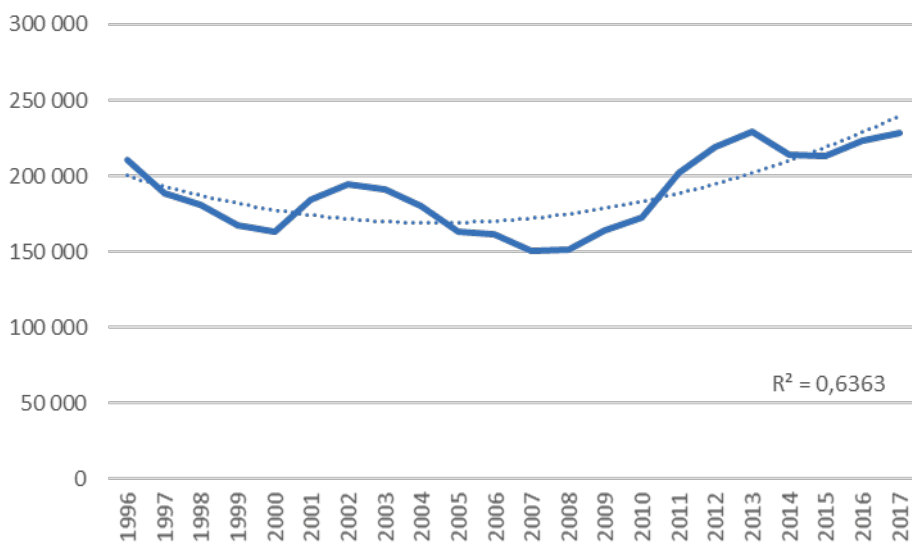
Majeurs, taux pour 1 000 habitants 1996 = 0,1 ; 2017 = 0,3 ; hausse significative sur la période.  
 Mineurs, taux pour 1 000 habitants 1996 = 0,2 ; 2017 = 0,3 ; hausse significative sur la période.



Source : ministère de l'Intérieur, état 4001.

### 4 - Cambriolages d'habitations

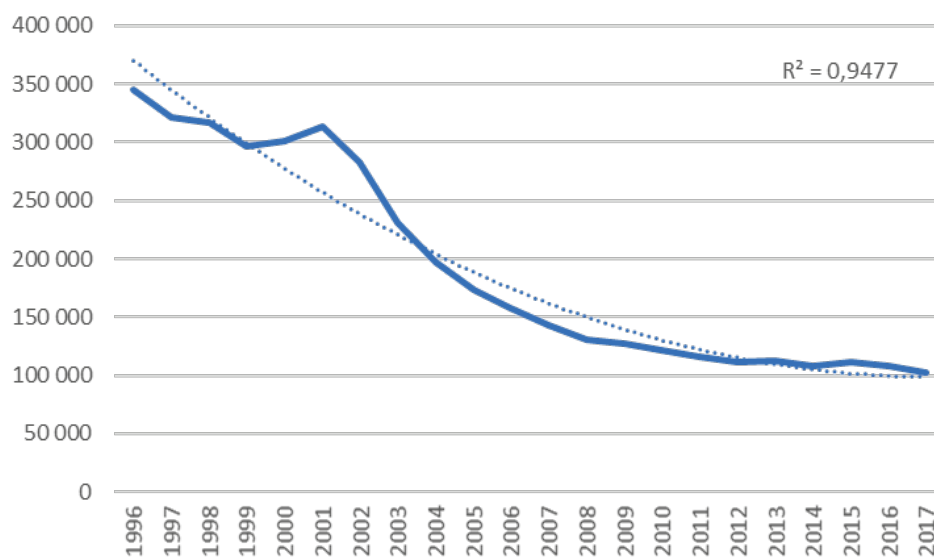
Taux pour 1 000 habitants 1996 = 3,6 ; 2017 = 3,4 ; pas de tendance significative sur la période.



Source : ministère de l'Intérieur, état 4001.

5 - Vols d'automobiles

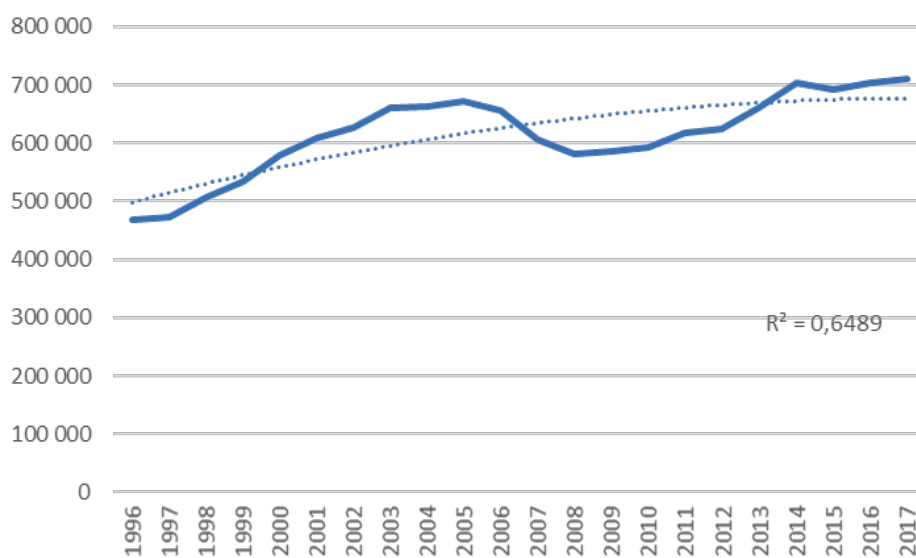
Taux pour 1 000 habitants 1996 = 6,0 ; 2017 = 1,5 ; baisse significative sur la période.



Source : ministère de l'Intérieur, état 4001.

6 - Vols simples

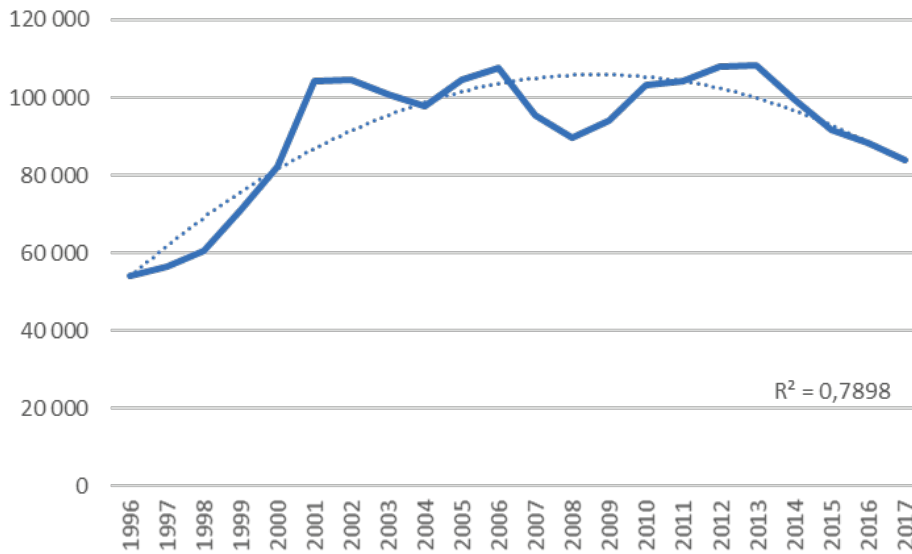
Taux pour 1 000 habitants 1996 = 8,1 ; 2017 = 10,6 ; hausse significative sur la période.



Source : ministère de l'Intérieur, état 4001.

7 - Vols avec violences

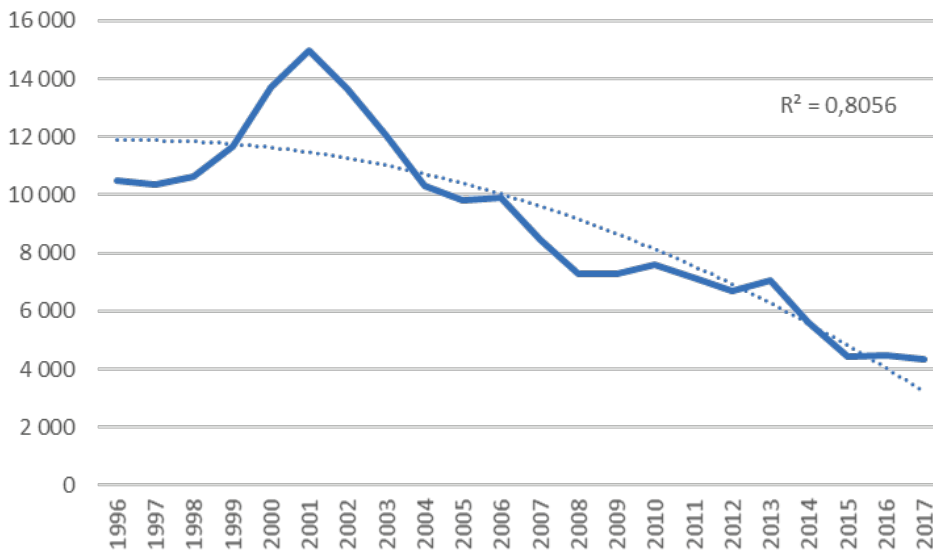
Taux pour 1 000 habitants 1996 = 0,9 ; 2017 = 1,2 ; hausse significative sur la période.



Source : ministère de l'Intérieur, état 4001.

8 - Vols avec armes blanches

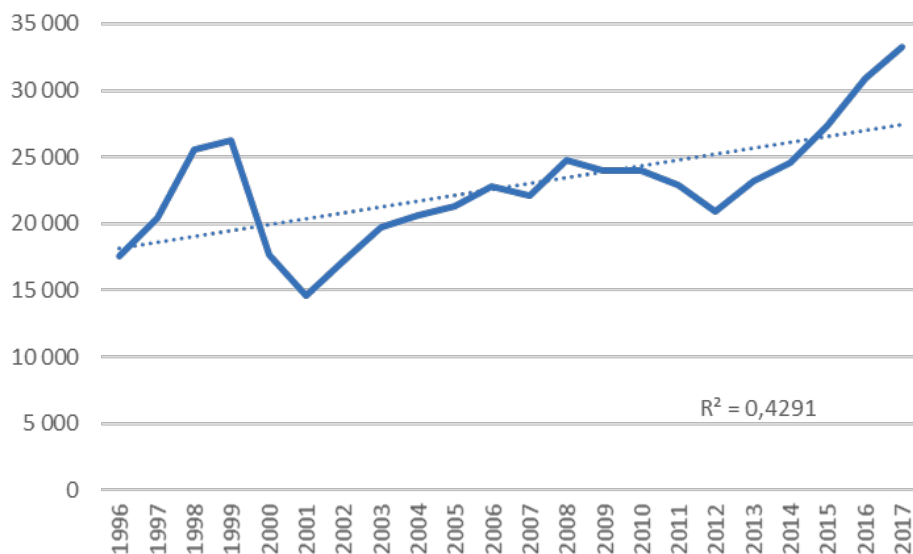
Taux pour 1 000 habitants 1996 = 0,2 ; 2017 = 0,1 ; baisse significative sur la période.



Source : ministère de l'Intérieur, état 4001.

### 9 – Trafic de stupéfiants et usage revente (infractions révélées à l'initiative des services)

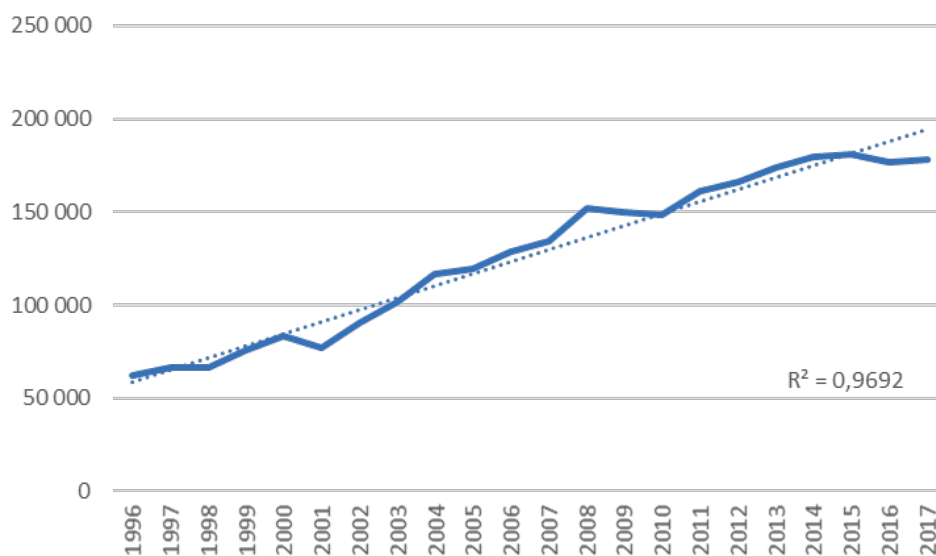
Taux pour 1 000 habitants 1996 = 0,3 ; 2017 = 0,5 ; hausse significative sur la période.



Source : ministère de l'Intérieur, état 4001.

### 10 – Usage de stupéfiants (infractions révélées à l'initiative des services)

Taux pour 1 000 habitants 1996 = 1,1 ; 2017 = 2,7 ; hausse significative sur la période.



Source : ministère de l'Intérieur, état 4001.

## Bibliographie

- APPLETON (R.), 2015, «Fresno police unveils state-of-the-art crime tracking system», *The Fresno Bee*, 7 Juillet.
- BAR-HEN (A.), 2018, « L'intelligence n'est ni artificielle ni innée », *The Conversation*.
- BENDLER (J.), BRANDT (T.), WAGNER (S.), 2014, *Investigating Crime to Twitter Relationships in Urban Environment of Human Behaviour*, Tel Aviv, ECIS.
- BENSOUSSAN (A.), 2019, « L'empathie artificielle de la personne robot », *Planete Robots*, Janvier-Février, Volume 55.
- BESSION (J.-L.), 2007, *Mesure du nombre de faits constatés d'atteintes volontaires à l'intégrité physique rapporté à la taille de la population présente en moyenne*, PARIS, ONDRP.
- BESSION (J.-L.), 2019, *La criminalité sur les territoires du Grand Paris*, Paris, INHESJ.
- BOVP, 2019, *Arrêté n° 2019-00079 autorisant l'installation du système de vidéoprotection de la préfecture de Police*, Paris, s.n.
- BRANTINGHAM & BRANTINGHAM, 1984, *Patterns in Crime*, New York, Macmillan.
- CAPLAN (J.-M.), KENNEDY (L.W.), PIZA (E.L.), BARNUM (J.D.), 2019, «Using Vulnerability and Exposure to Improve Robbery Prediction and Target Area Selection», *Applied Spatial Analysis and Policy*.
- CEPEJ, 2018, *Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires*, [En ligne] Available at: <https://www.coe.int/fr/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment> (accès le Septembre 2019).
- CHAN (J.) & BENNETT MOSES (L.), 2016, «Is Big Data challenging criminology? », *Theoretical Criminology*, p. 21-39.
- CHRISTENSEN (C.M.), RAYNOR (M.E.), 2013, *The Innovator's Solution: Creating and Sustaining Successful Growth*, Cambridge (Boston), Harvard Business Review Press.
- COHEN (L.E.), FELSON (M.), 1979, «Social Change and Crime Rate Trends: A Routine Activity approach», *American Sociological Review*, p. 588-608.
- CORNISH (D.), CLARKE (R.V.), 1986, *The Reasoning Criminal: Rational Choice Perspectives on Offending*, C&C éd. New York, Springer.
- ZIMRING (F.E.), 2011, *The City that Became Safe: New York's Lessons for Urban Crime and its Control*, Oxford, Oxford University Press.
- Eurostat, 2018, *Eurostat Statistics Explained* [en ligne] Available at: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime\\_statistics/fr#Les\\_vols\\_de\\_voitures\\_ont\\_diminu.C3.A9\\_de\\_36.C2.A0.25\\_entre\\_2008\\_et.C2.A02016](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime_statistics/fr#Les_vols_de_voitures_ont_diminu.C3.A9_de_36.C2.A0.25_entre_2008_et.C2.A02016) (accès le 24 novembre 2019).
- FERGUSON (A.G.), 2017, *The Rise of Big data Policing. Surveillance, Race and the Future of Law Enforcement*, New York, New York University Press.
- GERBER (M.S.), 2014, «Predicting crime using Twitter and Kernel Density Estimation», *Decision Support System*, p. 115-125.
- GOPNIK (A.), 2018, «The Great Crime Decline», *The New Yorker*, Issue 12 février.
- HARRIS (A.), 2002. *Research Finds that U.S Murder Rate Suppressed by Improved Emergency Medical Response*. [En ligne] Available at: <https://www.umass.edu/newsoffice/article/research-finds-us-murder-rate-suppressed-improved-emergency-medical-response> (accès le 24 novembre 2019).
- High-Level Expert Group on Artificial Intelligence, 2019, *Ethics Guidelines For Trustworthy Ai*, Bruxelles, Commission européenne.
- Home Office, 2019, *Home Office Counting Rules for Recorded Crime*, Londres, s.n.
- Insee-ONDRP-SSMSI, 2019, *Enquêtes « Cadre de vie et sécurité », 2007-2019*, Paris, INHESJ.
- INTERSTATS, 2018, *Insécurité et délinquance 2017 : premier bilan statistique*, Paris, ministère de l'Intérieur.
- JOUVENAL (J.), 2016, «The new way police are surveilling you: Calculating your threat "score"», *The Washington Post*.
- KEARNS (I.), MUIR (R.), 2019, *Data Driven Policing and Public Value*, Washington D.C., Police Foundation.
- KENNEDY (L.W.), CAPLAN (J.-M.), PIZA (E.L.), 2018, *Risk Based Policing: Evidence Based Crime Prevention with Big Data and Spatial analytics*, Oakland, University of California Press.
- KITCHIN (R.), 2014, «Big Data, new epistemologies and paradigm shifts», *Big Data & Society*, p. 1-12.

- LEE (Y.), ECK (J.E.), SOOHYN (O.), MARTINEZ (N.), 2017, «How Concentrated is Crime at Place? A systematic review from 1970 to 2015», *Crime Science*, Décembre.
- LUM (C.), KOPER (C.S.), TELEP (C.W.), 2011, «The Evidence-Based Policing», *Journal of Experimental Criminology*, Juillet, p. 3-26.
- MALLESSON (N.), ANDRESSEN (M.A.), 2015, «Spatio-temporal crime hot spots and the ambient population», *Crime Science*, Avril, p. 12-8.
- MASTROFSKI (S.D.), WILLIS (J.J.), 2011, «Police Organization», *The Oxford Handbook of Crime and Criminal Justice*, p. 479-508.
- MILGRAM (A.), 2014, *Pourquoi les statistiques sont des éléments clefs pour combattre le crime*, Vancouver, TED Institute.
- Ministère Intérieur, 2006, *Guide méthodologique projet de vidéoprotection*, Paris, Comité de Pilotage Stratégique pour le développement de la vidéoprotection.
- MU-HYUN (C.), 2020, Seoul to install AI cameras for crime detection: System will detect what passerby are wearing. Consulté 2020 sur : <https://www.zdnet.com/article/seoul-to-install-ai-cameras-for-crime-detection/>
- NICORA (H.), 2015, *Hitachi Data Systems Unveils New Advancements In Predictive Policing To Support Safer, Smarter Societies* [En ligne] Available at: <https://www.hitachivantara.com/en-us/news-resources/press-releases/2015/g1150928.html> (accès le 24 novembre 2019).
- OLLIGSCHLAEGER (A.M.), 1998, Artificial neural Networks and Crime Mapping, *Crime Mapping and Crime Prevention*, p. 313-347.
- ONDRP, 2018, *Victimation 2017 et perceptions de la sécurité*, Paris, INHESJ.
- ONDRP, 2019, *Victimation 2018 et perceptions de la sécurité*, Paris, INHESJ.
- O'NEIL (C.), 2016, *Weapons of Math Destruction. How Big Data Increases Inequality and Threaten Democracy*, Les Arènes éd., New York, New York Crown.
- PAGE (F.), 2017, *The inevitable rise of robocops*. [En ligne] Available at: <https://edition.cnn.com/2017/05/22/tech/robot-police-officer-future-dubai/index.html> (accès le 24 novembre 2019).
- PLACÉ (J.-V.), 2012, *Projet de loi de finances pour 2013 : sécurité (gendarmerie nationale et police nationale)* [En ligne] Available at: <https://www.senat.fr/rap/112-148-327-1/112-148-327-14.html>
- REAVES (B.A.), 2015, *Local Police Departments, 2013: Equipment and Technology*, Washington, Bureau of Justice Statistics (BJS).
- ROHAIDI (N.), 2019, *GovInsider* [En ligne] Available at: <https://govinsider.asia/innovation/ott-velsberg-estonia-chief-data-officer-ai-powered-government/> (accès le 24 novembre 2019).
- SHAW (C.R.), MCKAY (H.D.), 1942, *Juvenile Delinquency and Urban Areas: A Study of Rates of Delinquents in Relation to Differential Characteristics of Local Communities in American Cities*, Chicago, The University of Chicago Press.
- SHERMAN (L.W.), GARTIN (P.R.), BUERGER (M.E.), 1989, Hot spots of predatory crimes: Routine activities and the criminology of place, *Criminology*, p. 27-56.
- SUDWORTH (J.), 2017, *In Your Face: China's all-seeing state* [En ligne] Available at: <https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state> (accès le 24 novembre 2019).
- TREMBLAY (P.), CUSSON (M.), CLERMONT (Y.), 1992, « Contribution à une criminologie de l'acte : une analyse stratégique du vol de véhicules automobiles », *Déviance et société*, p. 157-178.
- UZBELGER (G.), 2018, *Conf@42 - 42 AI - IBM - Introduction à l'IA et le cognitif*. [En ligne] Available at: <https://www.youtube.com/watch?v=NGJyFXRNQeg>
- UZBELGER (G.), 2019, *Intelligence artificielle : état des lieux et enjeux principaux*, Paris, Colloque IA au défi de la sécurité et de la justice - INHESJ.
- VILLANI (C.) et al., 2018, *Donner un sens à l'intelligence artificielle*, Paris, s.n.
- WEISBURD (D.), ECK (J.E.), BRAGA (A.A.), 2016, *Place Matters: Criminology for the Twenty-First Century*, New York, Cambridge University Press.
- WILLIS (J.W.), MASTROFSKI (S.D.), WEISBURD (D.), 2007, Making Sense of COMPSTAT: A Theory-Based Analysis of Organizational Change in Three Police Department, *Law & Society Review*, 40(1), p. 147-189.
- YAN (L.), 2018, *Chinese police increase use of smart tech in arrests* [En ligne] Available at: <http://www.ecns.cn/2018/02-07/291784.shtml> (accès le 24 novembre 2019).

# Risk terrain modeling and the study of the physical determinants of criminal behavior

Alejandro GIMÉNEZ-SANTANA, Leslie W. KENNEDY, and Joel M. CAPLAN

*Rutgers Center on Public Security, Rutgers University*

## Introduction

À la fin des années 1820, André Michel Guerry (1802–1866) et Adolphe Quetelet (1796–1874) ont révolutionné la criminologie et la sociologie avec leur analyse détaillée des statistiques criminelles. Ils sont en effet considérés comme les précurseurs de ce qui sera, un siècle plus tard, dénommé ‘l’école écologique du crime’ (Elmer, 1933). Guerry & Quetelet ont ainsi eu un profond impact sur la réussite ultérieure de l’école de l’écologie urbaine de Chicago (Beirne, 1993). Ces deux statisticiens français sont particulièrement reconnus pour leurs premiers travaux (Guerry, 1833; Quetelet, 1835) qui ont contribué à cartographier la distribution spatiale du crime à travers les différentes régions de France. Il faudra attendre la publication de « La Criminalité à Paris » de Stanciu (1968) pour une première étude sur les effets de la structure des quartiers sur le crime, à Paris.

Dans son étude, Vasile Stanciu critique ouvertement l’utilisation des unités d’analyse plus larges qu’un pâté de maisons ou une portion de rue. Selon lui, toute unité d’analyse plus large peut produire des données infondées,

## Introduction

In the late 1820s, André Michel Guerry (1802–1866) and Adolphe Quetelet (1796–1874) revolutionized the study of criminology and modern sociology with their detailed account on criminal statistics. In fact, they are considered precursors of what a century later became known as the ecological school of crime (see Elmer, 1933). Not surprisingly, Guerry & Quetelet had a profound impact on the later success of the Chicago school of urban ecology (Beirne, 1993). Their early works (Guerry, 1833; Quetelet, 1835) resulted in the recognition of the two French statisticians for their contribution in mapping the spatial distribution of crime across different regions of France. It was not until Stanciu (1968) published his study of “La Criminalité à Paris” that Paris’s first comprehensive study on neighborhood effects on crime saw the light.

In his research, Vasile Stanciu openly criticized the use of larger units of analysis other than the city block or street segment. In his view, any unit of analysis larger than the street block could result in spurious findings,

### Alejandro GIMÉNEZ SANTANA



Alejandro Gimenez Santana est Docteur en Relations Internationales à l’Université de Rutgers où il est également doctorant au Département des

études internationales. Avant d’occuper le poste de directeur de projets, il a travaillé au Fonds pour la paix à Washington comme analyste en alertes et prévisions des risques puis comme coordinateur au Rutgers Center on Public Security (RCPS).

### Leslie W. KENNEDY



Leslie W. Kennedy est Docteur en sociologie de l’Université de Toronto. Il est Professeur à l’Université de Rutgers et enseigne également à la “School of Criminal

Justice”. Il l’auteur ou co-auteur de vingt ouvrages et écrit régulièrement dans les principaux publications de criminology et de droit pénal (*Criminology*, *Justice Quarterly*, *Journal of Quantitative Criminology*...).

### Joel M. CAPLAN



Joel M. Caplan est Docteur en Science politique de l’Université de Pennsylvanie et titulaire d’une maîtrise de droit pénal de l’Université de Rutgers.

Il est Professeur associé à la « School of Criminal Justice ». Il est l’auteur de deux ouvrages et a publié plus de 35 articles dans des revues à comité de lecture et plus de 10 monographies et chapitres d’ouvrages collectifs. Il siège aux comités de rédaction de trois revues à comité de lecture.



en raison de l'existence de différentes structures socio-économiques et comportementales à de plus larges échelles. Comme il le note (1968) : “Le brassage des groupes ne se fait que dans la même rue et encore pas sur l'ensemble de son parcours” (p. 12). Autrement dit, le comportement criminel est le résultat de l'environnement social immédiat, pas forcément le résultat du contexte de quartier.

Étonnamment, Stanciu a manqué l'opportunité, comme d'autres théoriciens écologiques, d'identifier les effets variés que l'environnement peut avoir sur la distribution spatiale du crime à Paris. Il a limité son analyse des facteurs criminogènes, ou de risque, à la présence des différentes situations de frustration, anxiété, pauvreté ou compétition. Par conséquent, l'influence spatiale de l'environnement physique n'a pas été prise en compte pour expliquer la présence de contextes criminogènes à Paris.

Près de deux siècles après les travaux de Guerry (1833) et Quetelet (1835), le débat continue sur l'effet de l'environnement physique et social sur la distribution du crime. D'un côté, les théoriciens écologiques (Shaw & McKay, 1942; Blau & Blau, 1982; Messner, 1982; Williams, 1984; Sampson, 1985; Hipp, 2007; Kelly, 2000) prétendent que des situations de désorganisation sociale et efficacité collective peuvent expliquer des variations de taux de crime. De l'autre côté, les théoriciens environnementaux (voir Brantingham & Brantingham, 1993; Cohen & Felson, 1979; Wortley & Mazerolle, 2008) prétendent que l'environnement physique est principalement responsable pour la création de situations uniques d'opportunité criminelle menant à des comportements déviants.

given the existence of differentiated socio-economic and behavioral structures in larger environments. As he noted (1968): “Le brassage des groupes ne se fait que dans la même rue et encore pas sur tout son parcours” (p. 12). In other words, criminal behavior is a byproduct of the immediate social environment, not necessarily the result of neighborhood contexts.

Surprisingly, Stanciu missed, as other ecological theorists did, the opportunity to identify the varying effects that the built environment has on the spatial distribution of crime in Paris. Instead, he limited his account of criminogenic factors to the presence of different contexts of frustration, anxiety, poverty, or competition. As a result, missing to account for the spatial influence of the physical environment to explain the presence of varying criminogenic contexts across Paris' landscape.

Nearly two centuries after the works of Guerry (1833) and Quetelet (1835), the debate continues over the effect that physical and social environments have on the distributions of crime. On the one hand, ecological theorists (Shaw & McKay, 1942; Blau & Blau, 1982; Messner, 1982; Williams, 1984; Sampson, 1985; Hipp, 2007; Kelly, 2000) claim that contexts of social disorganization and collective efficacy can explain variations in crime rates. On the other hand, environmental theorists (see Brantingham & Brantingham, 1993; Cohen & Felson, 1979; Wortley & Mazerolle, 2008) claim that the physical environment is primarily responsible in creating unique contexts of criminal opportunity leading to expressions of deviant behavior.



## Risk Terrain Modeling

In 2010, Joel Caplan and Leslie Kennedy developed risk terrain modeling (RTM) at the Rutgers Center on Public Security. This technique combines “key concepts from environmental criminology and spatial analysis, applied to the study of spatial vulnerabilities on crime outcomes” (Caplan & Kennedy, 2016, p. 11), thus allowing for the identification of micro-level locations presenting a high risk (i.e., spatial vulnerability) of victimization based on the spatial influences of a series of environmental factors.

The RTM method is rooted in the principles of environmental criminology (Wortley & Mazerolle, 2008) and risk assessment (Kennedy & Van Brunschot, 2009), allowing one to evaluate the influences of the physical environment’s crime attractors and generators (Brantingham & Brantingham, 1995). As noted by Caplan and Kennedy (2016), “RTM paints a comprehensive picture of the spatial dynamics of crime” (p. 90). It does so by modeling the spatial influences of an array of ecological features to determine the spatial association between these locations and past exposure to crime events. As discussed by Caplan (2011), understanding the spatial influence includes evaluating the relative effects of distance or the density of criminogenic features on crime occurrence. The RTM method allows one not only to identify the spatial distribution of risky places but also to weigh their relative risk on the dependent variable (i.e., violent crime event locations).

RTM’s analytical approach is supported by the theory of risky places (Kennedy & Caplan, 2012; Caplan & Kennedy, 2016), which postulates that the combined effect of spatial vulnerability (i.e., spatial influences that emanate from the built environment) and exposure to past crimes (e.g., areas with a concentration of past crime incidents) can yield actionable intelligence in the location of crime incidents. As noted by Kennedy et al. (2016, p. 3) in reference to the vulnerability-exposure framework, “incorporating exposure into a spatial vulnerability model helps to reduce the effects of false positives by considering the risks that past experience with crime present at vulnerable places,” thus indicating that crime is more likely to emerge at micro-level places that present a combination of past exposure (e.g., crime hot spots) and spatial vulnerability (e.g., environmental risk).

In 2013, the Rutgers Center on Public Security (RCPS) developed the first iteration of the RTMDx software (Caplan & Kennedy, 2018) with a revamped cloud-based version of the software launched in 2017. RTMDx automatizes the RTM process to produce an output list

of environmental risk features and their relative spatial influences on the outcome event (see Caplan, Kennedy, & Piza, 2013). This analytical process applies a precise set of statistical tests (see Caplan et al., 2013) to weigh and evaluate the relative importance of different risk factors that influence crime outcomes. First, the software builds an elastic penalized regression that assumes a Poisson distribution of events by using the cross-validation technique. Then, the model is further simplified via a bidirectional stepwise regression process that assumes a Poisson and a negative binomial distribution model to determine the “optimal fit” for the final RTM. This process calculates the Bayesian Information Criteria (BIC) of different candidate models by adding risk factors and re-measuring the BIC score at each iteration. As a result, the model with the lowest BIC score is selected as the “best candidate model.”

The resulting RTMDx output offers two main sets of information. The first is tabular data, and the second is the cartographic output for each significant risk factor within the final RTM model. The tabular output includes a relative risk value (RRV) for each significant risk factor that allows for comparisons to be made regarding the relative weight of risk factors within the model. These values are obtained by rescaling factor coefficients to obtain the relative weight of each risk factor. Lastly, tabular data offers information on the optimal operationalization and distance extent of spatial influences with the outcome event. As a result, RTM outputs offer a depiction of the spatial distribution of high-risk places throughout the study area. The distribution of high-risk places can be symbolized by displaying, on a map, all micro-level places (i.e., map cells) with a relative risk value (RRV) of two standard deviations over the mean (see Kennedy et al., 2016).

### Analyzing the physical determinants of violent crime in Paris, France

In the following example, the RTM technique was utilized to assess the spatial influences of a series of physical features, and how these features influence the risk of violent crime incidents in France’s capital, the city of Paris. As noted by the extant literature on crime and place, the presence of crime generators and attractors (CGAs) can contribute to creating criminogenic environments (see Bernasco & Block, 2011). Examples of CGAs included in the current analysis for Paris are schools (Roncek &

Faggiani, 1985), bars (Ratcliffe, 2012), hotels (Lebeau, 2011), parks (Groff & McCord, 2012), metro stations (Irvin-Erickson & La Vigne, 2015), and bus stops (Hart & Miethe, 2014). Each of these locations can contribute in increasing the likelihood of crime incidents in certain places.

As seen in Table 1, a total of 23 potential risk factors were tested using the RTMDx software against the location of 2012 violent crime incidents across Paris. All environmental factors were operationalized based on their spatial influence by proximity or density with a search radius that ranged from 150 meters to 450 meters (in increments of 150 meters). For instance,

car-sharing stations and post office locations were only operationalized as a function of their distance to the location of 2012 violent crime events; grocery stores and nightclubs were tested as a function of density or distance to the location of crime incidents.

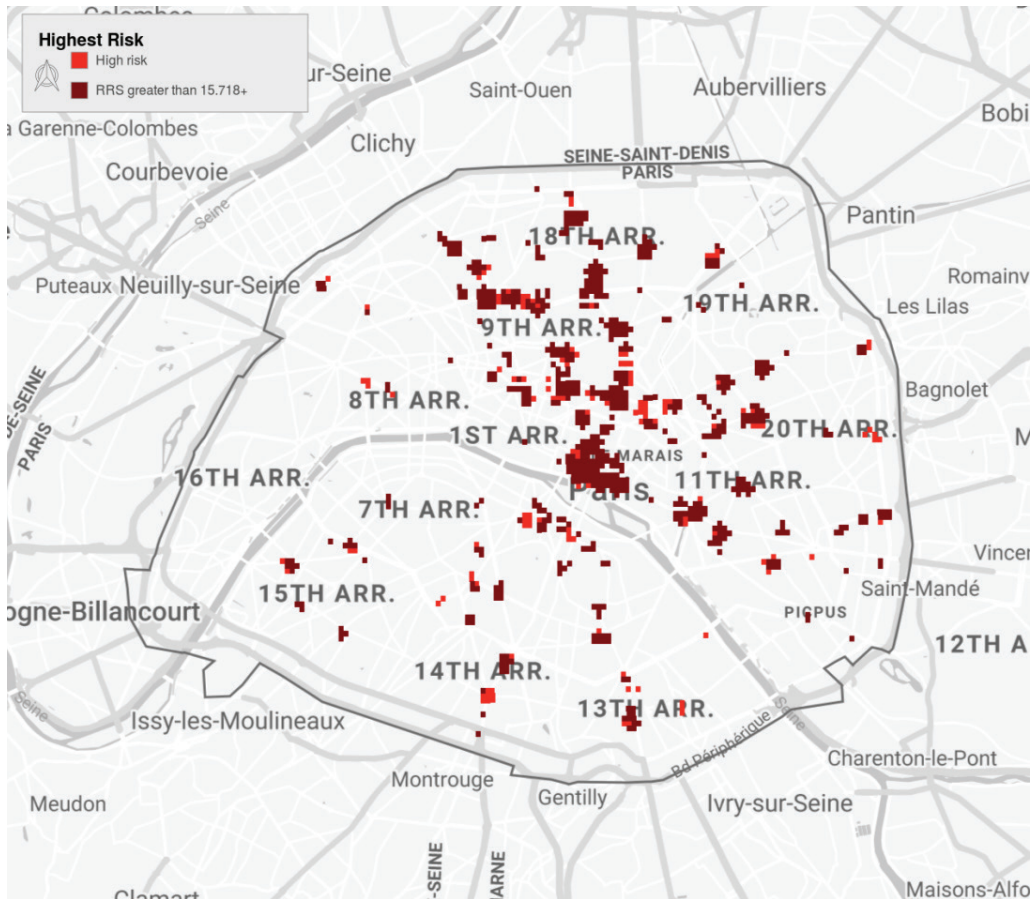
To model the spatial influences of all potential risk factors, the city was divided into a continuous surface GRID of 75 meter-by-75-meter cells ( $N=15,772$ ). The final RTMDx output found an RTM with a total of 11 statistically significant risk factors associated with the location of 2012 violent crime events. These risk factors included (ranked on the basis of their Relative Risk Value—RRV): Terraces (bars/clubs) and open-air stands<sup>2</sup>, fast food restaurants, coin-operated public restrooms, pharmacies,

Table 1. List of potential risk factors

Environmental Factors	N	Operationalization	Spatial Influence
Grocery stores	1260	Proximity and Density	Up to 450 meters (or up to 3 increments of 150 meters)
Bars and Nightlife	4448	Proximity and Density	
Low-cost Cafes (Café à 1 Euro)	178	Proximity and Density	
Car-sharing stations	113	Proximity	
Shops and Malls	36	Proximity	
Coffee Shops	3443	Proximity and Density	
Banks	2712	Proximity and Density	
Terrace / Outside seating areas / Stands	20893	Proximity and Density	
Fast food restaurants	113	Proximity and Density	
Gas Stations	144	Proximity and Density	
Post Office	210	Proximity	
Public Housing	2891	Proximity and Density	
Movie Theaters	86	Proximity and Density	
Parks and Public Gardens	511	Proximity and Density	
Pharmacies	1037	Proximity and Density	
Coin-operated public toilets (Sanisette)	395	Proximity	
Schools	1593	Proximity and Density	
Metro Stations	246	Proximity and Density	
Train Stations (RER and SNCF)	72	Proximity and Density	
Taxi Stations	120	Proximity	
Tourist Areas <sup>1</sup>	12	Proximity and Density	
Museum	37	Proximity and Density	
Bike-sharing Stations (Vélib)	68	Proximity and Density	

(1) Tourist areas were represented by 12 polygon-features of varying sizes.

Figure 1. RTM for violent crime (Paris, France)



grocery stores, low-cost cafes, schools, bars, public housing, metro stations, and post offices. The presence of these physical features creates unique spatial contexts that lead to varying expressions of deviant behavior. In this sense, locations within 150 meters of a bar terrace location in Paris presents a higher risk of victimization than any other places across the city of Paris. These risky locations offer an opportunity for offenders looking for potential victims that walk to or from these open space areas where people socialize. Similarly, places displaying a concentration of fast food restaurants were at a higher risk of violent crime victimization than other places not presenting the same attracting qualities. Therefore, at the micro level, these locations create unique contexts for victimization due to the presence of these environmental features across the city's landscape.

## Analyzing the physical determinants of violent crime in Bogotá, Colombia

A second example in the use of RTM can be drawn from a recent study by Giménez-Santana et al. (2018), which identified the micro-level variation of risky places across Bogotá's geography. The case for Bogotá is particularly relevant because of its existing socioeconomic stratification system. The stratification of Bogotá's dwellings allows to spatially analyze the city's social segregation patterns across socioeconomic groups within the city's neighborhoods. In Bogotá, the level of socioeconomic segregation is considerably higher than that of other world cities like Paris; making inequality patterns more pronounced and increasing the

(2) In Paris, retail businesses and bars/clubs require of a city permit to install terraces or stands/window displays. (<https://www.paris.fr/professionnels/l-entreprise-au-quotidien/terrasses-et-etalages-3516>)

distance between different social groups. According to a report from Bogotá's Planning Department (SDP)<sup>3</sup>, social segregation is reinforced by the spatial clustering of residents in distinct areas, effectively dividing social groups across class lines.

Bogotá's local government is directly responsible for measuring and periodically re-assessing stratum levels in the city through its Permanent Committee on Stratification which is formed by local government officials, representatives from utility companies, and other local stakeholders. According to Colombia's statistics department (DANE)<sup>4</sup>, the system of socioeconomic stratification is a mechanism that allows classifying people from different stratum levels or groups of people with similar social and economic characteristics, through the assessment of the physical characteristics of their dwellings, their immediate environment, and their urban context. It is important to note that the methodology used to calculate stratum level does not include any individual

or group assessment on income level. Thus, making this measure a purely environmental assessment of Bogotá's dwellings based on a series of locational and physical factors of the built environment.

The three major indicators, namely the physical characteristics of dwellings, the urban environment and the urban context; all constitute the basis for the existing socioeconomic stratification system in Bogotá. As a result, offering an ecological depiction of the built environment that is conducive to the level of socioeconomic development of entire neighborhoods. In this sense, dwellings located within lower stratum neighborhoods will lack access to proper roads or sidewalks, will not be paved and their façades will be unfinished or damaged, all of which can potentially generate unique contexts of criminal risk.

To spatially depict the geographic distribution of crime risk through Bogotá's geography, the city was subdivided

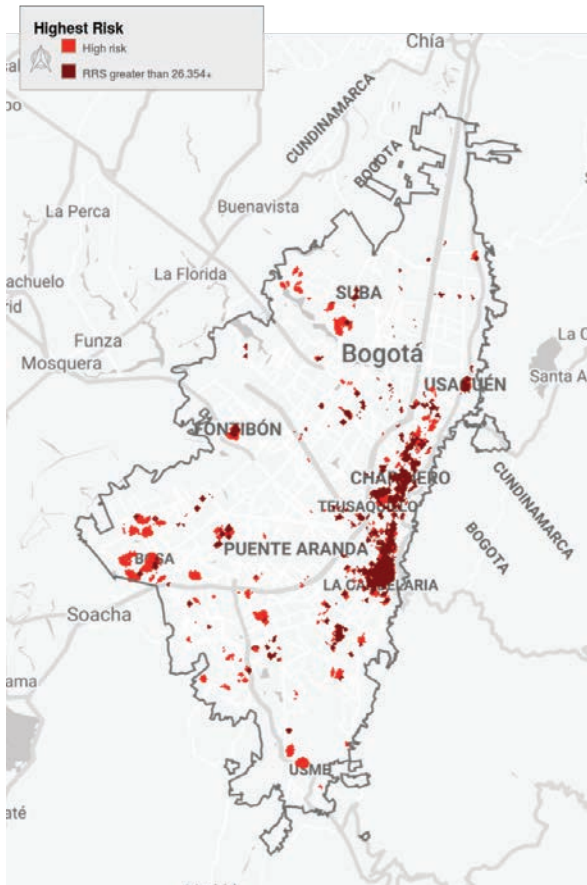
Table 2. List of potential risk factors

Environmental and Socioeconomic Risk Factors	N	Operationalization	Spatial Influence
Banks	1170	Proximity and Density	Up to 450 meters (or up to 3 increments of 150 meters)
Community Kitchens	320	Proximity and Density	
Higher Education Centers	151	Proximity and Density	
Hotels	413	Proximity and Density	
Tourist Areas	2024	Proximity	
Tourist Attractions	306	Proximity and Density	
TransMilenio Stations	145	Proximity and Density	
Drugstores	2526	Proximity and Density	
Medical Clinics	10554	Proximity and Density	
Motor Vehicle Bridges	2834	Proximity	
Pedestrian Only Bridges	2399	Proximity	
Public Hospitals	107	Proximity and Density	
Public Library	20	Proximity and Density	
Schools (Only Private)	1577	Proximity and Density	
Schools (Only Public)	920	Proximity and Density	
Low Strata	1251403	Proximity and Density	
High Strata	423579	Proximity and Density	

(3) <http://www.sdp.gov.co/portal/page/portal/PortalSDP/actualidad-SDP-home/LAESTRATIFICACION-BOGOTA-DIGITAL.pdf>

(4) [http://www.sdp.gov.co/portal/page/portal/PortalSDP/InformacionTomaDecisiones/Estratificacion\\_Socioeconomica/QueEs](http://www.sdp.gov.co/portal/page/portal/PortalSDP/InformacionTomaDecisiones/Estratificacion_Socioeconomica/QueEs)

Figure 2. RTM for Bogotá, Colombia



into a continuous surface GRID of 75 meter-by-75-meter cells ( $N=76,928$ ). The block size was set at 150 meters after assessing Bogotá's average city block size. According to Kennedy et al. (2015), a block size has a practical meaning as it is the most realistic unit the police can use to be deployed.

A total of 15 environmental variables and 2 socioeconomic variables were operationalized by their spatial influence, either by their proximity or density, to the location of 2012 violent crime incidents. The selection of these variables and their operationalization within the RTM framework were based on the visual inspection of each variable and their overlap with the location of 2012 violent crime incidents in a geographic information system (GIS). If a variable appeared (visually) to be concentrating near the location of crime events, this variable's spatial influence was operationalized for "density". However, if proximity (and not density) appeared to explain the overlap with

the location of crime incidents, then operationalization by "proximity" was selected. In those scenarios where these differentiations could not be "visually" established, the selection was made for both options. A full list of these environmental factors is presented in Table 2 with details on the number of observations for each variable ( $N$ ), the operationalization parameter used and the spatial influence applied during the analysis.

As per the results obtained from conducting an RTM analysis, a total of 13 risk factors were determined to be statistically significant within Bogotá's RTM model. A total of 76,928 cells of equal size<sup>5</sup> were created, each of which had a value ranging from 1 (lowest risk / no risk) to 134 (highest risk). As seen on Figure 2, a final RTM identified the downtown areas of Bogotá as presenting an aggravated risk for violent crime incidents. The results showed that low stratum units and drugstores were deemed to be the most important predictors for future violent crime incidents, with proximity to these locations presenting a risk of victimization two and three times higher<sup>6</sup> than any other location in the city. These results suggest that the location of these risky features at micro-level places throughout the city of Bogotá is responsible for creating unique contexts of violent crime victimization. In this regard, locations with a concentration of "low stratum" dwellings present an increased risk of victimization due to the attracting qualities (e.g., urban decay, unpaved roads, lack of proper public services, etc.) that these micro-level places pose compared to other places across the city of Bogotá.

## Discussion and Conclusion

These two examples illustrate how RTM can be applied across multiple jurisdictions throughout the world. The study of crime and place has undergone a series of major transformations over the last centuries. From the early works of Guerry and Quetelet in France to the research of Park and Burgess and of Shaw and McKay in the United States, the study of the spatial and temporal characteristics of crime has dramatically shaped the way in which crime research is conducted. The ecological school has played an essential role at identifying the presence of unique social contexts to explain the distribution of crime across communities and across jurisdictions. However, ecological theorists (see Park et al., 1925; Shaw & McKay, 1942;

(5) Each cell comprises an area of 5,625 sq. meters (75 m. \* 75 m.)

(6) Based on relative risk scores determined for low stratum units (RRV = 2.6) and drugstores (RRV = 1.9).

Sampson, 1985) have missed the opportunity to account for the spatial influence of the physical environment as a major contributing force driving expressions of criminal behavior.

Meanwhile, the area of research of environmental criminology (see Brantingham & Brantingham, 1993, 1995; Cohen & Felson, 1975; Cornish & Clarke, 1986) has proposed different theories that acknowledge the importance of the built environment and routine activities as major factors explaining the distribution of crime. Building from early works in environmental criminology and spatial analysis, the theory of risky places (Caplan & Kennedy, 2016) supports the interactive effect of the contexts of spatial vulnerability and past crime exposure in modeling the spatial dynamics of crime. These contexts of spatial vulnerability can be identified through the use of risk terrain modeling (RTM), an approach to spatial risk assessment that models the spatial influences of the built environment in creating unique behavior settings for criminal activity.

To date, the areas of research in environmental criminology and social disorganization have remained separated, with few studies including these two large theoretical frameworks into RTM research (see Drawve et al. 2016; Piza et al. 2017; Giménez-Santana, et al., 2018; Thomas and Drawve, 2018). Future research should address how unique physical and social contexts can explain the spatial distribution of violent crime rates across cities. In sum, future research should continue expanding the extant literature on neighborhood effects on crime by incorporating the areas of research of environmental criminology, spatial analysis, and the study of risky environments ■

## References

- Beirne, P. (1993). *Inventing Criminology: Essays on the rise of 'homo criminalis'*. SUNY Press.
- Bernasco, W., & Block, R. (2011). Robberies in Chicago: A block-level analysis of the influence of crime generators, crime attractors, and offender anchor points. *Journal of Research in Crime and Delinquency*, 48(1), 33-57.
- Blau, J. R., & Blau, P. M. (1982). The cost of inequality: Metropolitan structure and violent crime. *American Sociological Review*, 114-129.
- Brantingham, P. L., & Brantingham, P. J. (1993). Nodes, paths and edges: Considerations on the complexity of crime and the physical environment. *Journal of Environmental Psychology*, 13(1), 3-28.
- Brantingham, P. L., & Brantingham, P. J. (1995). Criminality of place. *European Journal on Criminal Policy and Research*, 3(3), 5-26.
- Caplan, J. M., & Kennedy, L. W. (2018). Risk terrain modeling diagnostics utility (Version 1.5). Newark, NJ: Rutgers Center on Public Security.
- Caplan, J. M., & Kennedy, L. W. (2016). *Risk Terrain Modeling: Crime Prediction and Risk Reduction*. University of California Press.
- Caplan, J. M., Kennedy, L. W., & Piza, E. L. (2013). Joint utility of event-dependent and environmental crime analysis techniques for violent crime forecasting. *Crime and Delinquency*, 59(2), 243-270.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.
- Cornish, D. B., & Clarke, R. V. (Eds.). (1986). *The reasoning criminal: Rational choice perspectives on offending*. New York: Springer.
- Drawve, G., Thomas, S. A., & Walker, J. T. (2016). Bringing the physical environment back into neighborhood research: The utility of RTM for developing an aggregate neighborhood risk of crime measure. *Journal of Criminal Justice*, 44, 21-29.
- Elmer, M. C. (1933). Century-old ecological studies in France. *American Journal of Sociology*, 39(1), 63-70.
- Giménez-Santana, A., Caplan, J. M., & Drawve, G. (2018). Risk Terrain Modeling and Socio-Economic Stratification: Identifying Risky Places for Violent Crime Victimization in Bogotá, Colombia. *European Journal on Criminal Policy and Research*, 1-15.

- Groff, E., & McCord, E. S. (2012). The role of neighborhood parks as crime generators. *Security Journal*, 25(1), 1-24.
- Guerry, A. M. (1833). *Essai sur la statistique morale de la France*. Paris: Crochard.
- Hart, T. C., & Miethe, T. D. (2014). Street robbery and public bus stops: a case study of activity nodes and situational risk. *Security Journal*, 27(2), 180-193.
- Hipp, J. R. (2007). Income inequality, race, and place: Does the distribution of race and class within neighborhoods affect crime rates? *Criminology*, 45(3), 665-697.
- Irvin-Erickson, Y., & La Vigne, N. (2015). A spatio-temporal analysis of crime at Washington, DC metro rail: Stations' crime-generating and crime-attracting characteristics as transportation nodes and places. *Crime science*, 4(1), 14.
- Kennedy, L.W. (1983). *The urban kaleidoscope: Canadian perspectives*. McGraw-Hill Ryerson.
- Kennedy, L. W., Caplan, J. M., Piza, E. L., & Buccine-Schraeder, H. (2015). Vulnerability and Exposure to Crime: Applying Risk Terrain Modeling to the Study of Assault in Chicago. *Applied Spatial Analysis and Policy*, 1-20.
- Kennedy, L. W., & Van Brunschot, E. G. (2009). *The Risk in Crime*. Rowman & Littlefield.
- Kennedy, L. W., Caplan, J. M., & Piza, E. (2011). Risk clusters, hotspots, and spatial intelligence: risk terrain modeling as an algorithm for police resource allocation strategies. *Journal of Quantitative Criminology*, 27(3), 339-362.
- Kennedy, L. W., Caplan, J. M., & Piza, E. L. (2018). *Risk-based policing: Evidence-based crime prevention with big data and spatial analytics*. University of California Press.
- Kelly, M. (2000). Inequality and crime. *Review of Economics and Statistics*, 82(4), 530-539.
- LeBeau, J. L. (2011). Sleeping with strangers: Hotels and motels as crime attractors and crime generators.
- Messner, S. F. (1982). Poverty, inequality, and the urban homicide rate: Some unexpected findings. *Criminology*, 20(1), 103-114.
- Park, R. E., Burgess, E. W., & McKenzie, R. D. (1925). *The City*. University of Chicago Press.
- Patterns, Prevention, and Geometry of Crime, 77-102.
- Piza, E., Feng, S., Kennedy, L., & Caplan, J. (2017). Place-based correlates of Motor Vehicle Theft and Recovery: Measuring spatial influence across neighbourhood context. *Urban Studies*, 54(13), 2998-3021.
- Quetelet, A. (1835). *Sur l'homme et le développement de ses facultés ou essai de physique sociale* (Vol. 1). Bachelier.
- Ratcliffe, D. (Ed.). (2012). *A nature conservation review: Volume 1: The selection of biological sites of national importance to nature conservation in Britain* (Vol. 1). Cambridge: Cambridge University Press.
- Roncek, D.W., & Faggiani, D. (1985). High schools and crime: A replication. *The Sociological Quarterly*, 26(4), 491-505.
- Sampson, R. J. (1985). Neighborhood and crime: The structural determinants of personal victimization. *Journal of research in crime and delinquency*, 22(1), 7-40.
- Shaw, C. R., & McKay, H. D. (1942). *Juvenile delinquency and urban areas: A study of rates of delinquents in relation to differential characteristics of local communities in American cities*. Chicago, Ill.: The University of Chicago Press.
- Stanciu, V. V. (1968). *La Criminalité à Paris*. Paris: Centre National de la Recherche Scientifique (Travaux du Centre d'Etudes sociologiques).
- Thomas, S. A., & Drawve, G. (2018). Examining interactive effects of characteristics of the social and physical environment on aggravated assault. *Journal of Criminal Justice*, 57, 89-98
- Williams, K. R. (1984). Economic sources of homicide: Re-estimating the effects of poverty and inequality. *American sociological review*, 283-289.
- Wortley, R., & Mazerolle, L. (Eds.). (2013). *Environmental criminology and crime analysis*. Willan Publishing.

# La clandestinité politique : balises pour un objet d'études émergent

Grégoire LE QUANG



## Grégoire LE QUANG



Grégoire Le Quang est docteur en histoire contemporaine, agrégé d'histoire

et ancien élève de l'École normale supérieure de Lyon. Actuellement enseignant dans le secondaire (collège de Pont-sur-Yonne, 89) et chercheur associé à l'IHTP (Paris 8-CNRS), il poursuit ses recherches sur la thématique des violences politiques et des terrorismes en Italie, de leur impact dans la société et de leur mémoire. Parmi ses publications récentes : « *La méfiance dans l'Italie des "années de plomb", entre peur et vigilance démocratique (1969-1981)* », *Tracés. Revue de Sciences humaines*, 2016, n° 31, p. 67-85 ; « *Résister à la peur : les mobilisations contre les terrorismes en Italie, de 1969 à 1980* », *Laboratoire italien. Politique et société*, 22, 2019 ; avec Virgile Cirefice, et Charles Riondet, il a dirigé *La part de l'ombre. Histoire de la clandestinité politique*, Ceyzérieu, Champ Vallon, 2019.

Les mouvements djihadistes contemporains, souvent analysés selon les paradigmes dominants de terrorisme, radicalisation ou dérives sectaires, incarnent avant tout des menaces clandestines. Sans dénier toute spécificité à chaque situation, une réflexion sur cette catégorie d'analyse, avec une profondeur historique mais dans une approche transdisciplinaire, apporte beaucoup pour comprendre les dynamiques de ces groupes, souvent armés, agissant dans une situation d'illégalité prolongée et de dissimulation. Ces enjeux renvoient à la fois à l'organisation de la subversion, à l'action de l'État et à la prolifération des imaginaires, à la fois politisés et lourds de conséquences politiques et sociales, liés à la figure de l'ennemi intérieur.

## Introduction

Malgré la diversité des contextes politiques, historiques et géopolitiques, le fait de se cacher dans le but de former une opposition à un pouvoir constitué est un choix lourd de conséquences – à la fois du point de vue des modalités stratégiques de l'action subversive et

du côté des méthodes de lutte développées par les services de sécurité<sup>1</sup>. La dissimulation apparaît comme une ressource, condition pour fomenter des actions d'autant plus spectaculaires qu'elles jouent d'un effet de surprise redoublé par le fait de se situer au cœur du territoire de l'ennemi et en dehors de toute guerre déclarée. Mais, d'un autre côté, la clandestinité est aussi une contrainte qui limite les possibilités de développement des organisations politiques, et entrave leur faculté à communiquer, à se financer ou à recruter des nouveaux membres.

(1) Cette réflexion repose à la fois sur ma recherche doctorale consacrée aux années 1970 en Italie [Le Quang, 2017] et sur un projet collectif issu d'une série de trois journées d'études, dont est tiré un ouvrage paru en octobre 2019 [Cirefice, Le Quang, Riondet, 2019]. Je remercie mes collègues et amis Virgile Cirefice et Charles Riondet, à qui la présente réflexion doit beaucoup.



Entrer dans l'illégalité et s'y maintenir : cette première définition, minimale, de la clandestinité peut s'appliquer à de nombreux mouvements ou groupes humains dans l'histoire, depuis les révoltés contre l'impôt en Judée romaine [Girardin, 2017], en passant par les nombreuses minorités religieuses ayant cherché à se protéger des persécutions au cours des siècles, jusqu'aux mouvements contemporains. Deux publications collectives, rassemblant des actes de colloques tenus l'un en 1977 [Audisio, Chiffolleau, Nathan-Tilloy, 1979], l'autre en 2006 [Aprile, Retaillaud-Bajac, 2008], constituent des jalons dans l'histoire comparée de ces attitudes très diverses, répondant à des motifs d'ordre politico-religieux, à des revendications d'indépendance ou de révolte contre un occupant, à une volonté de déclencher une dynamique révolutionnaire, mais pouvant également provenir de l'extrême droite. Pourtant, malgré leur importance, ces publications pionnières ne se donnent pas comme objectif d'envisager spécifiquement la clandestinité comme une variante de l'action politique, puisqu'elles sont élargies à toutes formes de dissimulation, voire d'illégalité, ce qui peut englober la quête spirituelle des ermites, la contrebande, la circulation d'imprimés érotiques ou la contre-culture gay.

Si l'on restreint donc la focale sur les formes clandestines d'action politique subversive, un ouvrage marque une véritable rupture : celui de la politiste italienne Donatella della Porta [2013], qui offre un premier essai de comparaison entre différents mouvements politiques clandestins de nature différente. L'intérêt de la problématique développée est qu'elle permet d'analyser de manière comparée un ensemble d'organisations politiques qui ressortent de catégories ou de concepts éloignés et rarement mis en dialogue : « résistance », « guérilla » ou « révolution », « terrorismes » ou « lutte armée », « mouvement de décolonisation », voire « guerre civile ». Sur cette lancée, au cours de ces dernières années, le prisme de la clandestinité est devenu le fil conducteur de recherches et de projets collectifs<sup>2</sup>. Il s'agit moins de proposer un concept alternatif à ceux, aux contours flous et discutés, de « terrorisme » ou de « radicalisation », que d'explorer les ouvertures permises par une catégorie d'analyse heuristique plutôt laissée en friche jusqu'à une date récente.

Comme souvent, l'actualité n'est pas étrangère à ce regain d'intérêt : la clandestinité s'est en effet imposée

comme la menace principale à même de déstabiliser des sociétés pacifiées ou non, sur tous les continents. S'il n'est nullement une nouveauté, le terrorisme ne cesse de gagner en puissance depuis deux décennies au moins [Ferragu, 2014 ; Raflik, 2016], et s'il prospère malgré les efforts stratégiques et technologiques considérables fournis par les services de sécurité, c'est bien parce que la clandestinité réussit à s'adapter aux mutations contemporaines. La menace clandestine n'est pourtant pas le fruit d'une évolution ultra contemporaine, et ne peut être assimilée au seul terrorisme. D'abord parce que les répertoires d'action clandestins ne sont pas exclusivement violents. Il peut y avoir des cas de dissimulation qui répondent aux persécutions<sup>3</sup>, et il existe également des exemples d'organisations de résistance essentiellement non violentes, comme celui de La Rose blanche dans l'Allemagne nazie<sup>4</sup>.

Ensuite, parce que certaines organisations clandestines ont commencé à jouer un rôle politique significatif au moins depuis le XIX<sup>e</sup> siècle. La Révolution française semble marquer un tournant, avec la multiplication de sociétés secrètes en lutte contre les despotismes, à l'échelle de l'Europe [Tardy, 2010 et 2015 ; Gainot, Serna, 2004]. Certaines organisations sont plus « discrètes » que véritablement clandestines, notamment la franc-maçonnerie : ses membres, souvent issus des élites politiques, dissimulent seulement une partie de leurs activités, sans vivre eux-mêmes dans un état de clandestinité, et les réunions peuvent être tolérées par les autorités. D'autres structures, comme la Charbonnerie, dont le système est plus pyramidal et en partie compartimenté, sont plus proches du fonctionnement de l'organisation clandestine [Lambert, 1995]. Mais c'est vers la fin du XIX<sup>e</sup> siècle que se situe la véritable rupture, autour des révolutionnaires russes et des anarchistes, même si les formes d'organisation de ces derniers sont débattues [Bouhey, 2008] : ce n'est plus seulement la nature de certaines activités qui est dissimulée, mais bien l'organisation elle-même, et, de plus en plus, l'existence de certains militants. La clandestinité s'impose donc progressivement du même coup comme une variante de ce que certains sociologues du politique nomment le « militantisme à haut risque »<sup>5</sup>.

C'est, du reste, à partir des premières années du XX<sup>e</sup> siècle seulement que se développe le substantif

(2) Se reporter aux publications récentes mentionnées en bibliographie. En outre, deux colloques ont eu lieu en 2018-2019 : « Êtres(s) clandestin(s) : expression et représentation », les 11 et 12 octobre 2018, à l'université de Dijon, et « Réseaux et pratiques de la clandestinité au temps des guerres de religion », le 12 juin 2019, à l'IEA de Paris.

(3) L'exemple d'Anne Frank est paradigmatique, mais pas isolé : voir par exemple le journal tenu par Moshé Flinker [2017].

(4) Cf. le témoignage d'Inge Scholl [2008].

(5) Notion théorisée en premier lieu par Doug McAdam [1986]. Voir aussi Sommier, 2015.

de « clandestinité », qui est attesté mais rare depuis le XVIII<sup>e</sup> siècle [Aprile, Retailaud-Bajac, 2008, p. 8]. C'est aussi de cette époque que date la première étude sociologique qui tente d'analyser le fonctionnement de ces organisations qui ne se contentent plus de dissimuler une partie de leurs actes mais « *pren [nent] le secret comme forme d'existence* » [Simmel, 1991, p. 63].

Dès lors, la question de l'organisation apparaît prépondérante. Alors que Donatella della Porta considère qu'il peut y avoir clandestinité isolée, en donnant l'exemple d'Anders Breivik [della Porta, 2013, p. 2], il paraît légitime de considérer que tout projet politique subversif dissimulé ne peut s'implanter sur le moyen ou long terme qu'en reposant sur un mouvement collectif, même minoritaire. Au-delà de l'existence de possibles actions clandestines, c'est plutôt la question de l'organisation et des moyens de développer un lien entre structure dissimulée et sphères politiques et sociales sympathisantes ou potentiellement alliées qui importe. Toute clandestinité n'apparaît, *in fine*, que relative, et n'existe que tant que dure l'invisibilité, aux yeux du pouvoir. Ses modalités sont donc variées et doivent être précisées.

## Cerner la lutte clandestine

### *Le choix de la clandestinité : une étape dans un processus de « radicalisation »*

La clandestinité politique peut être, de prime abord, reliée à un choix radical, qui résulte du refus sans concession d'accepter l'ordre politique en place. Les raisons du rejet de la légitimité de l'État sont variables, mais la légitimation de l'usage de la violence repose souvent sur la critique d'une violence systémique, rendue acceptable par des moyens jugés illégitimes [Guibet Lafaye, 2018]. Le processus d'acceptation des méthodes violentes lui-même renvoie à ce qu'on qualifie généralement de « radicalisation », même si ce concept reste flou et débattu [Guibet Lafaye, Rapin, 2017 ; della Porta, 2018].

Cet arrière-plan est capital à plus d'un titre. D'abord parce que le mouvement clandestin, s'inscrivant dans ces processus de radicalisation, concerne des individus souvent engagés dans ce que les sociologues nomment des « carrières » militantes [Bosi, della Porta, 2012 ; Bosi,

2016 ; Crettiez, Sèze, 2017]. L'analyse des trajectoires individuelles permet de saisir à la fois l'influence des déterminants familiaux et sociaux, ainsi que les indices d'une politisation qui permet de comprendre ce qui pousse certains individus à sauter le pas de la clandestinité, mais également tout ce qui peut représenter un obstacle ou un frein à cet engagement radical<sup>6</sup>. Cette perspective sociologique est incontournable dans le sens où elle démontre que la clandestinité est liée à un environnement militant, qui sert en même temps de vivier pour les recrutements, de support pour le financement et de soutien dans l'entreprise de dissimulation, et peut même présenter des situations de concurrence entre les différents groupes militants proches.

Le soutien des populations ou de certains groupes sociaux se matérialise de diverses manières, selon l'emprise territoriale, variable, des groupes armés clandestins, qui peut aller jusqu'à l'exercice d'une certaine forme de contrainte. C'est le cas des « impôts révolutionnaires » prélevés et parfois imposés sur certaines activités. Toutefois, il est à noter que l'évaluation de ce « soutien » est chose ardue – Isabelle Sommier remarque ainsi de manière lapidaire que « parler de soutien ne renvoie à rien de tangible » [Sommier, 2000, p. 81].

Certes, le consensus n'est pas mesurable quantitativement, et, si on considère un mouvement clandestin, d'autant plus s'il est violent, il est vain de parler d'« opinion publique » dans un sens monolithique. Pourtant, cette question ne peut être évacuée, ne serait-ce que parce que la conquête du soutien est un objectif capital des organisations politiques, y compris clandestines et y compris lorsque des méthodes terroristes sont employées : le but et l'horizon de la lutte subversive restent celui de construire une convergence, qui permette d'envisager une prise de pouvoir, ou à défaut une situation de conflit généralisé, voire de guerre civile. La clandestinité est ainsi souvent vue par les acteurs eux-mêmes comme une situation transitoire, un prélude à un bouleversement social et politique.

Quoi qu'il en soit, la clandestinité est une expérience minoritaire, même si son choix est revendiqué au nom d'un intérêt supérieur, et que les acteurs légitiment souvent leur activité illégale en référence à un groupe (le prolétariat, la Nation opprimée par l'étranger ou le colonisateur...). La seule convocation de ces idéaux permet de comprendre l'acceptation de la possibilité de donner la mort, ou du risque d'être tué ou emprisonné à vie. Les documents produits *a posteriori*, notamment les témoignages d'anciens

(6) C'est la perspective de l'ouvrage d'Isabelle Sommier [1998], tiré de sa thèse de doctorat.

militants, portent la trace de cet engagement total<sup>7</sup>. L'idéal de la mort en martyr, celui qui sacrifie à la « cause » sa vie personnelle et parfois sa vie tout court, irrigue le plus souvent les imaginaires des mouvements clandestins. Stephen Rindlisbacher le montre concernant les socialistes révolutionnaires dans l'Empire russe, qui circulaient avec des portraits des grandes figures de la lutte clandestine – Lénine lui-même ne se séparait jamais d'une image du révolutionnaire Tchernychevski, philosophe radical russe mort en 1889 [Rindlisbacher *in* Cirefice, Le Quang, Riondet, 2019, p. 132].

Dans un autre contexte, Hugo Melchior montre à quel point l'imaginaire héroïque que charrie l'expérience de la clandestinité peut jouer dans le choix même de la clandestinité, à partir de l'exemple d'une organisation qui n'a pas été concernée par la lutte armée : le Parti communiste marxiste-léniniste de France (PCMLF) [Melchior, 2017]. À l'annonce par de Gaulle, en juin 1968, de la dissolution d'une dizaine de groupes marxistes révolutionnaires, le PCMLF fait, seul, le choix de conserver le même nom et de passer à la clandestinité. Hugo Melchior démontre que cette décision a été autant une réponse à une contrainte répressive qu'un choix stratégique visant à démontrer, y compris par les militants eux-mêmes et par rapport à l'imaginaire révolutionnaire alors partagé, que l'organisation effectuait un saut qualitatif décisif. Alors même qu'il suffisait, comme l'a fait en particulier la Jeunesse communiste révolutionnaire (JCR), devenue Ligue communiste, de changer une lettre dans le sigle du groupe, le passage à une situation de clandestinité devient un marqueur identitaire qui a contribué à maintenir la fiction d'une avant-garde minoritaire mais conquérante, dissimulant la fonte réelle des effectifs militants au fil des ans. L'importance de cet imaginaire romantique de la clandestinité, qui masque les difficultés concrètes de la vie de l'ombre, est un élément important du prestige dont peuvent se prévaloir les organisations clandestines, qui stimule les vocations éventuelles.

### Contraintes et contradictions de l'état de clandestin

Mais la dissimulation permanente propre à la lutte clandestine est également un puissant facteur qui conditionne, négativement, cette modalité d'action militante. Sur le plan des contraintes matérielles, l'action



LA CONQUÊTE DU SOUTIEN EST UN OBJECTIF CAPITAL DES ORGANISATIONS POLITIQUES, Y COMPRIS CLANDESTINES ET Y COMPRIS LORSQUE DES MÉTHODES TERRORISTES SONT EMPLOYÉES : LE BUT ET L'HORIZON DE LA LUTTE SUBVERSIVE RESTENT CELUI DE CONSTRUIRE UNE CONVERGENCE, QUI PERMETTE D'ENVISAGER UNE PRISE DE POUVOIR, OU À DÉFAUT UNE SITUATION DE CONFLIT GÉNÉRALISÉ, VOIRE DE GUERRE CIVILE. LA CLANDESTINITÉ EST AINSI SOUVENT VUE PAR LES ACTEURS EUX-MÊMES COMME UNE SITUATION TRANSITOIRE, UN PRÉLUDE À UN BOULEVERSEMENT SOCIAL ET POLITIQUE.



clandestine est liée au développement d'un ensemble de techniques de dissimulation, sans lesquelles la survie est impossible : changer d'identité, adopter des pseudonymes (« noms de guerre »), des techniques de communication qui déjouent la surveillance, notamment par les déguisements, les faux papiers, les planques... Ces techniques peuvent d'ailleurs faire l'objet de transmissions : le cas des anciens résistants qui ont pu fabriquer des faux papiers en faveur des Algériens est connu [Gobin, 2017<sup>8</sup>]. Les contacts avec la criminalité sont fréquents, notamment en ce qui concerne la fourniture d'armes, parfois pour l'acquisition de compétences précises.

Dans la clandestinité, les méthodes développées pour échapper à la surveillance et augmenter les chances de survie individuelle et collective peuvent aller jusqu'à consommer la majorité du temps disponible. Ces caractéristiques sont mises en valeur par un tournant récent de l'histoire de la Résistance, qui s'inspire d'une approche anthropologique. L'ouvrage rédigé par Sébastien Albertelli, Julien Blanc et Laurent Douzou montre ainsi la diversité des expériences résistantes « *au ras de la quotidienneté clandestine* » [Albertelli (S.), Blanc

(7) Si on prend l'exemple des militants italiens des Brigades rouges, on peut se reporter avec profit au documentaire de Bianconi, 2007.

(8) Voir en outre l'exposition : Adolfo Kaminsky. Faussaire et photographe, du jeudi 23 mai 2019 jusqu'au dimanche 8 décembre 2019 au Musée d'art et d'histoire du judaïsme à Paris.

(J.), Douzou (L.), 2019, p. 11]. Bien loin d'une histoire héroïque consacrée, elle témoigne également de bien des tâtonnements, retournements de situation et prises de risque plus ou moins calculées. On retrouve le tableau de ces contraintes dans certains récits rétrospectifs d'anciens membres des Brigades rouges (BR) italiennes : Prospero Gallinari raconte ainsi son passage par un groupuscule totalement clandestin (Superclan), d'octobre 1971 à l'été 1972, précédant son entrée dans les BR ; quelques mois marqués par les séances de tir à la campagne, mais surtout l'ennui et la rareté des rencontres avec les « contacts » de l'organisation [Gallinari, 2006, p. 83]. Par ailleurs, la situation de tension et de fatigue domine, conduisant à un épuisement perceptible dans nombre de récits.

Une des conséquences essentielles de la clandestinité est l'isolement. La communication avec l'extérieur constitue bien évidemment un problème capital, ce qui bouleverse nécessairement la vie personnelle. Sauf exception, les militants qui passent à la clandestinité doivent rompre avec leur milieu d'origine : concernant les militants des BR, Mario Moretti rompt avec sa femme et ne voit plus son fils pendant dix ans [Moretti, Mosca, Rossanda, 1994], ainsi qu'Enrico Fenzi [Fenzi, 2008], Adriana Faranda se sépare de sa fille en bas âge [Bianconi, 2007]. Les rapports affectifs se font et se défont dès lors à l'intérieur de l'organisation. Mais la communication entre les différents militants présente également un caractère heurté et aléatoire, renforcé par l'usage des pseudonymes, le changement fréquent d'adresses, le cloisonnement en petites unités ne communiquant, dans l'idéal, que par un canal entre elles, souvent de manière hiérarchique. Ces pratiques sont aussi lourdes de conséquences sur le fonctionnement de l'organisation, favorisant souvent la constitution d'une structure verticale et autoritaire. Elles conduisent aussi à masquer une grande partie de la réalité de l'organisation aux militants eux-mêmes, ce qui a nécessairement un impact sur leur façon de se comporter au sein de celle-ci.

Enfin, la communication vers l'extérieur est limitée par la difficulté à diffuser un outil performant. Les publications clandestines peuvent réussir à se frayer un chemin sous le manteau, à condition de disposer d'un réseau de soutien étendu. C'est par exemple le cas des nombreuses publications durant la Résistance, dont les fameuses Éditions de Minuit. Pour de nombreux groupes clandestins, la communication peut passer par une technique plus artisanale : le graffiti, support essentiel pour démontrer l'importance du contrôle, au moins symbolique, sur le territoire revendiqué. Il en va ainsi aussi bien pour l'OAS, pour les groupes de lutte armée italiens, que pour les clandestins revendiquant un séparatisme

(ETA, IRA ou FLNC [Crettiez, Piazza, 2014]). Quoi qu'il en soit, ces canaux de communication sont toujours précaires, parfois considérés de manière péjorative.

Il est possible de pointer deux conséquences directes de cet isolement sur les modalités et les dynamiques du militantisme clandestin. D'une part, la clôture pourrait encourager les groupes clandestins à choisir un chemin toujours plus autoréférentiel. Comme l'écrit Donatella della Porta : « *plus les groupes sont radicaux, plus ils sont isolés de la culture des mouvements sociaux et plus leurs membres, en partageant les risques de leur militantisme, sont enclins à souscrire au schéma ami/ennemi* » [della Porta, 2013, p. 243]. De même, elle parle aussi d'un « *enfermement idéologique* » (*ideological encapsulation*), conduisant à l'extension d'une logique de guerre, qui, en particulier, légitime l'homicide, mais aussi le don total de soi. La déconnexion avec les mouvements collectifs ou contestataires qui peuvent partager une même culture et un même objectif mais choisissent de rester sur le plan de la légalité s'accroît, et devient source de polémiques grandissantes. C'est notamment le cas de l'isolement des BR en Italie au cours des années 1970, qui s'accroît à mesure que la clandestinité et la violence des actions progressent [Le Quang *in* Cirefice, Le Quang, Riondet, 2019].

L'autre conséquence possible qui dérive du choix de la clandestinité peut être un recours accru à la violence politique, voire à l'attentat. Pour conjurer le risque de la marginalisation, les groupes clandestins sont tentés de recourir à une stratégie médiatique qui vise à capter, parfois à monopoliser l'attention. Le terrorisme, dès lors, apparaît comme le moyen le plus efficace pour jouer sur la fascination-répulsion et l'engrenage du spectacle médiatique [Le Quang, 2017]. Même s'il n'existe aucun modèle, ni aucune trajectoire linéaire, force est de constater que les principaux groupes clandestins qui ont su résister à l'érosion sont ceux qui ont le mieux su occuper le terrain des médias et mettre en scène l'affrontement contre les puissances de l'État. L'exemple du Front de libération nationale corse (FLNC) démontre que cela peut passer autant par la mise en scène d'une symbolique militariste que par l'exercice concret de la violence : il s'agit avant tout d'incarner un contre-pouvoir en acte, et en image [Pietrera, *in* Cirefice, Le Quang, Riondet, 2019]. Ces processus d'escalade dépendent aussi en partie de la réaction des autorités.

## Dénoncer et/ou propager la menace clandestine

### *L'usage politique de la figure du clandestin : du complot à l'ennemi intérieur*

L'action répressive influe grandement sur la dynamique des mouvements sociaux, et les organisations clandestines n'échappent pas à la règle. Mais l'action des responsables politiques et des forces de police est elle-même le révélateur, et en partie la source, de puissantes représentations des phénomènes clandestins. Quelques caractéristiques émergent des différents imaginaires véhiculés par la clandestinité.

En premier lieu, la description des mouvements clandestins (dans le discours médiatique, politique) renvoie le plus souvent à l'image d'une menace intérieure, dans une logique de radicalisation de la figure de l'ennemi. À ce titre, il faut remarquer que le terme de « clandestin » n'est jamais ni revendiqué, ni appliqué comme catégorie d'analyse par les contemporains. Ceux-ci parlent de « brigands » ou de « terroristes », qui sont le plus souvent représentés comme des agents de l'étranger, des ennemis de l'intérieur. À ce titre, les organisations clandestines catalysent souvent des peurs spécifiques, en particulier celles qui sont liées à la menace de guerre civile. Ces peurs sont renforcées par l'inconnu, la difficulté à cerner les contours des mouvements clandestins, souvent à l'origine de phantasmes, qui s'attachent par exemple aux lieux de la clandestinité, eux-mêmes supports de représentations alimentant la suspicion (caves, greniers, maquis, banlieues...).

Mais la question des représentations liées à la clandestinité est également indissociable de l'usage de ces représentations par les pouvoirs. Face à une contestation souterraine d'intensité variable, les autorités sont de grands pourvoyeurs de ces mêmes représentations péjoratives, pouvant déboucher sur de véritables mythes politiques. Cette dimension rejoint l'analyse des imaginaires du « complot », que Frédéric Monier propose de distinguer de la « conspiration », qui renvoie à la pratique politique (organisation d'un coup d'État), et de la « conjuration », associée à la dimension mythique ou imaginaire (ce qu'on appellerait dans la langue d'aujourd'hui « théorie du complot »). Le « complot », lui, renvoie au discours des instances répressives et de l'État [Monier, 1998, introduction]. Un des premiers exemples d'instrumentalisation d'une menace clandestine est donné par la série d'attentats dirigés contre le

premier consul, Napoléon Bonaparte, engagé dans une stratégie de renforcement de pouvoir personnel. De juillet à décembre 1800, de nombreuses violences visent la personne de Bonaparte, notamment la conspiration dite « des poignards », le 10 octobre 1800, et l'attentat dit de « la machine infernale », le 24 décembre de la même année. Alors que le premier est probablement un coup monté par la police et que le deuxième est l'œuvre de royalistes, ces violences politiques sont interprétées comme le signe que les jacobins continuent de constituer une menace souterraine, par le biais d'associations criminelles clandestines [Salomé, 2010 ; Lignereux, 2012]. Des jacobins ou d'anciens révolutionnaires sont d'ailleurs emprisonnés ou déportés. Il y a donc une exploitation politique de la menace, qui peut être fortement amplifiée, parfois même inventée de toutes pièces pour justifier une politique répressive : la peur est aussi un moyen de gouverner [Robin, 2006], et l'imaginaire véhiculé par l'action clandestine y contribue en général puissamment.

Cette rhétorique visant à stigmatiser les clandestins peut donc s'intégrer à une logique de criminalisation de l'opposition politique. Un bon exemple est donné par la perception et l'instrumentalisation de la menace communiste dans l'après-guerre : les débats sur la « cinquième colonne » formée par les partis communistes, considérés comme à la solde de Moscou et donc dirigés en sous-main par l'étranger, sont alimentés par une suspicion permanente de double jeu : ces partis en apparence démocratiques ne seraient que des façades d'organisations paramilitaires cachées [Codaccioni, 2013 ; Girard, 2014]. Ces débats sur l'existence d'un plan révolutionnaire des communistes, dans les années 1950 en particulier, n'habitent pas seulement les franges les plus radicalement anticommunistes, mais nourrissent aussi des rhétoriques électorales de partis au pouvoir, comme, en Italie, la Démocratie chrétienne. Notons que ces représentations liées au péril révolutionnaire peuvent conserver des prolongements inattendus, réactivés en dehors de toute vraisemblance : en témoigne par exemple l'arrestation de ce qui a été décrit par les autorités et la plupart des médias comme le « groupe de Tarnac » en 2008. Le procès qui s'est tenu en 2017 et 2018 a, pourtant, démontré l'inanité de l'accusation de constitution d'une bande armée clandestine ayant des visées terroristes.

### *De l'imaginaire du clandestin à la théorie du complot*

Il ne faudrait pourtant pas surévaluer l'importance des actions institutionnelles sur la formation des imaginaires liés aux organisations clandestines. En



LES INTERPRÉTATIONS DU FAIT CLANDESTIN, PASSÉ OU PRÉSENT, RESTENT UN TERRAIN PRIVILÉGIÉ D'AFFRONTEMENTS IDÉOLOGIQUES ET DE POINTS DE VUE CONTRADICTOIRES. EN UN SENS, LES DISCOURS COMLOTISTES PEUVENT ÊTRE CONSIDÉRÉS COMME DES COROLLAIRES DE L'ACTION CLANDESTINE. PUISQUE L'ACTION EST DISSIMULÉE, ELLE PRÊTE LE FLANC À DES DÉFORMATIONS : CHAQUE DÉTAIL, ET PARFOIS CHAQUE HASARD PEUVENT ÊTRE INTERPRÉTÉS COMME LE SIGNE D'UNE MANIPULATION, LE PLUS SOUVENT ATTRIBUÉE À L'ÉTAT OU À UNE PUISSANCE ÉTRANGÈRE.



effet, ces représentations échappent d'une certaine manière largement à la sphère de la communication. Les interprétations du fait clandestin, passé ou présent, restent un terrain privilégié d'affrontements idéologiques et de points de vue contradictoires. En un sens, les discours complotistes peuvent être considérés comme des corollaires de l'action clandestine. Puisque l'action est dissimulée, elle prête le flanc à des déformations : chaque détail, et parfois chaque hasard peuvent être interprétés comme le signe d'une manipulation, le plus souvent attribuée à l'État ou à une puissance étrangère.

Le cas des groupes armés révolutionnaires des années 1970 est, à nouveau, éclairant : en France, en Italie ou en Belgique, ces groupuscules sont accusés dans nombre de publications d'être manipulés par des services secrets étrangers. Dans tous les cas, ces analyses aboutissent à une décrédibilisation aussi bien de l'État, accusé de laxisme, voire de complaisance, que des clandestins eux-mêmes, réduits au statut de marionnettes dénuées d'autonomie politique [Dubuisson *in* Cirefice, Le Quang, Riondet, 2019 ; Santalena, 2009]. En Italie, cette « diétrologie<sup>9</sup> » est

même un véritable champ littéraire (plus que scientifique), qui relie les attentats commis aussi bien par l'extrême droite (ceux de la « stratégie de la tension ») que par des groupes armés révolutionnaires au contexte international, au climat de Guerre froide et à la manipulation des services de l'État [Rayner, 2008]. Si la complicité de certains services de l'État italien avec des poseurs de bombes néofascistes est amplement prouvée, il n'en reste pas moins que la recherche d'un unique commanditaire, véritable serpent de mer de cette ligne interprétative, la réduction à une série de manœuvres occultes et la défiance érigée en dogme envers toute forme d'institution dessinent les contours d'une sorte de clandestinité « au carré » : derrière les organisations clandestines se dissimulerait une main invisible qu'il faudrait à son tour déceler.

L'action clandestine, on le voit, est un puissant incubateur de ce qu'on nomme de manière peut-être trop générique et stigmatisante les « théories du complot » – mais cette tendance à la défiance et à la recherche d'une explication simpliste et alternative n'est ni neuve ni née d'Internet. Ce qui est invisible, ce qui est seulement entrevu, suscite à la fois peurs et phantasmes, qui entrent en collision avec l'origine mystérieuse et sacrée du pouvoir. Mais ces représentations comportent un risque de perte de lisibilité et doivent être analysées avec un surcroît de critique, puisqu'elles rejouent en réalité des partitions bien connues, qui ne font que reproposer des figures d'ennemis intérieurs tapis dans l'ombre.

Un bon exemple de cette mobilisation des fausses évidences au service de la construction d'une menace clandestine : la manière dont le concept de « taqiya » s'est imposé dans les principaux médias de l'espace francophone depuis les attentats parisiens de 2015 : cette notion d'origine savante, renvoyant à une justification théologique de la dissimulation de la foi musulmane en contexte de persécutions, ne désigne concrètement aucune technique spécifiquement musulmane. Le mot reste pourtant utilisé de manière récurrente comme une allusion à un ensemble de nouvelles techniques de lutte clandestine<sup>10</sup>. Même une enquête sociologique fouillée comme celle menée par le sociologue Fabien Truong, qui montre que la plupart des parcours de terroristes issus des quartiers défavorisés sont l'aboutissement de longues carrières de délinquance, propose ce terme sans vraiment le questionner [Truong, 2017, p. 192]. Le mot attend encore de voir son contenu scientifique précisé,

(9) *Dietrologia* : de *dietro*, ce qui se situe derrière, est caché.

(10) Un exemple parmi beaucoup d'autres : « Taqiya : la dissimulation comme nouvel art de la guerre », Vladimir de Gmeline, *Marianne*, 23 juillet 2016.

s'il en possède véritablement un ; mais il recouvre déjà, son succès le prouve, exactement les contours de la peur larvée d'une invasion terroriste clandestine, celle qui ne dit pas son nom mais qui attend son heure.

## Conclusion

Toujours d'actualité et au service de groupes clandestins animés de desseins violents, la dissimulation d'activités politiques subversives a réussi à se réinventer et à emprunter de nouveaux véhicules, technologiques en particulier, pour contourner les mécanismes de prévention et de surveillance, et pour recruter. Preuve que l'imaginaire du combattant de l'ombre reste puissant, qu'il attire ou qu'il épouvante. À l'heure où certains craignent l'errance d'une partie des Européens partis en Syrie et orphelins de Daech, à l'heure où un « *retour progressif à la clandestinité* » est prôné par certains dirigeants [Thomson, 2016], il apparaît toujours plus nécessaire d'effectuer un retour critique sur les métamorphoses contemporaines de la clandestinité, qui, au-delà des clichés et des simplifications, reste au cœur de l'économie de la violence induite par le terrorisme contemporain.

Au terme de cette exploration, qui n'a aucune prétention à l'exhaustivité, plusieurs jalons apparaissent, qui permettent de rendre quelque profondeur à cette problématique extrêmement actuelle mais non sans précédents. D'abord, si les organisations clandestines restent si puissantes, c'est parce qu'elles sont en mesure de cristalliser un certain imaginaire héroïque, fait à la fois d'exaltation de la force et de don de soi. Réside aussi dans l'exhibition de la force, voire de la brutalité et jusqu'à la barbarie, la démonstration d'un pouvoir supérieur et sans limite qui vise à s'imposer partout, y compris face aux démocraties. L'espoir d'inverser le cours de l'Histoire, d'imposer une revanche paraît un point commun de ces expériences militantes radicales.

Les groupes clandestins sont rarement capables de démontrer d'importantes capacités de destruction. C'est davantage un combat symbolique de (dé)légitimation qui s'engage, et, d'un côté comme de l'autre, c'est le motif de la « guerre juste » qui prédomine. Il serait bon, plutôt que de céder au confort et d'entonner ce refrain, de chercher à expliquer ce qui reste, pourtant, injustifiable ■

## Bibliographie

- AUDISIO (G.), CHIFFOLEAU (J.), NATHAN-TILLOY (M.) (eds.), 1979, *Histoire et clandestinité : du Moyen-Âge à la Première Guerre mondiale*, Albi, Ateliers Professionnels de P.O.S.J.
- APRILE (S.), RETAILLAUD-BAJAC (E.) (eds.), 2008, *Clandestinités urbaines : les citadins et les territoires du secret, XVI<sup>e</sup>-XX<sup>e</sup>*, Rennes, Presses universitaires de Rennes.
- BIANCONI (L.), 2007, *Do you remember Revolution*, Bibliothèque publique d'information.
- BOSI (L.), DELLA PORTA (D.), 2012, «Micro-mobilization into Armed Groups: Ideological, Instrumental and Solidaristic Paths», *Qualitative Sociology*, 35-4, p. 361-383.
- BOSI (L.), 2016, *Vite di lotta armata : storie di attivismo nelle Provisional IRA*, Rome, Carocci.
- BOUHEY (V.), 2008, *Les Anarchistes contre la République. Contribution à l'histoire des réseaux sous la Troisième République (1880-1914)*, Rennes, PUR.
- CIREFICE (V.), LE QUANG (G.), RIONDET (C.) (eds.), 2019, *La part de l'ombre. Histoire de la clandestinité politique*, Ceyzérieu, Champ Vallon.
- CODACCIONI (V.), 2013, *Punir les opposants : PCF et procès politiques, 1947-1962*, Paris, CNRS éd.
- CRETTEZ (X.), PIAZZA (P.), 2014, *Murs rebelles : iconographie nationaliste contestataire Corse, Pays basque, Irlande du Nord*, Paris, Karthala.
- CRETTEZ (X.), SÈZE (R.) (eds.), 2017, *Saisir les mécanismes de la radicalisation violente*, Rapport pour la mission de recherche Droit et Justice/INHESJ/CESDIP.
- DELLA PORTA (D.), 2013, *Clandestine political violence*, Cambridge, Cambridge University Press.
- DELLA PORTA (D.), 2018, «Radicalization: A Relational Perspective», *Annual Review of Political Science*, 21-1, p. 461-474.
- FENZI (E.), 2008, *Armes et bagages : journal des Brigades rouges*, Paris, Les Belles lettres, p. 210.

- FERRAGU (G.), 2014, *Histoire du terrorisme*, Paris, Perrin.
- FLINKER (M.), 2017, *Carnets de clandestinité : Bruxelles, 1942-1943*, Paris, Calmann-Lévy.
- GALLINARI (P.), 2006, *Un contadino nella metropoli : ricordi di un militante delle Brigate Rosse*, Milan, Bompiani.
- GAINOT (B.), SERNA (P.) (eds.), 2004, *Secret et République : 1795-1840*, Clermont-Ferrand, Presses Universitaires Blaise Pascal.
- GIRARD (P.), 2014, « La perception de la menace communiste, en France et en Italie au début de la Guerre Froide », in BUTON (P.), BÜTTNER (O.), HASTINGS (M.) (eds.), *La Guerre froide vue d'en bas*, Paris, CNRS Éditions.
- GIRARDIN (M.), 2017, *L'offrande et le tribut : la représentation de la fiscalité en Judée hellénistique et romaine (200 av. J.-C.-135 apr. J.-C.)*, thèse pour le doctorat d'histoire, non publiée, université de Lorraine.
- GOBIN (C.), 2017, *Genre et engagement : devenir « porteur.e de valises » en guerre d'Algérie (1954-1966)*, thèse pour le doctorat d'histoire, non publiée, Université Lumière-Lyon 2.
- GUIBET LAFAYE (C.), RAPIN (A.-J.), 2017, « La "radicalisation" : individualisation et dépolitisation d'une notion », *Politiques de communication*, 8-2.
- GUIBET LAFAYE (C.) (ed), 2018, *Une juste violence ?*, numéro de la revue *Parlement [s]*, n° 28.
- LAMBERT (P.-A.), 1995, *La charbonnerie française, 1821-1823 : du secret en politique*, Lyon, PUL.
- LE QUANG (G.), 2017, *Construire, représenter, combattre la peur : la société italienne et l'État face à la violence politique des « années de plomb », 1969 - 1981*, non publiée, université Paris 8 Vincennes-Saint Denis et université de Macerata (Italie).
- LIGNEREUX (A.), 2012, « Le moment terroriste de la chouannerie : des atteintes à l'ordre public aux attentats contre le Premier Consul », *La Révolution française. Cahiers de l'Institut d'histoire de la Révolution française*, 1, en ligne.
- MELCHIOR (H.), 2017, « Le militantisme révolutionnaire à l'heure de la clandestinité dans les années 1968 », *Vingtième Siècle. Revue d'histoire*, 133, p. 39-54.
- MCADAM (D.), 1986, « Recruitment to High Risk Activism: the Case of Freedom Summer », *American Journal of Sociology*, 92, p. 64-90.
- MONIER (F.), 1998, *Le complot dans la République : stratégies du secret de Boulanger à la Cagoule*, Paris, La Découverte.
- MORETTI (M.), MOSCA (C.), ROSSANDA (R.), 1994, *Brigate rosse : una storia italiana*, Milan, Anabasi.
- RAFLIK (J.), 2016, *Terrorisme et mondialisation : approches historiques*, Paris, Gallimard, 2016.
- RAYNER (H.), 2008, « Les théories du complot dans les interprétations du terrorisme en Italie : la prégnance du point de vue cryptologique », in GARGIULO (G.), SEUL (O.) (eds.), *Terrorismes : l'Italie et l'Allemagne à l'épreuve des années de plomb (1970-1980), réalités et représentations du terrorisme*, Paris, M. Houdiard, p. 162-193.
- ROBIN (C.), 2006, *La peur, histoire d'une idée politique*, Paris, Armand Colin.
- SALOMÉ (K.), 2010, « L'attentat de la rue Nicaise en 1800 : l'irruption d'une violence inédite ? », *Revue d'histoire du XIX<sup>e</sup> siècle*, 40, p. 59-75.
- SANTALENA (E.), 2009, « La figure controversée de Mario Moretti, entre histoire et suspicion », colloque Littérature et « temps des révoltes » (Italie, 1967-1980), 27, 28 et 29 novembre 2009, Lyon, ENS LSH, en ligne.
- SIMMEL (G.), 1991 [1908], *Secret et sociétés secrètes*, Circé.
- SCHOLL (I.), 2008, *La Rose Blanche*, Paris, Éd. de Minuit.
- SOMMIER (I.), 1998, *La violence politique et son deuil : l'après 68 en France et en Italie*, Rennes, Presses universitaires de Rennes.
- SOMMIER (I.), 2000, *Le terrorisme*, Paris, Flammarion.
- SOMMIER (I.), 2015, « Sentiments, affects et émotions dans l'engagement à haut risque », *Terrains/Théories*, n° 2, en ligne.
- TARDY (J.-N.), 2010, « Le flambeau et le poignard », *Revue d'histoire moderne et contemporaine*, n°57-1, p. 69-90.
- TARDY (J.-N.), 2015, *L'Âge des ombres. Complots, conspirations et sociétés secrètes au XIX<sup>e</sup> siècle*, Paris, Les Belles Lettres.
- THOMSON (D.), 2016, *Les revenants*, Paris, Le Seuil, p. 290.
- TRUONG (F.), 2017, *Loyautés radicales. L'islam et les « mauvais garçons » de la Nation*, Paris, La Découverte.



# À quoi sert le terrorisme ?

## Les effets du terrorisme islamiste sur les musulmans de France (2015-2019)

Manuel SAN PEDRO

Largement virtuel au regard des décès violents en France, le terrorisme islamiste des années 2015-2019 constitue avant tout une procédure psychologique visant à modifier la société. Il oblige l'État à réagir dans l'urgence et contribue à promouvoir une césure mentale entre les musulmans et les autres. Il a, de fait, provoqué des changements de comportement observables chez les musulmans de France, en particulier parmi les plus jeunes. Le traitement médiatique des attentats a ainsi été l'accélérateur, sinon le déclencheur d'une fermeture vis-à-vis des sources d'information communes.

Sur fond de mise en insécurité, les musulmans ont connu une autre fermeture, celle de l'expression, verbale et non verbale, surtout vis-à-vis des représentants de l'État. Alors que les musulmans font a priori confiance aux institutions, la politique antiterroriste a provoqué dans cette population défiance, peur et rejet.

Le terrorisme est l'agent d'un repli informationnel, cognitif et surtout émotionnel. À la congruence des extrêmes voulue par les terroristes s'ajoute donc un risque de divergence entre les citoyens musulmans et les autres non seulement dans le domaine des comportements observables, mais surtout dans le domaine qui est le véritable champ de bataille du terrorisme, à savoir l'imaginaire, ciment d'une nation.

Depuis janvier 2015, les attentats terroristes ont suscité de nombreuses études sur l'islam de France qui ont apporté des éclairages intéressants et renouvelé les problématiques concernant la deuxième religion de France. Mais peu de travaux ont cherché à comprendre l'impact spécifique de ces actions sur

la population musulmane. Ainsi, dans quelle mesure les musulmans sont-ils visés et est-ce au même titre que les autres citoyens ? Comment sont-ils affectés par le terrorisme et ce qu'il engendre ? Cette étude fait le point sur la réception par les musulmans de France des attentats qui y ont été accomplis au nom d'un islam intégral.

### le terrorisme : « une technologie de l'imaginaire »

#### Qu'est-ce que le terrorisme ?

Sa définition pose problème en raison de son caractère multiforme et des implications idéologiques de la question. On a ainsi recensé 23

définitions allant de l'acte isolé aux bombardements massifs, renvoyant à des actions de résistance comme à des actes répressifs [Huyghe, 2002, p. 37-47]. Devant ce foisonnement, une définition simple, et opérante, sera retenue. Si le droit français définit le terrorisme par une longue liste d'infractions (atteintes aux biens et aux personnes, blanchiment, etc.), le Code pénal (art. 421-1) est précis quant à ses *objectifs* : « une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public ». Le terrorisme cherche donc à troubler l'équilibre du corps social. Comment cette partie du corps social constituée par les musulmans de France a-t-elle été affectée par cette tentative de déstabilisation ?

#### La rationalité du terrorisme

Une réflexion superficielle envisage le terrorisme comme l'action barbare

#### Manuel SAN PEDRO



Manuel San Pedro est enseignant en histoire. Il a travaillé sur les représentations collectives face au crime (« L'assassinat du conjoint à Paris au XVIIIe siècle ») et est actuellement auditeur à l'École Pratique des Hautes Etudes.



et inutile de personnes dévoyées. Militairement, son impact est nul : les terroristes ne s'attaquant pas aux infrastructures militaires. Du point de vue des pertes, son impact est également négligeable : 281 décès et 1 059 blessés depuis 2000. Toutefois, à l'instar de Raymond Aron [1962, p. 176], il faut distinguer les pertes civiles et matérielles des effets psychologiques, « *bors de proportion avec ses effets purement physiques* ». Loin d'être sauvage et anarchique, la violence est « *barbare rationnellement* ». En effet, le terrorisme doit produire un spectacle et on peut dire qu'il ne vise qu'à cela en premier lieu [Mannoni, 2005]. La violence spectaculaire est la voie royale d'accès aux médias, et « le succès d'une opération dépend presque entièrement de la publicité qu'elle obtient » [Laqueur, 1979, p. 120]. Dans cette logique, le véritable enjeu n'est pas l'exposition aux dangers réels, mais ce qu'on pourrait appeler « *l'exposition aux médias* ».

L'écho médiatique constitue donc « *la véritable onde de choc* » de celui-ci [Bonardi & Mannoni, 2003, p. 55-72], si forte qu'elle oblige l'État à formuler une réponse plus forte et plus spectaculaire que dans d'autres domaines. Produisant de puissants effets sur le psychisme collectif, le terrorisme provoque des réponses conscientes et inconscientes. Comme le souligne François-Bernard Huyghe [2002, p. 40], les attentats « *consistent à faire et à dire pour faire dire et faire faire* ». Le terrorisme force la pensée et l'action.

## Les objectifs du terrorisme islamiste

L'objectif final des terroristes est englobant et remonte au moins à Sayyed Qutb (1906-1966), pour lequel le but de tout combattant musulman est la *hakkimiyya*, la souveraineté politique de Dieu. Plus près de nous, Rachid Kassim, mentor en 2016 de plusieurs attentats, affirme : « *L'islam est une religion de puissance. Quand le peuple applique cette religion, il est impossible de le coloniser [...] Tout le reste ne nous intéresse pas* » [Puchot & Caillet, 2017]. Pour ses acteurs, loin des explications sociologisantes, les causes du terrorisme plongent dans la théologie musulmane, et ses fins ne sont que religieuses, même s'il suit des étapes. Ainsi *Gestion de la barbarie* (3) recommande de perpétrer des actes barbares, pour provoquer un cycle de violence-répression qui poussera les musulmans vers le califat. Il s'agit également d'humilier symboliquement les États et de les épuiser économiquement et militairement. L'effondrement moral, jugé capital, permettra d'instaurer l'islam [Naji, 2007].

Ce travail de sappe concerne le monde médiatique, véritable champ de bataille. Aura lieu tout d'abord une « capitulation morale », commençant par « *l'abjecte capitulation des chaînes de télévision* », qui démultiplient l'effet dévastateur du spectacle terroriste. De leur côté, les spectateurs « consomment » et par là même, « réclament » ce spectacle, auto-entretenant ainsi le phénomène. De

fait, par sa dépendance aux images, la population est solidaire du terrorisme, dans un syndrome de Stockholm généralisé [Hoffman, 1999, p. 246-247].

À long terme, l'objectif est de changer les comportements en se servant de la terreur – à la fois moyen et fin – et en agissant « *comme une procédure d'influence dans la perspective de subvertir le pouvoir en place et d'accaparer psychologiquement les populations* » [Mannoni, 2005, p. 64]. Cet objectif est souvent atteint : bien que moins grave que d'autres problèmes, le terrorisme vient en tête des préoccupations des Français. « *Il y a donc un consentement au terrorisme* » [Mannoni, 2003, p. 5]. Le changement de comportement attendu par les terroristes est d'abord d'ordre anthropologique. Le premier *Que sais-je ?* consacré au terrorisme, rédigé par un ethnologue, le définissait comme « *un combat selon l'imaginaire* » [Servier 1979, p.75]. Le terrain choisi par les terroristes est bien celui des mentalités. Pierre Mannoni [2004, p. 152] affirme : « *le terrorisme apparaissait bien comme une procédure psychologique agissant essentiellement par des idées sur des idées et il était cohérent de demander à la psychologie d'en rendre compte. Ainsi encore s'est élaborée notre hypothèse de travail selon laquelle le terrorisme nous a semblé pouvoir être défini comme un laboratoire de la peur ou, si l'on préfère, comme une technologie de l'imaginaire* ».

La victoire des terroristes est d'avoir placé dans les esprits un nouveau cadre de pensée, le leur. Le terrorisme est devenu une croyance autonome, devant amener chacun à réfléchir en termes religieux (sacré, blasphème, etc.) dans une société pourtant sécularisée. Comme l'affirme Pierre Mannoni [2003, p. 5], « *l'influence psychologique et sociale des attentats reviendrait en somme, sinon à une question de foi, sinon de croyance* ».

La langue elle-même est colonisée. C'est par le terrorisme que sont entrés dans la langue commune des mots tels que *djihad*, *shari'a*, *kalifat*, avec leur orthographe propre. Cette « coranisation du français » est dangereuse parce qu'elle est imposée par les attentats, et dans les termes choisis par les seuls terroristes. Ainsi, ce sont « les termes du débat » qui nous sont imposés via la violence. Soulignons avec humour que si on lit au contraire le *Recueil d'avis juridiques* du Conseil européen des fatwas émis par Tariq Ramadan et Yusûf Al-Qaradhawi, pourtant rigoristes, on n'y trouvera que des textes écrits dans un français parfait, dans lesquels Allah est remplacé par Dieu [Salazar, 2015, p. 66-69]. Les médias sont plus royalistes que le roi, puisqu'ils reprennent des mots, et donc des concepts appartenant au Califat. De fait, ils s'en font les vecteurs, voire les promoteurs dans la société, et *a fortiori* parmi sa composante musulmane.

Les djihadistes veulent donc transformer, « dès l'action terroriste », la société sécularisée dans laquelle nous

vivons, mais leur force d'impact se mesure surtout aux réactions qui prolongent les attentats.

## Les résultats : un impact non négligeable

### L'efficacité des terreurs collectives

Les psychopathologies collectives induites par l'exposition des citoyens aux médias relatant les actes terroristes sont loin d'être négligeables. Si la peur est un phénomène circonscrit aux jours qui suivent un attentat, l'impact le plus durable concerne une série d'affects négatifs (anxiété, hyper-attention, état de fatigue généralisé) [Mannoni, 2004, p. 87]. Cet emballement du système représentationnel conduit à une névrose obsidionale collective. Il s'agit à ce stade d'un « *conditionnement spirituel et idéologique* » jouant comme force de dissuasion, symbolique ou réelle : qui s'aventurerait aujourd'hui à caricaturer Mohammed ? Les terroristes sont ainsi des « *coupeurs de langue* ».

Ce conditionnement modifie aussi notre perception de l'État, atteint dans son prestige symbolique. La terreur classique, noble et garante de l'ordre public, est totalement subvertie. Désormais les djihadistes se revendiquent comme les « Soldats de la Terreur » [Al-Hayat, 2015, 2015, p. 17], s'arrogeant le monopole de la violence spectaculaire (exécution) [Bonardi & Mannoni 2003, p. 55-72]. « *Les terroristes ne seraient, de ce point de vue, que nos modernes porteurs de mort, dont la fonction profonde, inconnue d'eux, serait de faire contre eux l'union « sacrée » du groupe, rôle tenu dans le passé par les dévants de tout acabit : ils seraient les sorciers de notre temps* » [Mannoni, 2003, p. 5]. Or, c'est par les peurs que chacun accède à sa propre civilisation, la terreur collective étant la matrice d'un peuple [Elias, 1939]. Mais cette redéfinition s'opère ici dans les termes imposés par l'action violente et spectaculaire.

Les actes terroristes obligent la population à prendre parti, et créent une division entre un « Nous » et un « Eux », plus ou moins consciemment. Jean Birnbaum [2018, p.13] a montré de façon magistrale comment cette césure opère : « *Nous justement qui sommes si réticents à dire "Nous" parce que tracer un nous c'est forcément délimiter une frontière avec "Eux", au risque d'exclure, de discriminer [...] Un nous de toutes origines et de toutes sensibilités, qu'il faut se garder de claquemurer dans des limites arbitraires, mais dont il est urgent de laisser émerger les contours en posant la question : à quoi tient-il, ce nous ? À quoi tenons-nous ?* » Parmi les victoires symboliques du terrorisme se trouve l'apparition ou la revivification de l'idée, consciente ou non, que l'on s'en défende ou pas, qu'il peut exister au sein de la société une ligne de fracture, réelle, imaginaire ou à venir : les pointillés sont ainsi tracés.

Enfin, de tels actes « obligent », ce qui est en soi une victoire terroriste. Jean Delumeau [1978] affirme que ce qui rassure face à la peur est qu'une action soit « possible ». Mais ici l'action de l'État est un « besoin », et non une politique.

### La réponse du gouvernement et des médias aux stimuli terroristes : l'irrationalité ?

Le discours médiatique, largement en phase avec celui des autorités lors des semaines qui ont suivi les attentats, a déployé plusieurs réponses. Celle donnée d'emblée par le gouvernement est contenue dans les premiers mots de François Hollande devant le Congrès, le 16 novembre 2015 : « *Nous sommes en guerre* ». L'analyse de la presse confirme ce cadrage du discours, avec les mots « *allié* », « *cible* », « *combat* », « *conflit* », « *ennemi* », « *stratégie* », etc. Le mot est décliné : « *guerre civile* », « *sainte* », « *de civilisations* », « *totale* » [Tozzo, 2016, p. 80-82]. Avec le bombardement de positions djihadistes en Syrie, la réponse effective du pouvoir fut en phase avec le discours, mais pas entièrement avec le réel. Les terroristes étaient des citoyens français ou belges, entraînés au Levant, mais radicalisés avant leur départ. La racine du problème se trouvait ici, et non en Syrie. Or, que nous apprennent les études sur les terroristes ? Tout d'abord, qu'ils appartiennent à un profil récurrent, presque un cliché, mais qui renvoie bien à la sociologie. Il s'agit d'hommes, ayant entre 20 et 30 ans, presque toujours français (ce qui interroge la notion de guerre), issus de fratries nombreuses au père absent (mort, séparation) et à la mère très effacée. Ils appartiennent à la deuxième génération d'immigrés issus de l'ancien empire colonial, ou sont convertis. Déjà connus des services de police, souvent pour délinquance, leur niveau d'études tourne autour du baccalauréat, mais tous ont un travail. La radicalisation semble être relativement rapide [Robert, 2017, p. 1]. Si l'on considère un groupe plus large de djihadistes, leur pratique religieuse a été plus longue et s'est radicalisée avec le temps. Certains parmi les terroristes les plus aguerris avaient déjà été condamnés pour association de malfaiteurs en relation avec une entreprise terroriste (AMT) ou pour des délits de droit commun [Hecker, 2018, p.21-22].

Le deuxième cadrage concerne les rapports entre terrorisme et immigration. De nombreux médias ont repris, volontairement ou non, l'idée que l'immigration arabo-musulmane pose problème, avec des interventions parfois hostiles à l'islam. Ici intervient ce que Gilles Kepel nomme par ailleurs le phénomène de « *congruence* » : sans les mettre sur le même pied, il constate que le discours anti-immigration et anti-islam, d'une part, et celui des djihadistes, d'autre part, présentent des homothéties :

« *Ils s'articulent avec l'édification de barrières, identitaires ou communautaires, qui excluent l'autre à partir d'éléments ontologiques : ethno-racial contre religieux, vrais Français contre faux Français, bon musulman contre apostat ou mécréant* » [Kepel, 2016, p. 106]. Cette montée parallèle des extrêmes constitue un objectif avoué des terroristes et fait directement écho à la dichotomie entre un « Eux » et un « Nous » ; mais ici les frontières, jusque-là en pointillé, sont à présent remplies, et de façon conflictuelle.

Le troisième cadrage concerne le souhait d'une société apaisée et inclusive. Le discours anti-amalgame est ici prégnant et sincère chez une grande partie de la population. En effet, les villes qui ont défilé pour *Charlie* sont celles qui ont le moins de préjugés racistes [Zerhouni, Rougier, & Muller, 2016, p. 69-76]. Cependant ce discours généreux secrète malgré lui l'apparition d'une altérité : l'islam de France est perçu comme un corps spécifique, un *opt-group*, lui-même divisé entre des « bons » et des « méchants ». Pas d'amalgame avec les terroristes donc, mais sentiment que l'islam français est un corps à part. Enfin, le discours des médias laisse apparaître une territorialisation de la menace : la banlieue est nommément présentée dangereuse et hors du territoire de la République [Tozzo, 2016, p. 101 et 106-110].

L'action terroriste vise à promouvoir dans la société, et parmi les musulmans en particulier, l'idée qu'il existe deux groupes dissemblables et en voie de séparation. Mais dans quelle mesure les musulmans de France vivent-ils cette fracture ?

### Les effets du terrorisme dans la population musulmane de France

Elle constitue à double titre la « population cible » des terroristes. D'abord parce que les djihadistes veulent l'embrigader et la réislamiser, et ensuite parce que l'objectif djihadiste est de déclencher des pogroms antimusulmans, ou du moins une attitude sociale et légale antimusulmane, le tout servant de prélude à une guerre civile.

### Les Français musulmans face au terrorisme : « la grande épreuve »

D'emblée, le Conseil français du culte musulman (CFCM) et ses composantes ont condamné les attentats, appelant à manifester le 11 janvier 2015, UOIF<sup>1</sup> compris malgré sa plainte contre *Charlie Hebdo*. Le Rassemblement des musulmans de France (RMF), alors majoritaire au CFCM,

a demandé d'élever une prière à la France chaque vendredi [Geisser *et alii*, p. 45-46]. La volonté d'intégration a ainsi été démontrée. Les musulmans ne feraient ainsi que suivre le même processus d'intégration-méfiance que les juifs en leur temps [Cohen, 2000, p. 89 à 120 ; Dieckhoff, 1990, p. 168-169]. Longtemps gênée par toute référence nationale, la communauté musulmane évolue à l'occasion des attentats. Nabil Ennasri, proche du Qatar, présent à un rassemblement devant le Bataclan, avec drapeau tricolore et hymne national improvisé, en décrit les étapes : « *Il y a un infléchissement du discours chez les jeunes : ils s'affichent sans complexe comme Français et musulmans. [...] Il y a encore quatre ou cinq ans, je n'assumais pas ce côté identitaire français. Il y a même dix ans, c'était plutôt l'inverse : je crachais sur la France du fait de son histoire coloniale. Aujourd'hui, j'assume* » [Geisser *et alii*, p. 43].

Parallèlement, le premier contrecoup des attentats fut une augmentation des actes antimusulmans : 429 actes ont été recensés en 2015, contre 133 en 2004 [Geisser *et alii*, 2017, p. 262], touchant les femmes voilées et les lieux de culte (50 % des 2 450 lieux recensés en France passant sous protection). Enfin sont apparus des messages haineux sur le Net, ce qui est une nouveauté. Mais en général, ces réactions épidermiques s'éteignent au bout de quinze jours [Galland & Muxel s.d., 2018, p. 164] et, sur la durée, on remarque une évolution positive aussi bien dans l'opinion publique que dans l'opinion musulmane. Entre *Charlie* (7 janvier 2015) et l'assassinat du père Hamel (26 juillet 2016), les attentats deviennent de plus en plus inacceptables pour la communauté musulmane et suscitent de moins en moins d'actes islamophobes. Cela est notable chez les jeunes : si 24 % des lycéens musulmans interrogés ne condamnaient pas totalement les attentats de janvier 2015, ce taux descend à 13 % pour le Bataclan. Qualitativement, leur discours établit une différence entre les victimes de *Charlie* (« *Ils l'ont cherché* ») et celles du Bataclan (« *Ils étaient tranquilles* ») [Galland & Muxel, 2018, p. 169]. Entre 2015 et 2019, l'opinion publique se montre globalement plus favorable envers les musulmans, mais dans le détail, elle fait de plus en plus la différence entre les pratiques religieuses privées de mieux en mieux acceptées et des pratiques publiques considérées de plus en plus gênantes [Geisser *et alii*, 2017, p. 254-255]. Politiquement, les attentats ont fortement accru l'exigence sécuritaire, y compris chez les musulmans [Ragazzi *et alii*, 2018, p. 50]. Cette exigence a augmenté à droite par colère et à gauche par peur. Enfin, l'attitude envers les non-musulmans est échelonnée en fonction d'un gradient de proximité, la peur augmentant avec la distance physique ou sociale [Geisser *et alii*, 2017, p. 259-260].

Les institutions religieuses et les musulmans ont eu l'occasion de réaffirmer leur attachement au pays et à ses valeurs, mais sur fond de mises en demeure, en tant que communauté, ce qui signifie une forme de consolidation du concept. En regard, le reste de la population témoigne d'une acceptation partielle de l'islam sur fond de demande de sécurité et d'état d'urgence. Elle cherche également à mieux cerner ce que pense cet islam de France traversé par de nombreux questionnements.

## L'islam français face au terrorisme : le grand débat

Une grande partie de la communauté intellectuelle musulmane a ressenti le besoin de répondre doctrinalement et concrètement au terrorisme. Cela était d'autant plus urgent que Daesh possédait un organe de propagande performant : le Centre médiatique Al-Hayat, qui publiait la revue francophone *Dâr al-Islâm*. Elle a puisé avec érudition dans la tradition et le droit musulman pour justifier théologiquement les attentats, pas moins de 35 pages de son numéro 8 y étant consacrées [Al-Hayat, février 2016]. Peu après, la revue a défié les théologiens français de produire une réfutation du terrorisme [Al-Hayat, août 2016, p. 6], défi d'autant plus ardu qu'une autorité magistérielles telle qu'El Azhar a refusé de qualifier l'État islamique d'apostat. Quantitativement, des milliers de vidéos ont été diffusées par un autre organisme de Daesh, Al-Furkan Media (du nom de la sourate 25, Al-Furkan, c'est-à-dire « *Le discernement* »). Or, « *l'esthétique djihadiste* est puissante, combinant son et image pour provoquer une *conversion sensorielle* », prélude à la radicalisation et au passage à l'acte [Salazar, 2015, p. 117-131].

Le débat interne a d'abord montré les limites de « l'islam officiel ». Les critiques concernent la représentativité du CFCM, symbole de « l'islam consulaire », qui ne dirige que 13 % des 2 200 imams recensés. De ce fait, seuls 28 % des musulmans de France se sentent représentés par le CFCM [El Karoui, 2016, p. 59 et 37]. De plus, le CFCM, est phagocyté par des États (Algérie, Maroc, Turquie, Arabie saoudite, Qatar). Son fonctionnement, opaque et peu démocratique, est soumis aux aléas des politiques étrangères. Dans l'urgence des attentats a émergé le chantier de la coopération sécuritaire avec les autorités. Azzedine Gaci, membre du bureau de l'UOIF, a lancé un appel sans ambiguïté en ce sens. Le second chantier, largement inabouti, concerne la réforme de l'imamat [El Karoui, 2016, p. 51-57]. De fait, le CFCM est divisé et

(1) Union des organisations islamiques de France (UOIF) devenue Musulmans de France (MF) en 2017.



UNE GRANDE PARTIE DE LA COMMUNAUTÉ INTELLECTUELLE MUSULMANE A RESENTI LE BESOIN DE RÉPONDRE DOCTRINALEMENT ET CONCRÈTEMENT AU TERRORISME. CELA ÉTAIT D'AUTANT PLUS URGENT QUE DAESH POSSÉDAIT UN ORGANE DE PROPAGANDE PERFORMANT : LE CENTRE MÉDIATIQUE AL-HAYAT, QUI PUBLIAIT LA REVUE FRANCOPHONE DÂR AL-ISLÂM. ELLE A PUISÉ AVEC ÉRUDITION DANS LA TRADITION ET LE DROIT MUSULMAN POUR JUSTIFIER THÉOLOGIQUEMENT LES ATTENTATS, PAS MOINS DE 35 PAGES DE SON NUMÉRO 8 Y ÉTANT CONSACRÉES



incapable de se réformer. Les élections qui devaient se tenir en juin 2019 ont été repoussées. Son conseil théologique, créé en 2016, est toujours dans les limbes.

Le champ intellectuel musulman s'avère aussi éclaté que celui des islamologues [Dakhli, 2016, p. 4-17]. Un groupe important considère que « l'islam véritable » n'est pas en cause. Ainsi Nabil Ennasri privilégie les facteurs socio-politiques : les attentats constitueraient une forme de résistance à l'Occident, dans un contexte national et mondial post, voire néo-colonial. Au bout de cette logique on trouve la figure de l'imam salafiste de la mosquée Sunna de Brest, Rachid Abou Houdeyfa qui est très populaire et possède une chaîne YouTube forte de 800 000 abonnés. Les attentats, qu'il a condamnés, n'ont selon lui rien à voir avec l'islam, le terrorisme étant un égarement ne respectant pas les règles du djihâd. De même, « l'imam Ismail » de la mosquée des Bleuets à Marseille considère les terroristes comme des délinquants qui ont basculé sans avoir fréquenté leurs mosquées. La solution prônée passe donc par la restauration de la tradition, le « vrai islam » et le respect des « pieux ancêtres » constituant le meilleur rempart contre les dérives. La référence est le juriste Ibn Taymiyya (1263-1328), qui en prônant une religion dite du « *juste milieu* » s'avère très littéraliste.

D'autres théologiens estiment au contraire que le terrorisme peut être dû en partie à une sclérose théologique. Tarek Oubrou, mais aussi Ghaleb Bencheikh

ou Abdenour Bidar appellent à éliminer la violence de la charia et à promouvoir le principe d'égalité (hommes/femmes ; musulmans/non-musulmans). Rachid Benzine, enseignant à l'Université catholique de Louvain et à la faculté de théologie protestante de Paris, utilise une herméneutique du Coran renouvelant la vision des hadiths et de la Sîra, suivant le précurseur Mohammed Arkoun. Le danger serait de devenir identitaire, à l'instar d'une extrême droite, alors que les valeurs de la République et celles de l'islam sont compatibles. De plus, si l'on considère les finalités de la charia (sécurité des biens et des personnes), la France fait mieux que bien des pays dits « musulmans ». C'est donc un véritable *aggiornamento* qui est nécessaire et qui constitue la meilleure des préventions. Ainsi Tarek Oubrou, auteur du concept de « théologie préventive » a participé en 2015, avec la mairie de Bordeaux et la préfecture, à la création du Centre d'action et de prévention contre la radicalisation des individus (CAPRI), association loi 1901, financée par l'État et les collectivités, qui a géré une trentaine de cas en 2016 [Geisser, 2017, p. 142-146]. Abelali Mamoun, imam itinérant en région parisienne et chroniqueur sur Beur FM, cherche à repérer les échos de l'intégrisme chez les plus jeunes en vue d'élaborer un contre discours [Mamoun, 2017]. Un énorme travail de diffusion de l'herméneutique coranique est mené par l'association « Parle-moi d'islam » dirigée par Kahina Bahloul. Première femme imam de France, tenante d'un islam humaniste et spiritualiste, elle porte le projet d'une mosquée inclusive baptisée Fâtima. Plusieurs personnalités appartenant à « Parle-moi d'islam », dont Mohammed Chirani, ancien délégué auprès du préfet de Seine-Saint-Denis, rappellent que les attentats de 2015 furent à l'origine de leur engagement.

Des approches laïques du problème terroriste existent. Les sociologues Dounia Bouzar et Hasna Hussein étudient les étapes de la radicalisation, notamment chez les femmes. Leurs travaux montrent l'importance du contexte relationnel et émotionnel dans le passage à l'acte, et soulignent le rôle joué par l'absence d'une transmission familiale de la culture arabo-musulmane (même si la moitié des djihadistes n'y appartient pas). De plus, une plus grande attention doit être portée aux « *profils hybrides* », mêlant violence délinquante et religieuse [Bouzar, 2018]. Le gouvernement vient récemment de lancer une action en ce sens, mêlant politique de santé mentale, associations et autorités locales. Enfin, le djihadisme reproduirait les mécanismes d'une dérive sectaire. Cette thèse, très débattue, est portée par Dounia Bouzar et par l'imam d'Ivry-sur-Seine et de Montreuil, Mohamed Bajrafil, présentateur sur la chaîne Ère TV.

Géographiquement, on constate l'extrême hétérogénéité des réponses locales en fonction de la personnalité des

acteurs municipaux et religieux [Pingaud, 2016]. L'état d'urgence a eu pour vertu de remettre les préfets au centre du jeu local. Ils ont lancé trois consultations auprès des autorités musulmanes en 2015-2016, contournant les municipalités et d'éventuelles utilisations politiciennes de l'islam (clientélisme, arrêtés anti-burkini) [Geisser, 2017, p. 179-183].

### La perception du terrorisme chez les jeunes musulmans : une spécificité générationnelle

Au sein de la communauté musulmane, le débat est surtout le fait des moins de 35 ans, qui ignorent le CFCM et les mosquées traditionnelles. En effet, les imams sont à 80 % étrangers et âgés de plus de 50 ans, en complet décalage avec les musulmans de France, majoritairement Français (à 75 %) et dont 50 % ont moins de 50 ans [Jouanneau, 2013, p. 17]. Les plus jeunes ignorent également leur entourage pour se réfugier sur internet, dans « l'islamosphère », la plupart déclarant utiliser des pseudonymes pour une plus grande liberté de propos [Geisser *et alii*, 2017, p. 126-128]. Quelques grands sites se détachent, tels *Oumma.com*, *Saphirnews*, mais aussi *Islam & Info* dont le slogan est « *L'info par le Musulman, pour le Musulman* ». Pour les plus jeunes, l'accès à l'information suit des règles et des canaux particuliers. Chez les lycéens musulmans de zones sensibles, la méfiance à l'égard des médias traditionnels domine : une petite moitié (48 %) suit encore les médias français classiques, lesquels sont presque exclusivement télévisuels (*I-Télé* et *BFM*). Sur les réseaux sociaux ou via la télévision, la confiance est presque exclusivement accordée aux images et surtout à la « *force émotionnelle des informations* », qui « *devient même un critère de véracité de leur jugement* ». De plus, les élèves musulmans sont bien plus travaillés par les théories du complot que les autres adolescents : 44 % des lycéens musulmans interrogés y adhèrent partiellement et 7 % totalement [Galland & Muxel, 2018, p. 328-337]. Ce chiffre est à rapprocher de celui qui concerne la population musulmane adulte : interrogés sur la question « En France, les musulmans sont victimes d'un complot », 37 % des sondés répondent par l'affirmative [El Karoui, 2016, p. 41]. À cela s'ajoute le travers de toute leur génération : les lycéens musulmans font « *l'apologie des idées personnelles comme critère de sélection* ». Le droit d'avoir sa propre opinion semble l'emporter. Un « *bricolage personnel* », faisant peu appel aux discussions physiques entre pairs, se construit ainsi. [Galland & Muxel 2018, p. 332-335]. Au final, 67 % de ces lycéens musulmans pensent que les médias n'ont pas dit la vérité au sujet des attentats de 2015, pour seulement 5 % qui pensent qu'ils ont dit toute la vérité.

De plus, 9 % des lycéens musulmans « *participent de façon active aux flux informationnels de Daesh* », c'est-à-dire qu'ils reçoivent et retransmettent des contenus émanant d'Al-Furkan, voire de Dâr al-Islâm. Pour ces élèves, qui tout à la fois ne suivent pas les médias traditionnels français, adhèrent à des régimes de vérité alternative et retransmettent des contenus djihadistes, les chercheurs ont forgé le concept de « *radicalité informationnelle* ». Il y a chez eux une coupure complète vis-à-vis des sources d'information communes et de leur contenu [Galland & Muxel 2018, p. 317-319].

Ainsi s'éclairent les attitudes des lycéens musulmans face aux attentats de 2015. Ils font preuve d'une très grande « *distance émotionnelle* ». [Galland & Muxel 2018, p. 370]. 19 % d'entre eux se sont déclarés « pas concernés » par la minute de silence, et 13 % ne condamnent pas totalement les attentats de novembre 2015. Parmi ces derniers, un tiers affirme ne rien avoir éprouvé, n'en avoir rien à faire (parfois en des termes très crus) et a témoigné très peu d'empathie. Une fraction approuve les attentats de 2015 (3 %) et a ressenti de la joie (2 %). Pour expliquer de telles réactions, un facteur s'avère déterminant : la tolérance à la violence et à la déviance ordinaires (trouver acceptable qu'un conflit se règle en contournant la loi et en utilisant une certaine dose de violence). Ainsi, « *le terreau de la radicalité religieuse n'est pas uniquement religieux [...] (il) est aussi manifestement associé à des prédispositions à la violence ou à la déviance détachées de motifs religieux* ». Il existe en effet une « *socialisation à la violence et à la déviance* », [Galland & Muxel, 2018, p. 131] liée à l'existence d'une « *culture déviante* » [Cicchelli, 2007, p. 165-181]. Cet effet est plus important dans établissements où les élèves musulmans sont proportionnellement plus nombreux. Les facteurs prédictifs de la tolérance à la violence-déviance sont : une moindre intégration scolaire, l'idée d'un mode divisé entre faibles et forts, et surtout l'appartenance au sexe masculin. Le statut social des parents est inopérant [Galland & Muxel, 2018, p. 116-117]. Ce terreau détermine un modèle violent applicable à toutes les questions et à la religion en particulier.

L'autre grand facteur est l'adhésion à un « *modèle absolutiste* », ainsi défini : penser « *détenir la vérité absolue sur les questions religieuses, mais aussi vouloir l'imposer dans le monde séculier* ». La thèse visant à expliquer la radicalité par des facteurs socio-économiques est invalidée : « *L'effet «islam» est fort et résiste à l'introduction des variables socio-économiques, mais également à d'autres variables (discrimination, conflits familiaux)* ». Il y aurait donc un « *effet spécifique de l'appartenance à l'islam* », avec l'idée que « *la critique de la religion [...] témoigne d'un manque de respect envers les croyants eux-mêmes* ». [Galland & Muxel, 2018, p.77, 100, 140-142 et 172-174].

C'est la combinaison de la tolérance à la violence-déviance, et de l'absolutisme religieux qui produit les réactions de rejet face aux minutes de silence, et de « compréhension » à l'égard des actes terroristes. 13 % des lycéens musulmans interrogés sont à la fois tolérants à la violence et à l'absolutisme religieux (contre 2 % des élèves chrétiens et 0 % des sans-religion). S'il y a spécificité musulmane, interpréter « religieusement » la radicalité religieuse ne suffit pas : « *Le facteur le plus prédictif de la justification de la violence religieuse était les prédispositions à la violence et à la déviance* », et l'appartenance au sexe masculin [Galland & Muxel, 2018, p. 131 et 146], ce qui est à rapprocher de la « *personnalité autoritaire* » théorisée par Adorno (en particulier ce qu'il nomme « *l'échelle F* », qui mesure les tendances profondes de la personnalité. Par exemple : la valorisation de l'autorité et de la force, le traditionalisme, le refus de l'introspection posée comme une faiblesse, le rejet à l'extérieur des dangers qui nous menacent ou encore la tendance à la superstition). Hakim El Karoui [2016, p. 28] évalue à 28 % le pourcentage des musulmans adultes sondés combinant « *à la fois des attitudes autoritaires et d'autres que l'on pourrait qualifier de sécessionnistes* ».

Un certain repli intellectuel s'observe donc face aux flux médiatiques relatant les attentats, ainsi qu'un repli cognitif, certains jeunes se coupant des sources d'information communes, de leurs éclairages et pire, peut-être, des émotions qu'elles véhiculent. De plus, les musulmans de France ont été plus spécifiquement aux prises avec la politique antiterroriste menée depuis 2015. Analysons comment l'antiterrorisme, conséquence directe du terrorisme, a été perçu par les musulmans et quels changements de comportement il a provoqués.

## Les effets spécifiques de la politique antiterroriste sur les musulmans

### La perception de l'État et de l'antiterrorisme chez les Français musulmans

Les musulmans font davantage confiance *a priori* aux institutions que les autres habitants, et plébiscitent dans l'ordre : l'armée, la Sécurité sociale, l'école, le maire, les services de renseignement, la justice, le président de la République, le parlement. L'armée et l'école possèdent une aura particulière, y compris en zone sensible [Galland *et alii*, 2018, p. 179-181]. Toutefois, deux exceptions

négatives concernent les services de police/gendarmerie et les médias qui viennent également en bas de tableau pour l'ensemble des Français [Ragazzi *et alii*, 2018, p. 24-26]. Cela est important étant donné le rôle crucial joué par les médias dans la diffusion et la perception du terrorisme.

Concernant la politique antiterroriste française, musulmans et non-musulmans se sentent aussi (peu) rassurés par cette politique (score de 6/10). Mais trois fois plus de musulmans que la moyenne ne se sentent pas du tout en sécurité : 10 % d'entre eux ont choisi un score de 0/10. Les musulmans jeunes, surtout les hommes, sont les moins tranquillisés. Quant aux musulmanes, elles se sentent moins en sécurité (5,7 /10) que l'ensemble des femmes (6,3). À l'inverse, les personnes musulmanes entre 45 et 65 ans s'estiment plus protégées que la moyenne (7/10 contre 6,2).

Étudiions à présent « *l'exposition à l'antiterrorisme* » [Ragazzi *et alii*, 2018, p. 33-35]. Dans le cadre d'une politique antiterroriste ou anti-radicalisation, des personnes se sont en effet trouvées en contact avec des travailleurs sociaux, des éducateurs ou des représentants des forces de l'ordre. Lorsqu'on demande aux musulmans si le choix des groupes ciblés était justifié, 34 % répondent non (contre 15 % parmi l'ensemble de la population) et seulement 31 % répondent oui (contre 43 %) [Ragazzi *et alii*, 2018, p. 46-47]. Or, les musulmans ont été, de façon contre-intuitive, moins exposés que l'ensemble de la population (24 % des sondés contre 30 %), sauf pour les moins de 25 ans : 8 % des jeunes musulmans ont ainsi été mis en contact avec des éducateurs contre 2 % de l'échantillon global. Les musulmans sont même moins en contact avec la police (16 % contre 22 %), mais ce contact (essentiellement des contrôles d'identité) est fortement genré : 21 % des hommes contre 11 % des femmes de confession musulmane. Lorsqu'on demande aux personnes ayant été confrontées à des représentants de l'État si ces contacts leur semblaient justifiés, les musulmans répondent davantage par la négative, surtout pour les contacts avec la police (note de 5,6 sur 10 contre 7,7). 12 % des musulmans estiment ce contact comme absolument injustifié, contre 4 % de l'ensemble. Le rejet de cette politique est donc assez fort chez les musulmans, d'autant qu'ils évaluent la façon dont ils ont été traités de façon plus négative (6,9/10 contre 8,5). Plus finement, lorsque l'on interroge les personnes qui estiment avoir été choisies de façon délibérée, seuls 6 % des musulmans ne savent pas pourquoi (contre 26 % de l'ensemble). Les musulmans « ciblés » avancent comme raison leurs origines (37 %), leur couleur de peau (35 %) et leur religion (15 %).

Si la politique antiterroriste est acceptée dans son principe par les musulmans de France, elle fait l'objet d'un rejet



assez large en raison de son caractère jugé trop ciblé et de la manière dont certains interlocuteurs procèdent. Sur l'antiterrorisme, un clivage générationnel existe au sein de la population musulmane, d'une part, et entre les jeunes musulmans et le reste de la société, d'autre part. Surtout, un certain sentiment d'insécurité et d'injustice travaille la population musulmane [Ragazzi *et alii*, 2018, p. 42-44]. Mais les événements terroristes et l'antiterrorisme induit ont également modifié les comportements observables des musulmans de France.

### Les changements de comportement chez les Français musulmans

Il s'agit de savoir dans quels domaines les musulmans ont modifié leur comportement « *de peur d'être discriminé.e.s ou suspectes* » [Ragazzi *et alii*, 2018, p. 51-65]. Si 30 % de la population musulmane évite de dire ce qu'elle pense sur des questions de politique étrangère ou de société, cela n'est que légèrement supérieur à la moyenne. L'autocensure concerne donc l'ensemble de la société, en particulier les femmes. À l'inverse, les plus de 65 ans et les moins de 25 ans ont une grande liberté de parole. De même, les musulmans n'ont pas davantage changé leurs habitudes en ligne que la moyenne (80 % de non), et la population musulmane n'est pas gênée par de possibles intrusions dans la vie privée engendrées par l'antiterrorisme, alors que ce discours est prégnant parmi de nombreuses associations.

Mais devant des interlocuteurs institutionnels, le tableau change. Ainsi, 20 % des musulmans déclarent faire attention à leurs propos face aux personnels de santé, surtout les hommes et les plus âgés. De même, 26 % des musulmans se surveillent face à des éducateurs. C'est d'ailleurs le seul interlocuteur face auquel les jeunes se censurent davantage que l'ensemble de la population musulmane. Surtout, 42 % des musulmans appartenant aux classes d'âges ayant des enfants scolarisés ont demandé à ceux-ci de faire attention à leurs propos à l'école. Cette prudence culmine dans le domaine des œuvres caritatives : 40 % des musulmans de plus de 25 ans déclarent y réfléchir à deux fois avant de donner.

De façon plus visible, 8,5 % (contre 1,6 % dans le groupe témoin) des musulmans ont modifié leur manière de s'habiller ou leur apparence pour éviter une potentielle discrimination, surtout les hommes, notamment les moins de 45 ans et les plus de 65 ans.

Parallèlement à ce que la communauté musulmane montre d'elle, « *à ce qui sort d'elle en direction de l'extérieur* »,



SI LA POLITIQUE ANTITERRORISTE EST ACCEPTÉE DANS SON PRINCIPE PAR LES MUSULMANS DE FRANCE, ELLE FAIT L'OBJET D'UN REJET ASSEZ LARGE EN RAISON DE SON CARACTÈRE JUGÉ TROP CIBLÉ ET DE LA MANIÈRE DONT CERTAINS INTERLOCUTEURS PROCÈDENT. SUR L'ANTITERRORISME, UN CLIVAGE GÉNÉRATIONNEL EXISTE AU SEIN DE LA POPULATION MUSULMANE, D'UNE PART, ET ENTRE LES JEUNES MUSULMANS ET LE RESTE DE LA SOCIÉTÉ, D'AUTRE PART.



on observe une fermeture par rapport « *à ce qui entre* » [Ragazzi *et alii*, 2018, p. 59-60]. À la question : « *Vous avez arrêté de lire ou de regarder certains médias parce que vous pensez qu'ils ne représentent pas correctement la communauté musulmane* », 38 % des musulmans ont répondu « oui », les femmes étant surreprésentées ainsi que les 18-44 ans (42 %). Seule une petite moitié déclare avoir gardé ses habitudes en la matière. 43 % des musulmans ayant effectué ce changement l'expliquent par un manque de confiance dans les informations concernant spécifiquement le terrorisme et la lutte antiterroriste. Cette fermeture, déjà évoquée au sujet des plus jeunes en contexte « *pré-attentat* », est ici directement liée au terrorisme et à la façon dont il en est rendu compte. Le terrorisme est donc l'accélérateur sinon le déclencheur de la fermeture vis-à-vis des médias communs, beaucoup plus prononcée que dans le reste de la population.

## Conclusion

Largement virtuel au regard des décès violents en France, de valeur quasi nulle du point de vue économique, le terrorisme a su s'imposer dans l'imaginaire collectif en raison de son caractère spectaculaire, ce qui fait que chacun y croit désormais. Ainsi a été créé le champ du terrorisme spectaculaire islamique.

Dans cet espace mental, les manifestations du terrorisme contribuent à faire progresser les représentations percevant l'immigration et l'islam de façon négative parallèlement à celles qui, dans la population musulmane, jouent en

faveur d'un repli verbal, comportemental et surtout cognitif, sur fond d'insécurité ressentie. À la « congruence » des extrêmes décrite par Gilles Kepel s'ajoute donc un risque de « divergence » entre les citoyens musulmans et les

autres : non pas tant dans le domaine des comportements observables (ce qui en soi est déjà inquiétant), mais surtout dans le domaine qui est le véritable champ de bataille du terrorisme, à savoir l'imaginaire, ciment d'une nation ■

## Bibliographie

- ADORNO (T.), 2007, *Études sur la personnalité autoritaire*, Paris, Allia, 435 p. (première éd. 1980).
- AL-HAYAT, *Dabiq*, 8 avril 2015 (en anglais).
- AL-HAYAT, *Dâr al-Islâm*, 7 février 2016, « Attentats sur la voie prophétique », n° 8, 114 p.
- AL-HAYAT, *Dâr al-Islâm*, 20 août 2016, « Attentats sur la voie prophétique. Deuxième partie : Game Over », n° 10, 58 p.
- ARCISZEWSKI (T.), 2005, *La menace : sa perception, ses effets, son utilisation*, thèse soutenue à l'Université de Paris-V
- ARKOUN (M.), 2016, *Lectures du Coran*, Paris, Albin Michel, 512 p. (première édition en 1982).
- ARON, (R.), 1962, *Paix et guerre entre les nations*, Paris, Calmann-Lévy, 797 p.
- BIRNBAUM (J.), 2018, *La religion des faibles. Ce que le djihadisme dit de nous*, Paris, Seuil, 288 p.
- BONARDI (C.) & MANNONI (P.), 2003, « Terrorisme et mass media », *Topiques*, n° 83, p. 55-72.
- BOUZAR (D.), 2018, *Français radicalisés. Enquête. Ce que révèle l'accompagnement de 1 000 jeunes et de leur famille*, Paris, Éditions de l'Atelier, 302 p.
- CICCHIELLI (V.), 2007, « Les émeutiers de 2005 », *Le Débat*, n° 145, p. 165-181.
- COHEN (M.), 2000, « Juifs et Musulmans en France : le modèle républicain d'intégration en question », *Sociétés contemporaines*, n° 37, p. 89-120.
- DELUMEAU (J.), 1978, *La peur en Occident*, Paris, Fayard, 485 p.
- DEL VALLE (A.), 2018, *La stratégie de l'intimidation*, Paris, L'Artilleur, 560 p.
- DAKHLI (L.), « L'islamologie est un sport de combat », *Revue du Crieur*, Paris, La Découverte, février 2016, p. 4-17
- DELUMEAU (J.), 1978, *La peur en Occident*, Paris, Fayard, 485 p.
- DIECKHOFF (A.), 1990, « Les Logiques de l'émancipation et le sionisme » in BIRNBAUM, (P.) (dir.), *Histoire politique des Juifs de France*, Paris, Presses de la Fondation nationale des sciences politiques, 310 p.
- ELIAS (N.), 1973, *Sur le processus de civilisation*, Paris, Calmann-Lévy, 447 p.
- EL KAROUI (H.), 2016, *Un islam français est possible*, Paris, Institut Montaigne, 176 p.
- GALLAND (O.) & MUXEL (A.) dir., 2018, *La tentation radicale. Enquête auprès des lycéens*, Paris, PUF, 455 p.
- GEISSER (V.), MARONGIU-PERRIA (O.), SMAIL (K.), 2017, *Musulmans de France, La grande épreuve. Face au terrorisme*, Paris, Éditions de l'Atelier, 311 p.
- HECKER (M.), 2018, *137 nuances de terrorisme. Les djihadistes de France face à la justice*, IFRI, Focus stratégique n° 79, 52 p.
- HUYGUE (F.-B.), 2002, « Entre ravage et message. Spectacle, sous-titre et générique », *Les Cahiers de médiologie*, n° 13, p.37-47.
- HOFFMAN (B.), 1999, *La mécanique terroriste*, Paris, Calmann-Lévy, 302 p.
- IBN TAYMIYYA (I.), 2017, *Écrits politiques*, Paris, Nawa, 196 p.
- JOUANNEAU (S.), 2013, *Les imams en France. Une autorité religieuse sous contrôle*, Paris, Éditions Agone, coll. « L'ordre des choses », 528 p.
- KEPEL (G.), 2016, *La fracture*, Paris, Gallimard/France Culture, 288 p.

- LAQUEUR (W.), 1979, *Le terrorisme*, Paris, PUF, 292 p.
- MAMOUN (A.), 2017, *L'islam contre le radicalisme. Manuel de contre-offensive*, Paris, Cerf, 223 p.
- MANNONI (P.), 2003, « Le terrorisme : un sujet d'étude scientifique ? », *Les cahiers de psychologie politique* [En ligne], numéro 3, Avril. <http://lodel.irevues.inist.fr/cahierspsychologiepolitique/index.php?id=1616>
- MANNONI (P.), 2004, *Les logiques du terrorisme*, In Press, 227 p.
- MANNONI (P.), décembre 2004-janvier-février 2005, « Le terrorisme, un spectacle sanglant », *Sciences humaines*, Hors-série n° 47, p. 64-68.
- MICHERON (H.), 2019, *Les territoires du djibâd. Quartiers, prisons, Levant*, thèse pour le doctorat en sciences politiques, École normale supérieure.
- NAJI (A.), *Gestion de la barbarie*, Versailles, Éditions de Paris, 2007, 248 p.
- PINGAUD (E.), 2016, « La gestion municipale de l'islam. Les accommodements pragmatiques du pouvoir local », *Métropolitiques*, [en ligne] : [https://www.metropolitiques.eu/\\_Pingaud-Etienne\\_.html](https://www.metropolitiques.eu/_Pingaud-Etienne_.html)
- PUCHOT (P.) & CAILLET (R.), 2017, *Le combat vous a été prescrit*, Paris, Stock, 228 p.
- RAGAZZI (F.), DAVIDSHOFER (S.), PERRET (S.) et TAWFIK (A.), 2018, *Les effets de la lutte contre le terrorisme et la radicalisation sur les populations musulmanes en France*, Centre d'études sur les conflits, Paris, 102 p.
- RAMADAN (I.) & AL-QARADHAWI (Y.), 2002, *Recueil de fatwas. Avis juridiques concernant les musulmans d'Europe*, Lyon, Tawhid, 190 p.
- ROBERT (C.), *Terrorisme islamiste : quelles sont les vraies causes ?* <https://www.contrepoints.org/2017/01/02/261277-vraies-causes-du-terrorisme-islamiste>
- SALAZAR (P.), 2015, *Paroles armées. Comprendre et combattre la propagande terroriste*, Paris, Le Mieux éditeur, 262 p.
- SERVIER (J.), *Le terrorisme*, Paris, PUF, 1979, 128 p.
- TOZZO (S.), 2016, *Discours sur l'identité et l'altérité : une analyse de la représentation des attentats du 13 novembre 2015 à Paris dans la presse écrite*, thèse en langue moderne et communication, Université de Padoue, 142 p.
- ZERHOUNI (O.), ROUGIER (M.), & MULLER (D.), 2016, « Who (Really) is Charlie? French Cities with Lower Implicit Prejudice toward Arabs Demonstrated Larger Participation Rates in *Charlie Hebdo* Rallies », *International Review of Social Psychology*, 29, p. 69-76.

# Approche du traitement des traces d'outils dans la problématique des cambriolages par les systèmes d'information géographiques (SIG)

GRÉGORY BRICHE

## Grégory BRICHE



Le Lieutenant-colonel Grégory BRICHE est le chef de la Division Criminalistique Physique et Chimie (DCPC) de l'Institut de Recherche Criminelle

de la Gendarmerie Nationale (IRCGN). Il a été responsable de l'unité d'expertise Traces Manufacturées au sein du département Microanalyse (MCA) de 2004 à 2011, réalisant de nombreux examens scientifiques. Il a également pris part à des missions de constatations sur des scènes de crime importantes (Affaires Laetitia PERRAIS/Tony MEILHON, Marie-Christine HODEAU, ...) ainsi qu'à des missions d'identification de victimes de catastrophes. Il est à l'origine du Projet TACS pour « Toolmarks Analysis Comparison System », Système Automatisé de Comparaison de Traces d'Outils, mené au sein de l'IRCGN.



En France, un cambriolage a lieu toutes les 90 secondes et les délinquants s'affranchissent largement des frontières administratives. Une approche SIG de ces phénomènes devrait permettre de rendre encore plus efficaces les actions de prévention et les investigations des enquêteurs en augmentant le taux de résolution des faits de cambriolages. Le système TACS permet d'apporter aux enquêteurs une réponse optimale en facilitant les rapprochements entre procédures et ce, sur une zone géographique étendue. Une solution complète pour l'exploitation des traces d'outils relevées lors des cambriolages. Objectif : déterminer si le même outil a été utilisé sur différents lieux d'infraction.

Gives that a burglary occurs in France every 90 seconds and that offenders cross administrative borders, the investigations become even more relevant as the geographical area is important. À GIS approach to these phenomena should make it possible to make prevention actions and investigators' investigations even more effective by increasing the rate of resolution of burglary incidents. The TACS system offers an optimal response to the investigators by connecting criminal activities on a wide geographical area. À forensic evaluation of toolmarks encountered in crime scenes such as burglaries, thefts or violent interactions. Purpose : to determine if an evidence mark was made by a suspected tool.

Les délits d'appropriation ou vols sont aujourd'hui au centre des faits constatés par le système judiciaire français et, par voie de conséquence, des préoccupations de l'État et des forces de sécurité. Parmi ces faits, les vols par effraction occupent actuellement une part prépondérante dans le spectre de délinquance.

Le progrès technologique, la mise en place des banques de données FNAEG et FAED<sup>1</sup>, la possibilité pour les enquêteurs de recourir à une analyse quantitative pour les infractions dites « de masse » ont ainsi amené à une hiérarchie de la pertinence des traces au sommet duquel sont placées les traces génétiques et digitales considérées comme plus individualisantes. Ce succès a donc plus ou moins directement conduit la majorité des enquêteurs à concentrer les opérations de police technique sur la seule découverte de traces digitales ou génétiques. Cet état de fait a pour conséquence négative de voir la pratique des actes de criminalistique par les enquêteurs recentrée sur ces seules techniques.

Nombreux sont les vols par effraction constatés en France de nos jours et nombre d'entre eux laissent apparaître aux enquêteurs, lors de leurs constatations, des traces d'outils (casque barillet, perçage, crochetage, etc.). Ainsi, l'exploitation de telles traces s'avère-t-elle actuellement suffisante et pertinente ? Son utilisation n'est-elle pas perfectible ?

## Qu'est-ce qu'une trace d'outil?

L'AFTE (Association of Firearms and Toolmarks Examiners) définit un outil comme étant un objet qui permet d'obtenir un avantage mécanique pendant son utilisation. Ainsi, lorsque la force est suffisante [Van Dijk, 1995], le contact entre un outil et un support plus mou peut être visualisé de manière permanente par la présence d'une trace sur ce support.

En fonction du type d'outil utilisé, les traces laissées par celui-ci seront différentes : moulées, glissées ou superposées. Les traces moulées sont dues à un mouvement de compression. L'empreinte obtenue correspond à un moulage de l'outil en négatif. Ces traces s'observent lors de l'utilisation d'outils tels qu'un pied-de-biche ou un marteau. Les traces glissées sont le résultat d'une compression accompagnée d'un déplacement (abrasion). Ces traces sont laissées par des pinces,

des ciseaux ou encore des couteaux. Enfin, les traces superposées proviennent de l'accumulation de plusieurs traces les unes par-dessus les autres. Ce type de trace est obtenu après l'utilisation d'une scie par exemple.

La trace laissée sera différente en fonction du type d'outil et du support [Toso, 1995] (forme, taille, composition du matériau...), mais aussi en fonction de l'utilisation de l'outil (force, angle d'attaque...). En examinant une trace, on peut déterminer le type d'outil qui en est à l'origine. Des comparaisons peuvent aussi être faites pour déterminer si deux traces proviennent du même outil. Pour vérifier qu'un outil est à l'origine d'une trace, il faut la confronter (trace prélevée) à une trace de comparaison. Afin d'obtenir les meilleurs résultats possible, la trace de comparaison doit être reproduite dans les conditions les plus proches de celles de la trace en question (même type d'outil, même type de support...). La dénomination s'applique à toutes les traces laissées sur un support (pneumatique percé, tube sectionné, etc.) et sur l'outil incriminé (couteau, pince coupante, etc.).

Chaque outil possède des anomalies et des caractères qui lui sont propres. Trois types de caractéristiques permettent ainsi d'individualiser un outil. Les caractéristiques de classe permettent de connaître la forme et la taille de l'outil. Les sous-caractéristiques de classe présentent les défauts qui sont apparus lors de la production de l'outil. Cela permet de restreindre toute une gamme d'outils à une seule série. Les caractéristiques individuelles sont spécifiques d'un outil. Elles proviennent de son utilisation et de sa dégradation (corrosion, usure...). Ces dernières sont plus généralement appelées « stries », ce sont des micro-défauts, qui apparaissent sur sa surface au cours de son utilisation. Le travail de l'expert consiste donc à tenter de reproduire la trace en question, l'intérêt étant de réaliser un rapprochement entre les microstries présentes sur les échantillons et de les comparer.

Trois types de travaux sont alors possibles pour les experts :

- comparaison de trace à trace : le requérant doit effectuer en amont un travail d'enquête en vue d'établir des liens géographiques et temporels, sur la manière d'opérer afin que la comparaison soit efficace. Dans le cas d'une comparaison de trace à trace, le but de la mission est de déterminer si le même outil est à l'origine de différentes traces afin de pouvoir effectuer des rapprochements entre différentes affaires ;

(1) Fichier national automatisé des empreintes génétiques et Fichier automatisé des empreintes digitales.

- comparaison avec un outil : il s'agit de savoir si l'outil saisi lors d'une perquisition ou découvert lors de constatations est à l'origine des traces relevées. L'expert va alors effectuer une comparaison de la trace avec celle reproduite par l'expert avec l'outil saisi. Il procède à une mise en concordance des caractéristiques individuelles (microstries) dues à l'outil ;
- présence d'une trace unique : il s'agit de déterminer un type d'outil dans le cas de la fourniture d'une unique trace d'outil. Il peut s'avérer judicieux de déterminer le type d'outil, d'objet ou famille d'outils, information utile à la recherche ultérieure de l'outil sur un auteur ou lors d'une perquisition.

Ce travail est réalisé par les personnels de l'Unité d'expertise (UE) traces manufacturées (TM) du département Microanalyse (MCA) de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) installé à Pontoise (95) depuis 2015. L'IRCGN est un institut de sciences forensiques, englobant sur un même site toutes les technologies et sciences concernant la recherche de la vérité scientifique au procès pénal. Le statut militaire des gendarmes scientifiques leur permet d'œuvrer en tous lieux et tous temps, donnant à cette unité un statut opérationnel reconnu dans le monde entier. Le département Microanalyse s'intéresse à toute trace susceptible d'aider à la manifestation de la vérité et qui doit systématiquement être recherchée et prélevée. On distingue divers types d'échantillons, macroscopiques, voire microscopiques : les traces manufacturées (lampes à incandescence et traces d'outils), les résidus de tir ainsi que les traces de transfert (sols, fibres, éléments pileux et les verres). Révélés, étudiés et si nécessaire comparés à d'autres échantillons, ces prélèvements peuvent se montrer particulièrement déterminants pour l'enquête.

Pourtant, au-delà de la preuve matérielle qu'elle peut représenter, l'information contenue dans la trace d'outil, peut prendre une tout autre dimension informative et se constituer alors comme un élément à fort potentiel dès lors que son exploitation est mise en perspective avec des données à caractère géographique.

## Système d'information géographique

Un système d'information géographique (SIG) est un système d'information conçu pour recueillir, stocker, traiter, analyser, gérer et présenter tous les types de données spatiales et géographiques. Dans un sens plus général, le sigle SIG décrit un système d'information qui intègre, stocke, analyse et affiche l'information géographique. Les applications liées aux SIG sont des outils qui permettent aux utilisateurs de créer des requêtes interactives, d'analyser l'information spatiale, de modifier et d'éditer des données par l'entremise de cartes et d'y répondre cartographiquement. La science de l'information géographique est la science qui sous-tend les applications, les concepts et les systèmes géographiques.

Le SIG englobe un certain nombre de technologies, de processus et de méthodes. Celles-ci sont étroitement liées à l'aménagement du territoire, la gestion des infrastructures et réseaux, le transport et la logistique, l'assurance, les télécommunications, l'ingénierie, la planification, l'éducation et la recherche, etc. C'est pour cette raison que les SIG sont à l'origine de nombreux services de géolocalisation basés sur l'analyse des données et leur visualisation.

Trois grandes catégories de lieux sont visées par les cambriolages et retenues lors de la délivrance de statistiques sur le domaine : les résidences principales (RP), les résidences secondaires (RS) et les locaux industriels et commerciaux (LIC).

Lors des constatations « Traces d'Outils », notamment réalisées avec une certaine proximité temporelle, on peut obtenir comme explicité ci-dessus, diverses informations.

En l'absence de l'outil, mais en présence de plusieurs traces, on peut effectuer des rapprochements entre différentes affaires.

En présence de l'outil, surtout si on a identifié son propriétaire, on peut l'incriminer dans une ou plusieurs affaires.

←

AU-DELÀ DE LA PREUVE MATÉRIELLE  
QU'ELLE PEUT REPRÉSENTER,  
L'INFORMATION CONTENUE DANS  
LA TRACE D'OUTIL, PEUT PRENDRE  
UNE TOUT AUTRE DIMENSION  
INFORMATIVE ET SE CONSTITUER  
ALORS COMME UN ÉLÉMENT À  
FORT POTENTIEL DÈS LORS QUE  
SON EXPLOITATION EST MISE EN  
PERSPECTIVE AVEC DES DONNÉES À  
CARACTÈRE GÉOGRAPHIQUE.

→

L'identification d'un outil, ou d'un type d'outil, sera une information exploitable lors de constatations complémentaires ultérieures.

Dans ce cadre, et pour s'assurer de l'intérêt de procéder à ces comparaisons compte tenu du vécu supposé de l'outil, des travaux sur le nombre d'utilisation possible d'un outil avant que son exploitation ne soit plus possible en comparaison ont été réalisés [Boumail, 2010].

Ainsi, on peut mettre en évidence : une composante spatiale, une composante attributaire ou thématique, un ensemble de relations spatiales et une composante temporelle.

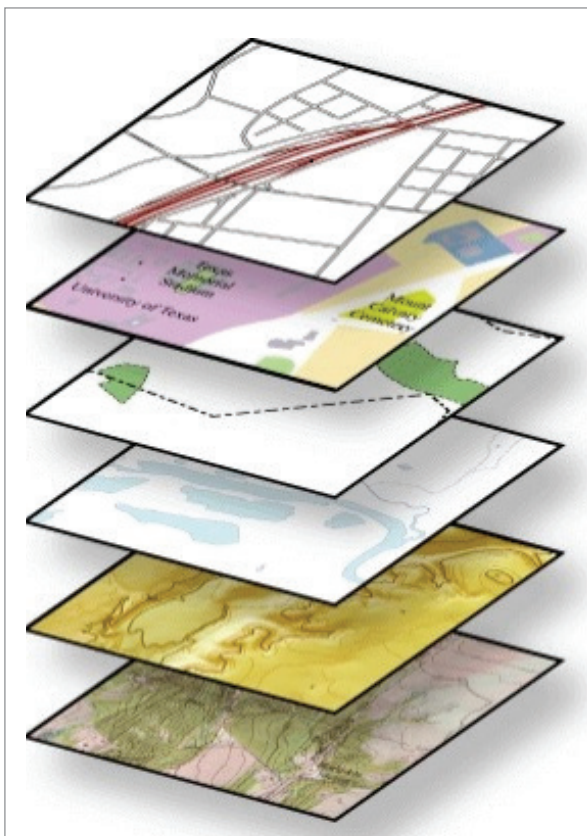
Nous sommes donc en présence de couches d'informations géographiques superposables, opération indispensable pour mettre en œuvre les traitements spatiaux spécifiques aux SIG.

Cela permet non seulement d'élaborer une stratégie d'occupation du terrain à des fins préventives, mais également de « voir » plus rapidement des recoupements moins visibles s'ils sont noyés dans des bases de données exploitées sous forme de tableaux.

Autrefois action d'opportunité commise généralement de façon individuelle, le cambriolage est aujourd'hui le fait de groupes criminels de plus en plus organisés usant de l'avantage fourni par la libre circulation des personnes et des biens. La gendarmerie nationale, acteur de la police judiciaire, s'est dotée d'une véritable architecture de police technique et scientifique propre à pouvoir intervenir dans le cadre des opérations de constatations sur les scènes de crimes, de rapprochement et recoupement, mais aussi d'analyse des traces recueillies.

L'information issue de la trace offre également un tout autre potentiel dans le domaine du renseignement criminel et permet alors, après exploitation, de pouvoir prévenir, anticiper, détecter les phénomènes sériels ou encore d'analyser une activité criminelle.

Trop souvent délaissés au profit de la trace génétique et digitale, les autres types de traces s'avèrent être un atout certain dans ces différents domaines. La trace d'outil en est un exemple plus que parlant. Reléguée trop souvent malgré elle au plan de simple information procédurale, la trace d'outil offre, une fois passée dans les mains expertes du département de micro-analyse de l'IRCGN, un potentiel bien plus important.



(Source IRCGN)

Nous pouvons donc imaginer mettre en évidence les voies de communication d'un territoire, ses limites administratives, l'implantation des unités de gendarmerie, la présence ou non d'une police municipale ou d'un garde champêtre, l'implantation d'un dispositif de vidéoprotection et l'adhésion d'un quartier à un dispositif de voisins vigilants...

Pour l'aspect technique, le type de local concerné : RP, RS ou LIC.

On s'attachera également à mettre en évidence les cambriolages constatés avec l'horaire, même approximatif : ceux avec des traces communes, mais sans outil saisi, ceux avec des traces d'outils identifiés et reliées à un outil et ceux où des points particuliers, en plus du type d'outil utilisé, sont à mettre en relief (mode opératoire, individu ou type de véhicule aperçu, résultats de police technique exploitables tels que des empreintes digitales relevées ou un ADN...).



AUTREFOIS ACTION D'OPPORTUNITÉ COMMISE GÉNÉRALEMENT DE FAÇON INDIVIDUELLE, LE CAMBRIOLAGE EST AUJOURD'HUI LE FAIT DE GROUPES CRIMINELS DE PLUS EN PLUS ORGANISÉS USANT DE L'AVANTAGE FOURNI PAR LA LIBRE CIRCULATION DES PERSONNES ET DES BIENS. LA GENDARMERIE NATIONALE, ACTEUR DE LA POLICE JUDICIAIRE, S'EST DOTÉE D'UNE VÉRITABLE ARCHITECTURE DE POLICE TECHNIQUE ET SCIENTIFIQUE PROPRE À POUVOIR INTERVENIR DANS LE CADRE DES OPÉRATIONS DE CONSTATATIONS SUR LES SCÈNES DE CRIMES, DE RAPPROCHEMENT ET RECOUPEMENT, MAIS AUSSI D'ANALYSE DES TRACES RECUEILLIES.



## Commentaires

Pour lutter contre les cambriolages, des initiatives locales existent. Par exemple, le département de la Charente-Maritime s'est doté d'une base de données spécialement dédiée à l'enregistrement, l'analyse des traces en vue de pouvoir effectuer des recoupements et rapprochements [Hubert, 2017].

Cette base a été primée aux ateliers de la performance en octobre 2016, programme original et efficace pour recueillir et diffuser les bonnes pratiques des personnels mis en place au sein de la gendarmerie nationale depuis 2007, et a été validée par le Service des technologies et des systèmes d'information de la sécurité intérieure (STSI2).

Cette base, hébergée au niveau groupement de gendarmerie et sécurisée via la connexion intranet, est alimentée par les enquêteurs, les techniciens en investigations criminelles de proximité (TICP) et les techniciens en investigations criminelles (TIC) puis exploitée par le coordinateur de la criminalistique (Cocrim) notamment. Elle est structurée en trois parties principales : les données administratives et judiciaires, le recueil des traces et le volet exploitation. Ce système permet l'insertion de tous types de traces criminalistiques : papillaires, génétiques, semelles, gants, pneumatiques, empreintes d'oreilles, outils, fibres, etc. Elle peut être ensuite exploitée par le Cocrim à des fins de

renseignement criminel (identification, rapprochements, etc.). Cette base a permis d'apporter une réelle plus-value dans le travail de renseignement criminel et se trouve également déployée dans cinq autres groupements de gendarmerie départementale.

Malgré tous les efforts déployés par l'instigateur de cette base de données, elle souffre de la méconnaissance de l'intérêt à porter à la trace d'outil lors des constatations aux dépens des traces papillaires ou génétiques. L'existence du FAED et du FNAEG laisse toujours supposer que la trace va délivrer un nom, encore faut-il que le donneur, son propriétaire, soit dans la base...

Il y a donc là un réel intérêt à se doter d'un système d'information géographique envisageant la problématique du traitement des traces d'outils dans la thématique des cambriolages.

Cela passe par l'élargissement des capacités de recueil de la trace en bannissant le recours à la seule recherche de la trace digitale et génétique. Il s'agit de systématiser le recueil, mais surtout la saisie et la remontée de tous les types de traces par les enquêteurs lors de leurs constatations et notamment la trace d'outil.

Cette opportunité ne peut s'avérer viable sans une sensibilisation des enquêteurs et surtout des TICP dans les unités élémentaires. Il faut en outre intégrer dans le cursus de formation des TICP, les méthodologies de criminalistiques associées à ces actes pour pouvoir garantir la légalité de leur action et du traitement ultérieur de la trace.

Dans le même temps, il faut doter ces personnels de matériels de prélèvement qui ne sont actuellement disponibles qu'au niveau TIC, ces derniers ne pouvant physiquement intervenir sur toutes les scènes de cambriolages, car ils sont en effectif limité au niveau de chaque département (capacité à réaliser un moulage de la trace d'outil lorsque le prélèvement du support s'avère impossible).

Pour pouvoir assurer ensuite l'analyse de l'intégralité de ces traces d'outils, il est également nécessaire de revoir la capacité du département MCA de l'IRCGN. Dans sa configuration actuelle, l'unité d'expertise Traces manufacturées de ce département ne peut traiter qu'un volume de 700 dossiers par an. Or, cette unité pourrait se trouver hypothétiquement face à plus de 150 000 faits. Même si cette unité a acquis une expérience reconnue dans le domaine de la comparaison des traces d'outils, l'ensemble des comparaisons de traces se fait toujours de façon manuelle. Une « bibliothèque » de



traces photographiées et/ou moulées couplée à une mémoire des traces du technicien permet de détecter les comparaisons pertinentes à réaliser. Néanmoins, ce processus chronophage et opératoire dépendant oblige les techniciens à limiter leurs rapprochements au niveau d'un département. Compte tenu d'une criminalité en perpétuel mouvement et s'affranchissant largement des frontières administratives, cette limitation géographique ne permet pas d'apporter une réponse efficiente aux requérants. Il y a là une réelle nécessité de montée en puissance du département en termes de capacité d'analyse. Cette nécessité, au-delà du nombre de personnels affectés au service, passe par la mise en place d'un outil informatique de numérisation systématique des traces et moulages, permettant d'accélérer le travail d'analyse et l'archivage des données. À cette fin, un système automatisé de comparaison de traces d'outils, le système TACS (Toolmarks Analysis Comparison System) est à l'étude et devrait se concrétiser en 2019. La mise en place d'un tel outil permettra d'apporter une réponse adaptée et optimale en termes de rapprochements sur une zone géographique étendue et d'accroître les capacités de traitement des experts en traces d'outils.

L'idée est de développer un système permettant de réaliser des comparaisons de traces d'outils de manière automatique. Ce système se diviserait en trois parties, à savoir un système d'acquisition d'image avec un éclairage optimisé, qui uniformiserait la saisie des traces, un logiciel spécifique dédié à l'incrémentement des traces dans une base de données ainsi que des algorithmes permettant la comparaison entre traces. Un parallèle technique est à faire avec le système EVOFINDER pour la comparaison

de stigmates de tir pour la balistique et l'appliquer au domaine des traces d'outils.

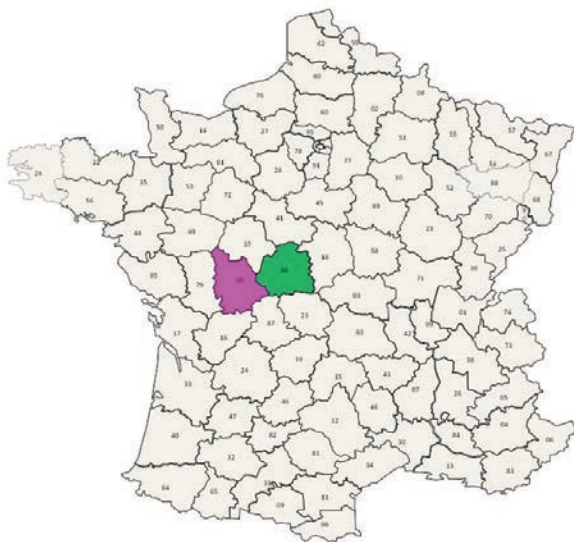
Perspectives : un cambriolage a lieu toutes les 90 secondes en FRANCE (zones gendarmerie et police confondues) et une effraction est généralement produite pour pénétrer dans les lieux où assez souvent le barillet est retrouvé brisé. Cela se fait par effraction du cylindre. C'est le mode d'effraction le plus courant, essentiellement parce qu'un cambrioleur chevronné, à l'aide de cette technique, mettra dans la plupart des cas moins d'une minute pour ouvrir une porte. Concrètement, le cambrioleur, avec un outil adapté, vient saisir le cylindre et appliquer un bras de levier jusqu'à rupture. Il ne lui reste plus ensuite qu'à glisser un crochet dans la serrure et le tour est joué.

Alors que les enquêteurs de certaines régions ne sollicitent que très rarement les experts du département MiCroAnalyse de l'IRCGN, d'autres qui ont compris la plus-value que peut apporter la prise en compte des traces d'outils le saisissent régulièrement.

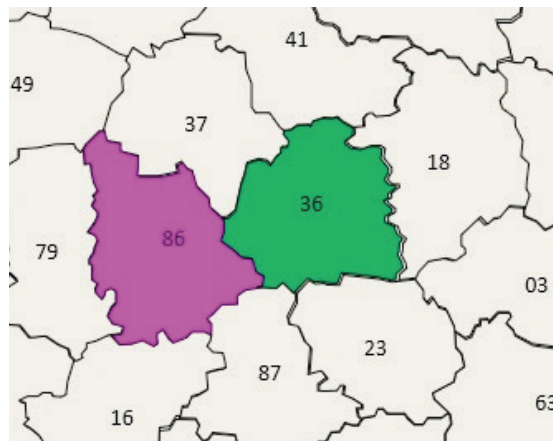
La plus-value pourrait être d'autant plus grande s'il était possible de répondre de manière plus efficiente et pour une zone géographique plus étendue.

Ainsi des rapprochements formels, mettant en évidence l'utilisation d'un seul et même outil, deviendraient possibles entre des procédures issues de départements différents et ce dans des délais moindres.

Prenons ici les exemples de La Vienne (86 – Région Nouvelle Aquitaine) et de l'Indre (36 – Région Centre-



(Source IRCGN)



(Source IRCGN)

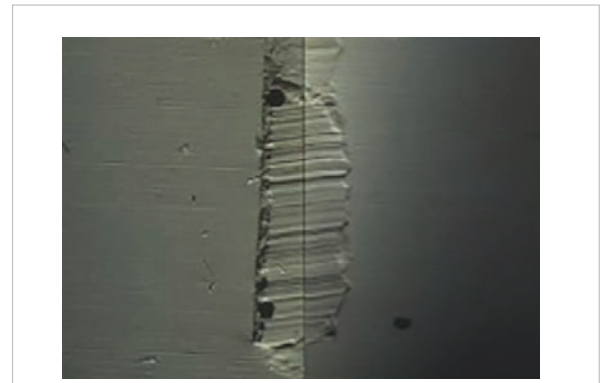
Val de Loire) où avec les techniques et moyens actuels à sa disposition, et sur une forte suspicion de l'enquêteur, l'expert a réussi à recouper, plus ou moins laborieusement, des procédures issues de faits s'étant déroulés sur toute l'année 2018. L'utilisation d'un outil automatisé tel que TACS, cumulé à un système d'information géographique, aurait permis de gagner en efficacité et en délais de traitement, en apportant des informations non négligeables pour les enquêteurs, dans le but de résoudre davantage de faits.

À noter que certains départements frontaliers ont déjà établi des conventions avec les pays voisins afin de réaliser des rapprochements sur des bris de barillet.

Une première version du système automatisé de comparaison de traces d'outils se limitera aux traces de pesée sur barillet, traces les plus fréquemment rencontrées au sein de l'unité d'expertise « Traces manufacturées » (entre 200 et 300 supports par an). De plus il s'agit de traces dont les caractéristiques se prêtent le plus facilement à la comparaison automatique. Le système pourrait ensuite s'améliorer et intégrer d'autres traces d'outils rencontrées sur différents supports (emboutissage de plaques d'immatriculation, cadenas, câbles sectionnés, maillons de chaînes coupées, pneumatiques...).

## Conclusion

La trace, vestige de l'acte criminel, est un reflet observable, mesurable, objectif et fidèle, même si fragmentaire et imparfait, du passé. Dans le système actuel, l'information issue de la trace est utilisée pour orienter les investigations



Exemple de la comparaison de deux traces (moules) de clés à molette, réalisée à l'aide d'un microscope de comparaison.

On note les similitudes entre les caractéristiques individuelles (microstriations) qui permettent d'affirmer que le même outil est à l'origine des deux traces.

des enquêteurs, permettre l'individualisation, voire l'identification de la source et/ou de l'auteur des faits.

Une approche SIG de ces phénomènes devrait permettre de rendre encore plus efficaces les actions de prévention et les investigations des enquêteurs en augmentant le taux de résolution des faits de cambriolages.

De même, tendre vers davantage de recoupements et de mise en évidence de phénomènes « sériels » ou « organisés » grâce à un système automatisé donnera à l'autorité judiciaire plus d'informations concrètes et établies, permettant d'en incriminer les auteurs ■

## Bibliographie

BOUMAIL (A.), 2010, *Évaluation du nombre limite d'utilisations d'un outil à partir duquel les caractéristiques individuelles sont suffisamment modifiées pour empêcher l'identification*, Rapport de stage présenté et soutenu pour l'obtention du Master I Chimie et Matériaux, université Paris-Est Créteil, année universitaire 2009-2010.

HUBERT (C.), 2017, *Approche de la problématique des vols par effraction par les traces d'outils : point de situation et avenir*, Mémoire présenté et soutenu publiquement pour l'obtention du Master II Droit et stratégies de la sécurité, CHOUVEL (F.) (dir.), université Panthéon-Assas-Paris II, Droit-Économie-Sciences sociales, année universitaire 2016 – 2017.

TOSO (B.), 1995, « Quels sont les outils qui peuvent laisser des traces de faibles ou fortes valeurs identificatrices », Séminaire de deuxième année, Institut de police scientifique et de criminologie, Université de Lausanne.

VAN DIJK (T.M.), 1995, « Toolmark Identification », *Expert Evidence*, Freckelton I. and Selby H., The Law Book Company Limited, 4, 2501-2752.

# La police et les contradictions de l'individualisme post-moderne

Jean-Louis LOUBET DEL BAYLE



Ce n'est pas une hypothèse sans fondement de penser que l'histoire de la fonction et des institutions policières reflète pour une grande part l'évolution générale de la société. Aussi réfléchir sur la police et ses problèmes conduit souvent à retrouver les questions fondamentales que sociologues, politologues, historiens ou philosophes peuvent se poser sur le devenir des sociétés. Tel est bien le sentiment qu'éprouve le sociologue de la police en relisant par exemple l'ouvrage de Gilles Lipovetsky, *L'ère du vide. Essais sur l'individualisme contemporain*<sup>1</sup>. Celui-ci, publié en 1983, a constitué une contribution importante et remarquée à une réflexion sur l'évolution individualiste des sociétés modernes dont la lecture reste aujourd'hui très riche d'enseignements pour comprendre des situations et des événements qui, eux, sont très contemporains. Il n'est donc pas sans intérêt de voir comment, trente ans

plus tard, cette relecture peut aider à comprendre une évolution de fond des sociétés occidentales qui est encore en cours, avec des conséquences qui restent d'actualité.

Le point de départ de cette étude ambitieuse est, en effet, une analyse de l'évolution des sociétés occidentales, qui voit dans un certain nombre de phénomènes caractéristiques des dernières décennies un dénominateur commun : l'émergence d'un individualisme entrant dans un nouveau stade historique propre aux sociétés démocratiques avancées, qui définirait spécifiquement ce que l'auteur appelle « l'âge postmoderne ». Cette transformation culturelle profonde se traduirait fondamentalement par un processus de personnalisation s'ordonnant autour d'une valeur essentielle, celle de l'accomplissement personnel, celle du respect de la singularité subjective de chaque individu. La formule pirandellienne « *À chacun sa vérité* » deviendrait la maxime de base d'une culture « *visant à permettre le libre déploiement de la personnalité intime, à légitimer la jouissance, à reconnaître les demandes singulières, à modeler les institutions sur les aspirations des individus* » [p. 10].

Jean-Louis LOUBET DEL BAYLE



Professeur émérite de Science politique à l'Université des sciences sociales de Toulouse-Capitole.

(1) Paris, Gallimard, 1963, 250 p.



Cette promotion de l'individu comme valeur suprême serait le point commun à des phénomènes aussi divers que l'importance croissante accordée à la vie privée, l'érosion des identités sociales, le déclin des grands systèmes, idéologiques, le désintérêt pour la politique, l'exaltation de la spontanéité et la méfiance à l'égard des organisations, le pluralisme des modes et des styles de vie, la désuétude des rites sociaux, l'explosion et la diversité des activités associatives, le succès des valeurs hédonistes, psychologues et permissives au détriment des valeurs ascétiques, le respect des différences et le souci de l'épanouissement individuel, le goût de la décontraction, de l'humour et de la sincérité, l'attrait du naturel et de la cordialité, la réhabilitation de l'affectif et de l'irrationnel, l'occultation de la mort et le culte du corps, la plasticité et la fragilité des personnalités, etc.

Sur ces bases culturelles, tendrait à se construire une société « personnalisée », où « l'important est d'être soi-même, où n'importe quoi, dès lors, a droit de cité et de

reconnaissance sociale, où plus rien ne doit s'imposer impérativement et durablement, où toutes les options peuvent cohabiter sans contradiction ni relégation » [p.14]. Une société caractérisée par « *le moins de contrainte et le plus de choix privés possibles, avec le moins d'austérité et le plus de désir possible, avec le moins de coercition et le plus de compréhension possible* » [p. 9]. C'est une « mutation sociologique globale » [p. 8] qui serait ainsi en cours, en rupture avec le mode d'organisation traditionnel des sociétés, que l'auteur qualifie de « *disciplinaire* », qui socialisait l'individu en l'immergeant dans un système homogène de normes à caractère général, sous forme de conventions sociales, d'impératifs moraux, de règlements fixes et standardisés qui, de manière plus ou moins directe, se traduisait par une subordination de l'individu à des règles censées exprimer une rationalité collective.

Si, pour l'auteur de *L'ère du vide*, la période récente s'est traduite par l'épanouissement de cet individualisme post-moderne dans tous les domaines, ce phénomène

n'est pas cependant le produit d'une sorte de génération spontanée, mais le résultat d'une évolution amorcée depuis plusieurs siècles, qui s'est brutalement accélérée au cours des dernières décennies, en allant jusqu'au bout d'un processus inauguré par le développement de l'État et du capitalisme et poursuivi par l'avènement des sociétés démocratiques et de la consommation de masse. À la fois cause et conséquence de ces changements, la mutation culturelle qu'a représentée l'émergence de cet individualisme ne s'est donc opérée que progressivement, en ne libérant que lentement les virtualités dont elle était porteuse, l'individualisme post-moderne représentant alors en quelque sorte le stade ultime de cette laborieuse genèse, après une maturation qui a souvent mêlé des vestiges des temps anciens aux novations dont était grosse cette nouvelle logique sociale.

Telle est donc la « lecture » de l'évolution des sociétés occidentales que faisait l'ouvrage de Gilles Lipovetsky. Cette réflexion générale

rejoint, trente ans après, les préoccupations du sociologue de la police dans un dernier et important chapitre qui, à la lumière de cette hypothèse, proposait une suggestive analyse de l'histoire de la violence et de l'évolution de la gestion sociale de celle-ci, afin de comprendre « *l'irrésistible mouvement de pacification de la société* » [p. 195], qui, selon l'auteur, en dépit des apparences, a accompagné l'avènement de l'individualisme post-moderne.

Remontant quasiment aux origines de l'humanité, l'auteur évoque d'abord les millénaires qui ont vu régner ce qu'il appelle la « *violence sauvage* » de sociétés régulées en ce domaine par les codes de l'honneur et de la vengeance. Selon lui, dans ces sociétés, le recours à la violence était pour les individus non seulement une nécessité vitale, « *utilitaire* », pour survivre, mais aussi une sorte d'obligation morale, d'une part, pour construire leur image sociale, en s'assurant l'estime de leurs semblables (code de l'honneur), et, d'autre part, pour prouver leur solidarité avec les membres de leur groupe en punissant l'offense faite à ceux-ci, vivants ou morts (code de la vengeance).

À partir de là, la thèse de G. Lipovetsky est que la cruauté et la « *violence privée* » des sociétés « *sauvages* » n'étaient pas le résultat d'une impulsivité naturelle non maîtrisée, mais le produit de sociétés « *holistes* », fondées sur un contrôle social « *sociétal* » ou « *communautaire* », dans lesquelles l'individu n'avait d'existence que sociale, et n'avait pas d'autre choix que de vivre par rapport aux autres, en s'identifiant aux membres du groupe auquel il appartenait. Ainsi, d'une manière quelque peu paradoxale, le déchaînement de la violence privée serait ici le produit d'une écrasante pression sociale pesant sur les individus et les obligeant à traduire par la violence leur subordination au groupe et à ses normes, car, dans

ce contexte, « *personne ne peut laisser le crime ou l'offense impunis, personne ne détient le monopole de la force physique, personne ne peut renoncer à l'impératif de verser le sang ennemi, personne ne peut s'en remettre à personne pour assurer sa sécurité* » [p. 201].

Ces sociétés « *sauvages* » sont de ce fait, par définition, des sociétés pré-étatiques, sans organisation politique, car « *en faisant de la vengeance un devoir imprescriptible tous les hommes sont égaux devant la violence, aucun ne peut monopoliser la force ou y renoncer, aucun n'a à être protégé par une instance spécialisée* » [p. 201]. Au contraire, c'est en créant cette « *instance spécialisée* » qu'est un pouvoir politique, que l'humanité va passer au stade « *barbare* » puis « *civilisé* » de son développement, avec l'apparition d'une nouvelle logique tendant à l'éradication, ou, au moins, au contrôle de la violence « *privée* », tant à l'extérieur – guerre – qu'à l'intérieur du groupe. Par exemple, par la monopolisation publique des capacités guerrières et par l'organisation d'une justice publique se substituant à la vengeance privée. Néanmoins, si la logique de l'organisation politique est celle-là, cette logique ne s'est affirmée que progressivement et, pendant longtemps, ont subsisté des vestiges des pratiques antérieures, comme le prouve la persistance jusqu'à une période relativement récente du duel ou de la vendetta.

En fait, dans les sociétés occidentales, c'est à partir du XVIII<sup>e</sup> siècle que cette évolution se concrétise véritablement et que le développement de l'État et de sa fonction « *policrière* » contribue à rendre progressivement inutile le recours privé à la violence et à pacifier les rapports sociaux. « *Lorsque n'existe aucun monopole militaire et policier et que, partout, l'insécurité est constante, l'agressivité est une nécessité vitale. En revanche, à mesure que se développe la division des fonctions sociales et que, sous l'action des organes centraux monopolisant*

*la force physique, s'institue une large sécurité quotidienne, l'emploi de la violence individuelle s'avère exceptionnel* » [p. 214].

Ainsi, avec le développement de l'État, comme, sur un autre plan, avec l'apparition de l'économie de marché, s'amorce l'émergence de l'individu au sein d'un type de société dans laquelle l'homme individuel tend progressivement à se considérer isolément, avec pour fin ultime sa survie et son intérêt propre. « *Le risque de la mort cesse d'être une valeur, se battre n'est plus glorieux. La violence n'a plus de sens social, n'est plus moyen de reconnaissance et d'affirmation, dans un temps où se trouvent sacralisés la longévité, l'épargne, le travail, la prudence, la mesure* » [p. 218]. Toutefois, selon G. Lipovetsky, ce mouvement culturel, faisant apparaître de nouvelles valeurs et un rapport inédit de l'homme à la société, est autant la cause que la conséquence des changements politiques et économiques qui viennent d'être évoqués, ce processus d'individualisation étant en fait un processus global dans lequel les changements culturels sont aussi déterminants que les changements politiques et économiques.

Aujourd'hui, avec l'épanouissement post-moderne de ce processus de personnalisation arrivant au bout de sa logique, la violence s'effacerait progressivement du paysage social, en dépit des survivances de l'âge « *holiste* » que constitueraient certains phénomènes, comme les violences politiques des régimes totalitaires du XX<sup>e</sup> siècle. Ainsi, malgré les apparences, la diminution sur le long terme des homicides, des rixes, des coups et blessures volontaires, des agressions et cruautés dont étaient victimes femmes, enfants ou animaux, la disparition des châtiments corporels, l'humanisation des peines seraient autant de signes de cette évolution qui tend à faire de la violence « *au même titre et plus encore que la mort, l'interdit majeur de*



AINSI, AVEC LE DÉVELOPPEMENT DE L'ÉTAT,  
 COMME, SUR UN AUTRE PLAN, AVEC  
 L'APPARITION DE L'ÉCONOMIE DE MARCHÉ,  
 S'AMORCE L'ÉMERGENCE DE L'INDIVIDU AU  
 SEIN D'UN TYPE DE SOCIÉTÉ DANS LAQUELLE  
 L'HOMME INDIVIDUEL TEND PROGRESSIVEMENT  
 À SE CONSIDÉRER ISOLÉMENT, AVEC POUR FIN  
 ULTIME SA SURVIE ET SON INTÉRÊT PROPRE.  
 « LE RISQUE DE LA MORT CESSE D'ÊTRE UNE VALEUR,  
 SE BATTRE N'EST PLUS GLORIEUX. LA VIOLENCE  
 N'A PLUS DE SENS SOCIAL, N'EST PLUS MOYEN DE  
 RECONNAISSANCE ET D'AFFIRMATION, DANS UN  
 TEMPS OÙ SE TROUVENT SACRALISÉS LA LONGÉVITÉ,  
 L'ÉPARGNE, LE TRAVAIL, LA PRUDENCE, LA MESURE »



*nos sociétés* » [p. 224<sup>2</sup>]. Tout cela étant donc la conséquence d'un processus culturel de désocialisation et d'individualisation : « *De plus en plus repliés sur des préoccupations privées, les individus se pacifient non par éthique, mais par hyper-absorption individualiste dans l'indifférence au destin et aux jugements des autres* » [p. 224].

Telle serait la logique du développement des sociétés post-modernes qui s'accompagne – ce qui nous intéresse ici – d'une interprétation de la croissance de leur appareil policier. Celui-ci ne serait pas alors le produit d'une recrudescence de la violence, mais, au contraire, d'une allergie croissante de la majeure partie de la population à toute forme de violence : « *À mesure que les hommes se retirent dans leur sphère privée et n'ont en vue qu'eux-mêmes, ils ne cessent d'en appeler à l'État pour qu'il assure une protection plus constante, plus vigilante de leur existence* ».

C'est finalement à accroître les prérogatives et la puissance de l'État qu'œuvre le processus de civilisation : « *L'État policier n'est pas seulement l'effet d'une dynamique autonome du monstre froid, il est voulu par les individus désormais isolés et pacifiques. La multiplication des lois pénales, l'accroissement des effectifs et des pouvoirs de police, la surveillance systématique des populations sont les effets inéluctables d'une société où la violence est dévalorisée et où simultanément augmente le besoin de sécurité publique* » [p. 219].

Comme le soulignait encore Gilles Lipovetski, c'est donc, paradoxalement, un individualisme arrivant au bout de sa logique qui expliquerait un appel croissant à la protection de l'État et à l'intervention de « *professionnels de la sécurité* » : « *L'État moderne a créé l'individu détaché socialement de ses semblables, mais celui-ci en retour crée son isolement, son absence de bellicosité, sa peur de la violence, conditions*

*constantes de l'accroissement de la force publique. Plus les individus se sentent libres d'eux-mêmes, plus ils demandent une protection régulière, sans faille, de la part des organes étatiques ; plus ils exècrent la brutalité, plus l'augmentation des forces de sécurité est requise* » [p. 219].

Ce bref résumé permet de mesurer l'intérêt que cette lecture peut présenter aujourd'hui pour le sociologue de la police, en faisant apparaître des contradictions dont l'actualité permet de vérifier l'acuité, et en contribuant ainsi à éclairer la genèse de certains phénomènes très contemporains.

Une première contradiction latente liée à cette évolution tient au fait que, si l'individu post-moderne se décharge volontiers de l'exercice de la violence sur le monopole d'une institution spécialisée, son allergie à la violence concerne non seulement la violence qu'il serait susceptible d'exercer ou dont il serait susceptible d'être victime, mais aussi celle qui est exercée et subie par autrui. Comme le constatait déjà Tocqueville, l'individualisme entraîne une capacité d'identification à l'autre qui expliquerait que, malgré son indifférence générale à autrui, l'individu post-moderne se montre néanmoins très sensible au spectacle de la violence subie par d'autres<sup>3</sup>. Dans cette perspective, l'allergie à la violence de l'individualisme post-moderne peut aider à comprendre l'ambiguïté des réactions de l'opinion en face de l'institution policière, qui mêlent une tendance à un appel croissant à ses interventions et une attitude rapidement critique lorsque l'institution policière met en œuvre des moyens à caractère violent ou limitant l'autonomie individuelle. Ainsi, les mêmes motivations qui

(2) Cf. dans le même sens, Robert Muchembled, *Histoire de la violence*, Paris, Le Seuil, 2008.

(3) Tocqueville notait déjà cette capacité d'identification comme une conséquence de l'individualisme démocratique : « *s'agirait-il d'étrangers ou d'ennemis, l'imagination le met aussitôt à leur place : elle mêle quelque chose de personnel à sa pitié, et le fait souffrir lui-même tandis qu'on déchire le corps de son semblable* » (*La démocratie en Amérique*, Œuvres, Bouquins, 1986, p. 512).

poussent de plus en plus les individus à s'en remettre aux institutions policières pour leur sécurité les rendent aussi réticents devant les moyens que ces institutions sont amenées à utiliser pour atteindre cet objectif.

Ce problème est d'autant plus réel que si l'individualisme postmoderne entraîne une pacification globale de la vie sociale dans son ensemble, la déstructuration des relations et des normes sociales qu'il engendre laisse néanmoins subsister des abcès de violence, qui ont certes un caractère minoritaire et résiduel, mais qui n'en sont pas moins ressentis comme dangereux. D'une part, parce qu'ils ont tendance à échapper à toute régulation sociale et, d'autre part, parce qu'ils sont d'autant plus perturbateurs qu'ils sont résiduels, dans des sociétés qui sont à la fois matériellement et psychologiquement fragiles. L'irrationalité d'un grand banditisme « hors milieu », le développement du terrorisme, les explosions de guérilla urbaine seraient ainsi des symptômes de l'ambivalence de cet individualisme post-moderne qui, dans la majorité des cas, favorise un repliement narcissique et pacifique sur la sphère de la vie privée, mais qui, pour une minorité, aboutit « à une montée aux extrêmes désacralisée et cynique, liée à la liquéfaction des principes, encadrements et autocontrôles » [p. 235]. Une autre contradiction apparaît donc ici, avec les problèmes posés par le contrôle social de ces foyers de violence « résiduelle », dans une société par ailleurs fondamentalement non-violente et respectueuse de l'autonomie individuelle, et, qui, de ce fait, est d'autant plus vulnérable et exposée à l'influence déstabilisatrice de cette violence.

Plus largement, une autre contradiction de l'individualisme post-moderne tient sans doute au fait que cette évolution individualiste



L'ALLERGIE À LA VIOLENCE DE L'INDIVIDUALISME POST-MODERNE PEUT AIDER À COMPRENDRE L'AMBIGUÏTÉ DES RÉACTIONS DE L'OPINION EN FACE DE L'INSTITUTION POLICIÈRE, QUI MÊLENT UNE TENDANCE À UN APPEL CROISSANT À SES INTERVENTIONS ET UNE ATTITUDE RAPIDEMENT CRITIQUE LORSQUE L'INSTITUTION POLICIÈRE MET EN ŒUVRE DES MOYENS À CARACTÈRE VIOLENT OU LIMITANT L'AUTONOMIE INDIVIDUELLE. AINSI, LES MÊMES MOTIVATIONS QUI POUSSENT DE PLUS EN PLUS LES INDIVIDUS À S'EN REMETTRE AUX INSTITUTIONS POLICIÈRES POUR LEUR SÉCURITÉ LES RENDENT AUSSI RÉTICENTS DEVANT LES MOYENS QUE CES INSTITUTIONS SONT AMENÉES À UTILISER POUR ATTEINDRE CET OBJECTIF.



aboutit paradoxalement à limiter d'une certaine manière l'autonomie effective de l'individu au profit des institutions auxquelles il s'en remet pour assurer sa sécurité. L'exaltation post-moderne de l'individualité pourrait être ainsi en partie illusoire et se payer d'une perte effective psychologiquement peu sensible, parce que peu perceptible dans la vie quotidienne et, surtout, parce que se réalisant à travers des mécanismes sociaux lointains, abstraits et complexes, dont la signification est difficilement saisissable par les individus. Le sentiment subjectif d'insécurité qui augmente, alors que diminue le niveau objectif de violence, pourrait d'ailleurs être la conséquence de cette contradiction et « le corrélat inéluctable d'un individu déstabilisé, désarmé, amplifiant tous les risques, obsédé par ses problèmes personnels, habitué à être protégé, traumatisé par une violence dont il ignore tout » [p. 230].

Ces considérations inspirées par le livre de G. Lipovetsky, ou suggérées

par celui-ci au lecteur, conduisent le lecteur d'aujourd'hui, encore plus que le lecteur d'hier, à s'interroger sur la dissolution des normes collectives qui semble être le revers de l'individualisme post-moderne et de son respect de l'autonomie des choix individuels. Cette orientation a, en effet, pour conséquence de saper les mécanismes de régulation culturelle assurant la coordination des comportements individuels par l'adhésion intériorisée à un système de valeurs et de normes communes et l'on peut se demander si, à terme, ce phénomène n'est pas, lui aussi, susceptible de contribuer à une dérive « policière » des sociétés post-modernes, celles-ci pouvant être conduites à compenser par des contraintes externes des contraintes institutionnelles, comme la dissolution de leur armature culturelle. C'est, par exemple, cette question, qui reste d'actualité, que posait il y a déjà quelques décennies un politologue comme Maurice Duverger, lorsqu'il écrivait : « Les sociétés ne peuvent se maintenir que par un

*mécanisme d'ordre. Elles doivent intérioriser cet ordre pour que les contraintes deviennent moins fortes... Quand les gens croient plus à des systèmes de valeurs, la société ne se maintient plus que par la police<sup>4</sup>*. Ainsi, même si on peut être tenté de considérer cette affirmation comme, peut-être, un peu trop catégorique, celle-ci conduit à se demander si l'individualisme post-moderne ne porte pas de ce fait en lui des contradictions qui peuvent conduire à douter de ses capacités de survie, sur le long terme notamment.

Si cette analyse, avec les contradictions qu'elle fait apparaître, conserve toute sa pertinence pour déchiffrer l'évolution des sociétés occidentales, on peut s'interroger sur son lien avec certaines innovations sociales caractérisant les années les plus récentes, notamment avec l'influence de ce qu'il convient d'appeler les « réseaux sociaux ». Combinés aux médias, ceux-ci semblent en effet capables de susciter des réactions sociales soudaines, d'apparence spontanée, stigmatisant telle ou telle opinion, tel ou tel comportement, ce que l'on peut être tenté de considérer comme un démenti aux tendances de fond de l'individualisme post-moderne et à la tolérance sociétale généralisée qui le caractérise. En termes sociologiques, la question est alors de savoir si ces phénomènes constituent un embryon de retour à des formes de contrôle social « sociétal » spontané, immédiat, fondé sur une pression sociale « normalisatrice » directe de l'opinion – que l'individualisme postmoderne avait marginalisé. Ou bien s'il s'agit là de phénomènes, plus ou moins artificialisés

et instrumentalisés par leur médiatisation, qui finissent d'ailleurs le plus souvent par se traduire par des revendications institutionnelles – édicton de lois et de règlements et appel à des interventions policières ou judiciaires – en illustrant les rapports contradictoires évoqués précédemment entre l'atomisation des repères culturels et le progrès des contraintes institutionnelles.

Même si les thèses anthropologiques exposées par Gilles Lipovitsky peuvent prêter à discussion, en particulier lorsqu'il écarte un peu catégoriquement ce qu'il appelle les interprétations « utilitaires » de l'histoire de la violence, et même si le sociologue soucieux d'une approche empirique de la réalité est tenté de se montrer circonspect devant la fresque ambitieuse qu'il brosse et devant la « *mutation sociologique* » qu'il diagnostique, on ne peut cependant rester indifférent aux hypothèses qu'il avançait il y a trente ans, qui restent d'une surprenante et éclairante actualité pour interpréter certains aspects de l'évolution la plus récente des sociétés occidentales. En particulier, celles-ci sont loin d'être sans intérêt pour le sociologue de la police s'interrogeant sur l'histoire et le devenir contemporain des institutions policières, en soulignant à quel point l'histoire de la fonction et de l'institution policières est associée aux problèmes les plus fondamentaux concernant l'évolution des sociétés, de leur culture et de leur organisation politique.

Si cette analyse, avec les contradictions qu'elle fait apparaître, conserve toute sa pertinence pour

déchiffrer l'évolution des sociétés occidentales, on peut s'interroger sur son lien avec certaines innovations sociales caractérisant les années les plus récentes, notamment avec l'influence de ce qu'il convient d'appeler les « réseaux sociaux ». Combinés aux médias, ceux-ci semblent en effet capables de susciter des réactions sociales soudaines, d'apparence spontanée, stigmatisant telle ou telle opinion, tel ou tel comportement, ce que l'on peut être tenté de considérer comme un démenti aux tendances de fond de l'individualisme post-moderne et à la tolérance sociétale généralisée qui le caractérise. En termes sociologiques, la question est alors de savoir si ces phénomènes constituent un embryon de retour à des formes de contrôle social « sociétal » spontané, immédiat, fondé sur une pression sociale « normalisatrice » directe de l'opinion – que l'individualisme postmoderne avait marginalisé. Ou bien s'il s'agit là de phénomènes, plus ou moins artificialisés et instrumentalisés par leur médiatisation, qui finissent d'ailleurs le plus souvent par se traduire par des revendications institutionnelles – édicton de lois et de règlements et appel à des interventions policières ou judiciaires – en illustrant les rapports contradictoires évoqués précédemment entre l'atomisation des repères culturels et le progrès des contraintes institutionnelles ■

(4) Cité par *Le Figaro*, 15/1/1978.



# Passage à l'acte État de la recherche internationale

Jacques DUBUCS

L'article analyse la littérature récente relative au passage à l'acte dans le domaine du crime et du terrorisme. La conception du passage à l'acte proposée dans les années 1980 par la théorie situationnelle de la prévention du crime reposait sur une hypothèse d'optimalité : les criminels procèdent au mieux compte tenu des informations dont ils disposent. Elle avait pour conséquence une politique de prévention consistant à fournir aux délinquants un supplément d'informations supposées les dissuader de passer à l'acte, comme la multiplication ostensible des caméras de surveillance. Le développement des sciences du comportement rend l'hypothèse d'optimalité largement caduque, et suggère d'appuyer une politique de prévention sur les « biais cognitifs » sous-jacents au comportement effectif des délinquants. Sur cette base, peut être développée une criminologie « expérimentale » mieux fondée sur les données disponibles. Reste alors à articuler, dans ces données, celles qui résultent de l'expérience intuitive et directe des policiers et celles qui sont déposées dans les larges bases qui enregistrent les actes délictueux. Des arguments sont donnés pour écarter, en criminologie comme en médecine, le remplacement pur et simple de la connaissance intuitive des praticiens par le recours à des *Big Data* et l'idée de « systèmes d'apprentissage continu » est proposée et discutée en lieu et place de cette substitution. Quelques conséquences en sont tirées pour la situation française en matière de recherche sur la sécurité.

This article reviews recent literature on the subject of deeds in the field of crime and terrorism. The concept of action proposed in the 1980s by situational crime prevention theory was based on an assumption of optimality : criminals proceed as best they can with the information at their disposal. As a result, it resulted in a prevention policy aiming to provide offenders with additional information that was supposed to deter them from taking action, such as the ostensible increase in the number of surveillance cameras. The development of behavioural sciences renders the optimality hypothesis largely obsolete, and suggests that a prevention policy should be based on the «cognitive biases» underlying the effective behaviour of offenders. On this basis, an «experimental» criminology can be developed that is better based on the available data. It remains to articulate, in these data, those resulting from the intuitive and direct experience of the police officers and those deposited in the large databases that record criminal acts. Arguments are given to rule out, in both criminology and medicine, the outright replacement of practitioners' intuitive knowledge by the use of Big Data and the idea of «continuous learning systems» is proposed and discussed in place of this substitution. Some conclusions have been drawn for the French situation in terms of security research.

## Jacques DUBUCS



Jacques Dubucs est directeur de recherche dans le laboratoire Sciences, Normes, Démocratie (CNRS/Sorbonne Université). Ses domaines de spécialisation sont la logique, les sciences cognitives et la philosophie des sciences. Il est directeur scientifique du Département des sciences de l'homme et de la société à la direction générale de la Recherche et de l'Innovation (ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation).



On distingue couramment entre les facteurs (raisons ultimes, *drivers*, *roots*) qui expliquent ou favorisent les processus et les facteurs (*triggers*) qui déclenchent ces processus ou font passer à l'acte (*acting out*) les entités qui y sont impliquées.

En ce qui concerne les processus d'action terroriste, l'examen des bases de données internationales montre que la littérature de recherche consacrée au passage à l'acte est extrêmement minoritaire (moins de 10 %) par rapport à celle qui est consacrée aux causes lointaines (souvent qualifiées de « vraies causes ») du terrorisme, à ses contextes socio-économiques, à ses corrélats historiques et à son interprétation d'ensemble.

Cette prévalence de la recherche « distale » est particulièrement nette en France, ce qui tient probablement aux paradigmes dominants, au plan national, dans le domaine des sciences de l'homme et de la société (SHS) : elles y sont encore, comme elles l'étaient dans la seconde moitié du XX<sup>e</sup> siècle à l'époque des « Grands penseurs », marquées par la prévalence d'un paradigme historisant et interprétatif, au détriment d'un paradigme « modélisant », plus soucieux de formulation explicite d'hypothèses et d'évaluation de ces hypothèses sur la base de données empiriques consolidées.

Les conséquences de cette particularité des SHS françaises sur la recherche relative à la radicalisation et au terrorisme, conformes à ce à quoi l'on pouvait s'attendre, ont été explicitement tirées dès le mois de mai 2016 dans le Plan d'action contre la radicalisation et le terrorisme, qui distinguait (p. 49) entre un horizon de recherche fondamentale à long terme et la nécessité d'un transfert accru à échéance brève.

Sur le premier plan, il s'agit de trancher l'actuel « conflit des interprétations » (historiens, sociologues), sommairement résumé dans l'alternative entre radicalisation de l'islam (exacerbation clivante de pratiques se référant à certaines conceptions radicales de l'islam actuellement en expansion dans nombre de pays musulmans) et islamisation de la radicalité (expression religieuse de surface pour des comportements ayant leur origine réelle dans un processus de désintégration sociale affectant la société française et notamment sa jeunesse).

Le texte du Plan d'action souligne, d'une part, que nous manquons du recul historique requis pour arbitrer ce conflit d'interprétations relatif aux « causes profondes » des phénomènes de radicalisation, d'autre part, que l'action publique est confrontée à des décisions qui doivent être prises dans un horizon temporel plus bref que celui-là. Il invite, en conséquence, à organiser une action immédiate de transfert accru de la recherche vers la décision publique : il est souhaité que les orientations de la politique publique dans le domaine de la lutte contre la radicalisation puissent s'appuyer sur des données et sur des préconisations concrètement implémentables.

Cette orientation demande donc une attention accrue à la recherche portant sur les mécanismes « proximaux » du passage à l'acte. La présente note vise à présenter un état sommaire de la recherche internationale sur cette question.

## Difficultés particulières de la recherche relative au passage à l'acte

La faiblesse comparative de la recherche sur le passage à l'acte résulte avant tout d'une difficulté générique, qui peut être illustrée assez simplement dans le domaine de la physique nucléaire.

On sait déterminer la période de demi-vie d'une substance radioactive, c'est-à-dire le temps nécessaire à cette substance pour que sa radioactivité soit réduite de moitié. On connaît ici la cause « profonde » du processus (l'instabilité atomique caractéristique de la substance considérée) et on sait même la quantifier avec précision, mais il n'en découle aucune information sur le moment précis du déclenchement de ce processus (éjection d'une particule chargée) au niveau d'un atome individuel pris parmi ceux dont la substance est composée.

Autrement dit, même dans le monde très simple des atomes, il n'existe aucune théorie déterministe du « passage à l'acte » individuel : le mieux qui peut être fait, en matière de prévision, est d'indiquer le délai au terme duquel un atome particulier aura une chance sur deux d'avoir éjecté une particule chargée.

Or, en passant de la physique nucléaire à la criminologie, les choses se compliquent :

- si le changement d'état d'un atome isolé n'a aucune incidence macroscopique, le passage à l'acte d'un individu peut en avoir de considérables au plan social ;
- la décroissance radioactive est « intrinsèque », c'est-à-dire ne peut être modifiée par aucun processus adventice, alors même que nous espérons non seulement anticiper, mais prévenir les passages à l'acte terroriste

La théorie « standard », pour répondre à cette difficulté, est la « théorie situationnelle », qui joue toujours un rôle de premier plan en criminologie. Elle soulève un certain nombre de difficultés, notamment dans son application aux phénomènes terroristes. D'autres perspectives sont aujourd'hui en compétition avec cette théorie, reposant notamment sur les sciences du comportement.

## La théorie situationnelle (Situation Crime Prevention) du passage à l'acte

Cette théorie, déjà ancienne, représente un paradigme dominant dans la littérature criminologique anglo-saxonne. Elle met en avant une distinction tranchée entre les *drivers* des actes criminels et les facteurs qui les déclenchent, et elle propose une conception unitaire de ces derniers. Elle tire de cette conception un ensemble de dispositions pratiques destinées à prévenir le passage à l'acte, et ces dispositions ont été largement mises en œuvre par la police et les institutions en charge du maintien de l'ordre.

L'article séminal, pour la théorie situationnelle, est de Ronald V. Clarke, «Situational Crime Prevention: Theory and Practice», *British Journal of Criminology*, 1980, p. 136-147.

Le point de départ de Clarke (criminologue britannique, professeur à Rutgers U. de 1987 à 1998) est simple : il faut s'intéresser non au criminel, à sa situation sociale objective et aux causes distales que nous pourrions attribuer à ses actes, mais au crime lui-même et à ce qui le déclenche. Un criminel passe à l'acte lorsqu'il pense avoir de bonnes raisons de le faire, c'est-à-dire lorsque les bénéfices qu'il escompte de la commission de l'acte l'emportent sur les bénéfices qu'il croit pouvoir attendre de son abstention.

Autrement dit, le criminel agit parce qu'il est rationnel et qu'il sait calculer son intérêt. Naturellement, cette rationalité est d'ordre « instrumental » et non pas « cognitif » : son estimation subjective de la rentabilité de son acte et de la probabilité d'être pris peut être erronée, et les objectifs qu'il poursuit peuvent être absurdes. Néanmoins, le calcul qu'il effectue sur ces bases « exogènes » est un calcul rationnel : en agissant comme il le fait il maximise bel et bien son « utilité espérée », et le constat selon lequel l'acte délictueux possède à ses yeux une utilité positive joue précisément le rôle de déclencheur de cet acte.

Cette théorie situationnelle est évidemment de toute beauté.

D'une part, elle évite de traiter les actes criminels comme des actes *sui generis* : le genre d'explication proposée par Clarke pour le comportement criminel pourrait s'appliquer, *mutatis mutandis*, au choix des plats dans un restaurant ou aux dispositions financières que prennent les salariés pour préparer leur retraite. Toutes les actions humaines sont rationnelles au regard des opinions et des



AUTREMENT DIT, LE CRIMINEL AGIT PARCE QU'IL EST RATIONNEL ET QU'IL SAIT CALCULER SON INTÉRÊT. NATURELLEMENT, CETTE RATIONALITÉ EST D'ORDRE « INSTRUMENTAL » ET NON PAS « COGNITIF » : SON ESTIMATION SUBJECTIVE DE LA RENTABILITÉ DE SON ACTE ET DE LA PROBABILITÉ D'ÊTRE PRIS PEUT ÊTRE ERRONÉE, ET LES OBJECTIFS QU'IL POURSUIT PEUVENT ÊTRE ABSURDES. NÉANMOINS, LE CALCUL QU'IL EFFECTUE SUR CES BASES « EXOGÈNES » EST UN CALCUL RATIONNEL : EN AGISSANT COMME IL LE FAIT IL MAXIMISE BEL ET BIEN SON « UTILITÉ ESPÉRÉE », ET LE CONSTAT SELON LEQUEL L'ACTE DÉLICIEUX POSSÈDE À SES YEUX UNE UTILITÉ POSITIVE JOUE PRÉCISÉMENT LE RÔLE DE DÉCLENCHÉUR DE CET ACTE.



préférences de leurs auteurs, et ces actions sont justement déclenchées, après calcul, par le constat de cette rationalité.

La pertinence alléguée de la théorie du choix rationnel pour la criminologie est systématiquement défendue dans Derek B. Cornish & Ronald V. Clarke, *The Reasoning Criminal. Rational Choice Perspectives on Offending*, Springer Verlag, New York, 1986, rééd. Transaction Publ., New-Brunswick, NJ, 2014

Les auteurs y soulignent que la rationalité de l'action criminelle doit s'entendre non en un sens objectif, mais rapportée à la façon subjective dont les délinquants perçoivent leur environnement : « *C'est l'idée selon laquelle les délinquants se comportent dans des situations (environnements physiques et sociaux) selon la façon dont ils les perçoivent [...] Pour un observateur extérieur de leur comportement, les actions entreprises par les délinquants peuvent ou non apparaître*

*rationnelles. Mais le délinquant lui-même perçoit son comportement comme un moyen rationnel de parvenir à une fin ».*

D'autre part, la théorie situationnelle est en mesure de conduire à des préconisations définies en matière de prévention du crime. Elle mène directement à de la recherche opérationnelle, qui a pour objectifs de rendre le crime plus difficile à accomplir sans être pris, moins rentable une fois effectué et plus lourd à expier si l'on est jugé<sup>1</sup>, mais surtout de rendre ces changements notoires aux criminels. Puisque c'est la positivité de l'utilité espérée qui déclenche le passage à l'acte, on prévient ce passage en diminuant cette utilité, telle que calculée par le criminel en puissance. Dans les termes de Clarke, il conviendra donc de « *rendre le crime plus difficile ou risqué, ou moins rentable et excusable aux yeux d'un large spectre de délinquants* ». En bref, on laisse intact les *drivers* (il ne s'agit pas de « *chercher à éliminer le criminel ou les tendances délinquantes grâce à une amélioration de la société hors de ses institutions* », car de tels objectifs sont à la fois hasardeux à poursuivre et d'efficacité trop lointaine<sup>2</sup>), et l'on s'attache plutôt à inactiver les *triggers*.

Un livre, qui cumule près de 2 500 citations académiques, a constitué ici une référence centrale pour la criminologie anglo-saxonne : Ronald C. Clarke (ed.), *Situational Crime Prevention. Successful Case Studies*, Harrow & Heston, New York, 1992, rééd. 1997

Pour agir sur la « *structure d'opportunité du crime* » et sa réfraction dans l'esprit des délinquants potentiels, un certain nombre de techniques de « réduction d'opportunité » sont préconisées (l'ouvrage, p. 18, en énumère 16<sup>3</sup>), allant de l'édification de clôtures à la systématisation des interphones et à la multiplication des caméras de vidéosurveillance, avec, à chaque fois, un effort pour rendre ces mesures publiquement notoires (par exemple, le fait qu'une zone est sous vidéosurveillance devra être clairement affiché<sup>4</sup>). Cette « applicabilité » de la théorie situationnelle est sans doute, pour une large part, dans le succès qu'elle a connu auprès des institutions chargées du maintien de l'ordre.

(1) Les situationnistes accordent néanmoins un faible poids à l'alourdissement des peines dans la décision du passage à l'acte, l'horizon judiciaire et pénitentiaire étant jugé trop lointain pour entrer de façon décisive dans les délibérations du délinquant. Cf. Braga (A.), Kennedy (A. & D), 2012, « Linking situational crime prevention and focused deterrence strategies » in Tilley (N.) & Farrell (G.) (eds.), *The reasoning criminologist: Essays in honor of Ronald V. Clarke*, New York, Routledge.

(2) Cf. Freilich (J. D.), Newman (G. R.), 2016, « Transforming Piecemeal Social Engineering Into "Grand" Crime Prevention Policy: Toward a New Criminology of Social Control », *Journal of Criminal Law and Criminology*, 105(1), p 209-238.

(3) La dernière version de la théorie, due à Joshua D. Freilich et Graeme R. Newman (« Situational Crime Prevention », soumis en mars 2017 à *Oxford Research Encyclopaedia of Criminology*) présente, quant à elle, 25 dispositions de « réduction d'opportunité ».

(4) Sur l'importance de la publicité des mesures de prévention, à la fois auprès du public général et des délinquants potentiels, cf. Bowers (K), Johnson (S.), 2005, « Using Publicity for Preventive Purposes » in Tilley (N.) (Ed.), *Handbook of crime prevention and community safety*, Portland, Willan Publishing.

L'évaluation de l'efficacité de ces dispositions, qui n'entre pas dans le champ de la présente note, semble avoir été considérable, à en juger par la liste des *success stories* dont le livre est orné, même si des interrogations peuvent être formulées sur les ressorts réels de certains de ces résultats<sup>5</sup>.

Les objections qui peuvent être adressées à la théorie situationnelle sont, pour l'essentiel, de trois ordres :

- un reproche de trivialité. Naturellement, une théorie qui conduit à préconiser le renforcement des serrures pour diminuer la rentabilité des cambriolages ne saurait être foncièrement mauvaise. *Sed verum ex quolibet* : la vérité d'une conclusion triviale ne suffit pas à établir la correction des hypothèses dont cette conclusion découle ;
- une variante sophistiquée de l'objection de trivialité touche à la manière dont le situationnisme utilise la théorie du choix rationnel. En l'absence de tout intérêt porté aux criminels et à l'expression verbale de leurs opinions et de leurs objectifs, la seule source d'accès à leurs représentations mentales est précisément leur comportement délictuel. Dans ces conditions, l'hypothèse selon laquelle ce comportement est maximisateur est une pure et simple postulation, qu'aucune donnée empirique ne saurait démentir. Très différent serait le cas où l'on disposerait d'un autre type d'accès – par exemple par des entretiens – aux croyances et aux préférences des délinquants, et où il serait ainsi possible, au moins en principe, de mettre en évidence des infractions à la théorie du choix rationnel. En l'absence de ce recours, l'approche du crime en termes de choix rationnel est, par construction, en mesure de s'accommoder de la totalité des faits, et ne répond donc pas aux critères poppériens de falsifiabilité généralement considérés comme nécessaires pour qu'une théorie soit tenue pour scientifique ;
- la théorie situationnelle ne tient aucun compte des résultats obtenus depuis un demi-siècle par les sciences du comportement, lesquelles réfutent purement et simplement la théorie du choix rationnel dans ses ambitions descriptives (ladite théorie reste,

bien entendu, précieuse au plan normatif, comme présentation systématique de la manière dont les agents seraient bien avisés de raisonner). Ce défaut handicape sérieusement le situationnisme non seulement dans sa compréhension des mécanismes du passage à l'acte, mais dans sa capacité à proposer des dispositifs de nature à prévenir ou entraver ce passage (*vide infra*) ;

- *Last not least*, l'extension de cette théorie aux questions touchant au terrorisme est, *prima facie*, problématique (l'exaltation des terroristes est peu compatible avec l'image d'un calcul délibératif méticuleux).

Les premiers travaux d'ensemble qui étendent au terrorisme la théorie situationnelle sont Ronald V. Clarke & Graeme R. Newman, *Outsmarting the Terrorists*, Westport, CT : Greenwood, 2006 et Joshua D. Freilich & Graeme R. Newman, *Reducing Terrorism Through Situational Crime Prevention*, Criminal Justice Press, Crime Prevention Studies Series, 2009.

La pertinence de ces recherches peut être considérée comme assez élevée dans le « cas facile », celui du terrorisme organisé du type Al-Qaida, dans lequel la question du passage à l'acte n'est guère plus problématique que dans le cas d'une guerre, où ce qui déclenche l'acte est la réception de l'ordre d'agir, et où la théorie du choix rationnel peut être appliquée, par exemple, au choix des cibles.

Pour des exemples d'analyse de ce type : Laura Dugan, Gary LaFree & Alex R. Piquero, «Testing a Rational Choice Model of Airline Hijackings», *Criminology* 43-4 (2005), p. 1031-1065 ; Jeff Gruenewald, Kayla Allison-Gruenewald & Brent R. Klein, «Assessing the Attractiveness and Vulnerability of Eco-Terrorism Targets A Situational Crime Prevention Approach », *Studies in Conflict & Terrorism*, 38-6 (2015), p. 23-39 ; Graeme R. Newman & Henda Y. Hsu, «Rational Choice and Terrorist Target Selection», in Updesh Kumar & Manas Mandal (eds.), *Countering Terrorism: Psychosocial Strategies*, Thousand Oaks, CA : Sage, 2012, p. 227-249.

Néanmoins, la théorie situationnelle rencontre des difficultés plus considérables avec les formes les plus

(5) Un cas particulièrement intéressant concerne le succès de la « géographie du crime » (Weisburd (D.), Groff (E.R.) & Yang (S. M.), 2012, *The Criminology of Place: Street Segments and Our Understanding of the Crime Problem*, Oxford University Press), dont a découlé la présence accrue et visible de forces de l'ordre dans les endroits signalés comme criminogènes dans les bases de données (dans ses versions les plus récentes, la théorie situationnelle n'a pas manqué de confluer avec la thématique porteuse des *Big Data*). La diminution des actes délictueux dans ces endroits, pour laquelle les « situationnistes » proposent des exemples éloquentes, pourrait être interprétée non comme l'effet direct des informations nouvelles apportées à la police par le *data mining* dans ces bases de données, mais comme l'effet d'une manière d'obligation implicite désormais dirigée vers la police de stationner davantage dans les endroits désignés – endroits dont l'identité était préalablement connue de façon empirique par les forces de l'ordre, sans le secours de la machinerie informatique...

récentes du terrorisme, qui mettent en jeu des structures beaucoup moins organisées que ne l'était Al-Qaida : « Après le 11 septembre 2001, l'appareil de la sécurité globale et du contre-terrorisme a été dramatiquement réorienté vers la poursuite d'Al-Qaida et d'autres groupes terroristes transnationaux. On a, depuis lors, de plus en plus reconnu que les menaces terroristes pouvaient se manifester sous la forme d'un acteur indépendant et sans l'assistance d'une organisation extrémiste étrangère ou domestique. On peut considérer que la dissuasion ou l'interdiction de tels individus est l'objectif principal des efforts du contre-terrorisme en Occident ». (John P. Sawyer & Justin Hienz, «What Makes Them Do? Individual-Level Indicators of Extremist Outcomes», in Gary LaFree & Joshua D. Freilich (eds.), *Handbook of Criminology of Terrorism*, John Wiley & Sons, 2017, p. 47).

Dans ce nouveau contexte, la théorie situationnelle se heurte à deux types de difficultés.

D'une part, la stratégie de « réduction d'opportunité » devient ici particulièrement difficile à mettre en œuvre :

- les sites à traiter sont plus nombreux et variés (le terrorisme de ce type est plus ubiquitaire que le grand banditisme) ;
- un grand nombre des techniques de réduction proposée par la théorie perd sa pertinence, dès lors que le risque d'être pris ou tué lors de l'attaque n'est pas pris en compte par le terroriste, ou bien, *a fortiori*, est valorisé par lui.

D'autre part, le passage à l'acte n'est plus le résultat d'un ordre reçu (les déclarations d'allégeance à Daesh enregistrées par les terroristes avant d'agir ne témoignent généralement pas qu'un ordre quelconque leur ait été donné au préalable), si bien que le problème du déclenchement de ce passage à l'acte reste entier.

Certains partisans de la théorie situationnelle de la prévention persistent à affirmer que les actes de ce type maximisent l'utilité des terroristes, et que la théorie du choix rationnel leur demeure applicable.

Un article typique, consacré aux attentats-suicides, est celui de Simon Perry & Badi Hasisi, «Rational Choice Rewards and the Jihadist Suicide Bomber», *Terrorism and Political Violence*, 27-1 (numéro spécial sur la théorie criminologique et le terrorisme), 2015, p. 53-80 : « On attribue ce type de terrorisme à des motivations altruistes, en assumant que les auteurs sont d'accord pour se sacrifier eux-mêmes pour une cause plus haute. Notre étude utilise la théorie criminologique du choix rationnel pour analyser la motivation du terrorisme djihadiste par suicide. En passant en revue les incitations

religieuses, personnelles et sociales, nous démontrons que même ceux qui se tuent eux-mêmes dans des attaques suicides, ce qui semble un exemple de comportement irrationnel ou altruiste, agissent ainsi en vue de bénéfices futurs. Puisque ce comportement autodestructeur est la plupart du temps motivé par l'anticipation de coûts et de bénéfices, nous considérons qu'il n'y a pas de différence fondamentale entre les motivations de ceux qui perpètrent ces attaques et celles des autres criminels ; les deux groupes sont engagés dans un comportement maximisateur visant au bénéfice et à l'auto-gratification ».

Mais cette orientation *ad hoc* appelle deux remarques.

D'une part, on a ici abandonné la théorie situationnelle d'origine, qui demandait que l'on ne s'intéresse qu'à l'acte, et non au criminel. Pour éviter que l'hypothèse de la rationalité du terroriste soit purement et simplement postulée, les auteurs sont conduits à enquêter sur les « motivations » des terroristes à la lumière d'autres sources que l'acte criminel lui-même. En d'autres termes, les situationnistes sont contraints de faire place, au-delà de la commission de l'acte, à l'analyse de l'« esprit » du terroriste.

Cette conclusion, qui demande que l'on ne se contente pas de regarder le terroriste comme un entomologiste regarde les fourmis, mais que l'on s'efforce de comprendre ses motifs, n'est scandaleuse que par la banale équivocité du mot « compréhension », ambigu entre mansuétude et intellection. Au reste, elle avait déjà été formulée dans un article ancien, «The Mind of Terrorist. A Review and Critique of Psychological Approaches» (*Journal of Conflict Resolution*, 49-1, 2005, p. 3-42), dans lequel le neurologue Jeff Victoroff, à partir d'une étude bibliographique étendue relative aux bases de données sur la psychosociologie du terrorisme jusqu'en 2003, montrait que l'analyse de l'« esprit » du terroriste est le seul recours, dès lors que son mode d'action ne dépend pas de sa seule place dans une organisation stratifiée.

Un autre plaidoyer efficace pour la « compréhension » des terroristes est développé dans John G. Horgan, *The Psychology of Terrorism* (2<sup>e</sup> édition, Taylor & Francis, 2014), qui souligne que la contribution efficace de la psychologie à l'analyse et à la prévention des actes terroristes ne saurait résider ni dans un effort d'assignation de traits de personnalité spécifiques, ni dans une entreprise de profilage statique. Les résultats qui pourraient être obtenus de cette manière sont en eux-mêmes dénués de valeur prédictive : le passage à l'acte est caractérisé par une « dépendance au chemin » (*path-dependence*) qui explique qu'une même situation cognitive et émotionnelle peut se traduire par des conséquences futures divergentes au regard du passage à l'acte. C'est donc moins l'état mental instantané qui peut avoir un effet catalytique, que

l'ensemble de la trajectoire qui y conduit, et qui doit donc être étudié.

Cf. aussi John G. Horgan, «From Profiles to Pathways and Roots to Routes : Perspectives from Psychology on Radicalization into Terrorism», *The Annals of the American Academy of Political and Social Science*, 618-1, 2018, p. 80-94.

D'autre part, la rationalité (substantielle, et non pas postulée « à vide ») du terrorisme est une réalité depuis longtemps admise, si l'on y voit une stratégie politique rivale de l'engagement militaire : Robert A. Pape, «The Strategic Logic of Suicide Terrorism», *American Political Science Review*, 97-3, 2003, p. 343-361.

Néanmoins, l'inférence de l'échelle « macro » à l'échelle individuelle est inapplicable, et il n'y a aucune raison de conclure, de l'éventuelle rationalité d'ensemble de la stratégie terroriste, à la rationalité du passage à l'acte des individus qui y sont impliqués, ainsi que le montre l'article déjà cité de John P. Sawyer et Justin Hienz, fondé sur une étude de la base *Profiles of Individual Radicalization in the United States (PIRIUS)* :

Loin de confirmer la rationalité du comportement terroriste individuel, c'est-à-dire l'hypothèse selon laquelle le passage à l'acte maximise l'utilité espérée du terroriste, cette étude conclut au contraire à l'importance du déphasage, chez les terroristes, entre les croyances et les aspirations, d'une part, et le comportement de l'autre. Au reste, la dépendance au chemin mise en évidence par John G. Horgan est évidemment incompatible avec l'idée que le comportement terroriste effectif serait optimisateur au regard des croyances des individus : un calcul d'optimisation, de son côté, s'effectue sur le fondement d'une situation mentale instantanée – c'est, si l'on veut, un processus markovien, dans lequel les antécédents de la situation au moment de l'évaluation sont effacés (*screening*).

## Analyses du passage à l'acte sans hypothèse d'optimalité

On entre ici dans le domaine des sciences du comportement, s'étendant depuis les travaux de psychologie cognitive ayant établi la sub-optimalité des mécanismes de décision jusqu'au secteur des neurosciences qui analysent les processus neurologiques sous-jacents à ces mécanismes.

Autant dire que l'articulation de ce champ d'études aux *terrorism studies* ne va de soi ni dans la pratique académique, ni dans les normes implicites qui régissent les rapports entre les « grands règnes » de l'entreprise scientifique.

La littérature pertinente, du côté des sciences du comportement, se publie dans des périodiques qui ne sont lus ni par les criminologues, ni par leur public habituel – cette segmentation explique pour une grande part que la théorie situationnelle, dont les hypothèses d'optimalité ont été réfutées depuis une bonne trentaine d'années dans le champ des sciences cognitives, prospère sans qu'apparemment ombrage n'en soit pris (tout au plus ses zélotes éprouvent-ils parfois le besoin de mentionner que les décisions des criminels ou des terroristes pourraient bien être « satisfaisantes » au sens de Herbert A. Simon plutôt qu'optimales à proprement parler). L'économie *mainstream* a été tout à fait ébranlée par les travaux de psychologie cognitive et d'économie expérimentale poliétablissant l'irréalisme de ses présupposés<sup>6</sup>. Rien de tel du côté de la criminologie, dont le cours semble se dérouler à l'abri des controverses<sup>7</sup>.

Pour un exemple récent, presque pris au hasard, de persistance dans l'hypothèse d'optimalité, cf. Rachael Steele, «How Offenders Make Decisions: Evidence of Rationality», *British Journal of Community Justice*, 13-3, 2016, p. 7-20<sup>8</sup>.

(6) Pour une perspective cavalière sur les débats homériques provoqués chez les économistes par les travaux de Tversky et Kahneman, on peut consulter Richard H. Thaler, *Misbehaving: The Making of Behavioral Economics*, New York, Norton, 2015.

(7) Par ailleurs, l'expérience semble plaider en faveur du diagnostic de J. Victoroff (op. cit., p. 33) sur la « division culturelle » qui sépare les spécialistes des sciences du comportement des praticiens de l'application de la loi, du renseignement et de la chose militaire : « Les forces du contre-terrorisme occupent une position d'antagonisme et doivent s'armer contre toute considération de sympathie à l'égard des terroristes. Les spécialistes de sciences du comportement, quel que soit le mépris que leur inspirent les actions terroristes, doivent eux-mêmes s'armer pour adopter la position d'observateurs et d'interprètes impartiaux du comportement. Alors qu'il peut leur arriver de reconnaître chez les terroristes une hétérogénéité psychologique marquée, et même certains traits pro-sociaux qui pourraient être exploités dans le développement de la politique, les forces du contre-terrorisme et même les décideurs peuvent résister à ces conclusions [...]. Cette division, malheureusement, peut avoir un retentissement sur l'efficacité du contre-terrorisme en isolant les praticiens des théoriciens – une séparation voisine de celle qui isole les ingénieurs des découvertes des physiciens ».

Sur ce point, voir déjà David A. Soskis, «Behavioral Scientists and Law Enforcement Personnel: Working Together on the Problem of Terrorism», *Behavioral Science and the Law*, 1-2, 1984, p. 47-58.

(8) Je [JD] n'ai pu trouver qu'une seule étude explicitement consacrée à discuter la pertinence de l'hypothèse d'optimalité en criminologie, un mémoire de M.A. soutenu en 2009 au Département de criminologie de l'université de Floride du Sud par le dénommé Douglas J. Wholl, lequel ne semble pas avoir fait par la suite de carrière académique particulièrement signalée : *A Rational Choice Approach to Professional Crime Using a Meta-synthesis of the Qualitative Literature*.

Dans un entretien retranscrit dans le numéro 365 (2003) du magazine *La Recherche*, David Kahneman, Prix Nobel d'économie et auteur, avec Amos Tversky, des travaux de psychologie cognitive auquel il est fait ici référence, affirme que le lien entre la psychologie et l'économie a été fait par Richard Thaler, figure centrale de l'économie expérimentale et fondateur de la théorie des « nudges » (*vide infra*). La criminologie, visiblement, attend encore son Thaler...

## L'approche cognitive du passage à l'acte

Le genre de données sur lesquelles travaillent actuellement les partisans de cette approche peut être illustré par l'article suivant (beaucoup d'autres choix auraient été possibles) : Eidad Yechiam & alii, «Neurocognitive Deficits Related to Poor Decision-Making in People Behind Bars», *Psychonomic Bulletin & Review*, 15-1, 2008, p. 44-51.

Les auteurs y identifient chez les délinquants qu'ils étudient (l'étude porte sur des délinquants de droit commun, non sur des terroristes) une série de biais cognitifs caractéristiques, parmi lesquels :

- minimisation de l'appréciation des risques ;
- la forte prévalence, dans la formation des opinions, des événements les plus récents (i.e. la difficulté de gérer rationnellement la mémoire à long terme) ;
- l'aversion à la « prise de perte » (si l'on s'est procuré une arme, on sera réticent à ne pas l'utiliser, même si la perception de la situation actuelle en présente l'usage comme beaucoup plus risqué qu'il ne le semblait lors de son acquisition – si c'était à refaire, on s'abstiendrait de se la procurer).

De tels biais possèdent trois propriétés remarquables :

- 1) Ils incitent au passage à l'acte. Autrement dit, et contrairement à la thèse situationniste, c'est la sub-optimalité qui est un déclencheur. Par exemple, pour ce qui est du second biais, le fait que le souvenir de déconvenues passées s'estompe devant celui du dernier coup réussi élimine une inhibition possible à l'action. Les deux autres biais, de façon évidente, ont un effet semblable ;
- 2) Ils représentent une version simplement plus intense de biais cognitifs qui affectent tous les individus. Cas par cas :

2a) L'existence de préférences pour la prise de risque, qui va à l'encontre du dogme classique de l'aversion au risque, a été démontrée dans l'article fondateur de Kahneman et Tversky : «Prospect Theory: An Analysis of Decision under Risk», *Econometrica*, 47-2 (1979), p. 263-291. Les auteurs y mettent en évidence deux phases dans la prise de décision, et en particulier dans la décision face au risque (c'est-à-dire dans les choix dont les conséquences dépendent de la réalisation d'événements auxquels des probabilités sont attachées) : une phase d'« édition », dans laquelle l'agent se formule à lui-même les différentes options en présence dans le but de s'en faciliter l'évaluation et la phase d'évaluation proprement dite. Ils établissent que, lorsque la décision est formulée en termes de gains plutôt que de pertes, les agents ont généralement tendance à surévaluer les petites probabilités (l'inverse est vrai dans le cas d'une formulation en termes de pertes, où l'aversion au risque reste la règle) ;

2b) La prévalence des événements les plus récents dans l'évaluation des probabilités est une réalité psychologique attestée expérimentalement, à rebours des dogmes usuels sur l'apprentissage bayésien. C'est une variante de l'« heuristique de disponibilité » qui nous fait essentiellement régler nos prévisions sur la base des événements les plus immédiatement disponibles à notre mémoire. Cf. D. Kahneman & A. Tversky, «On the Psychology of Prediction», *Psychological Review*, 80-4 (1973), p. 237-251 ;

2c) Enfin, le refus de prise de perte est le biais cognitif très commun, qui nous porte, par exemple, à continuer à fréquenter une salle de gymnastique dont nous n'attendons plus que des courbatures, au simple motif que nous en avons sottement acquitté les droits d'inscription à un moment où nous n'avions pas bien considéré la chose. Cf. R. Thaler, *op. cit.*, Chapitre VIII, *Sunk Costs*. En d'autres termes, l'approche comportementaliste du passage à l'acte délictuel possède le même avantage que sa concurrente situationniste. Pas plus qu'elle, elle n'introduit d'hypothèses *ad hoc* pour traiter du comportement criminel : le passage à l'acte criminel est une simple variété du passage à l'acte en général, régie par les mêmes mécanismes mentaux. La différence entre les deux théories réside simplement dans le fait que la machinerie mentale invoquée par les sciences du comportement est empiriquement vérifiée, et que l'autre, et pour cause, ne l'est pas ;

3) Une autre propriété intéressante des biais mis en avant par les sciences du comportement est qu'ils font partie d'un système d'évaluation qui peut être,



dans une certaine mesure et dans certaines conditions, « débrayé » ou corrigé. L'ouvrage *Thinking, Fast and Slow* [Allen Lane, 2011], où Kahneman rassemble ses conclusions, résume la situation en opposant deux régimes mentaux. D'une part, le « système 1 », responsable des biais en question, est le régime rapide, automatique et inconscient, mais faillible, que nous utilisons dans l'urgence de l'action. Le « système 2 », quant à lui, est le régime lent, analytique, conscient et plus rigoureux que nous adoptons dans la délibération réfléchie, et qui est en mesure de corriger les erreurs et les biais du premier.

S'offrent ici deux moyens, distincts mais complémentaires, de prévenir les décisions malencontreuses.

- 3a) Une *medicina mentis* consistant à inciter les sujets, de manière générale, à faire retour réflexivement sur leurs croyances et leurs évaluations (d'où provient ma croyance que les Américains n'ont jamais mis les pieds sur la Lune ?) ;
- 3a') Dans une variante largement disséminée de cette première option, on peut aussi tenter d'intervenir, non sur la célérité avec laquelle le système 2 prend la main sur le système 1, mais sur le contenu même du système 2. Ce que l'on appelle l'enseignement (non, la bonne interprétation des sourates de Médine n'est pas celle que vous croyez, et je vais vous le démontrer (?)). Cette variante a l'avantage d'être exempte du reproche de manipulation qui est parfois formulé à l'endroit de l'option 3b : la pédagogie, la dissémination des bonnes informations et, à un moindre degré, la rhétorique, sont les seules manières réputées licites d'intervenir sur l'esprit d'autrui. L'expérience montre néanmoins que cette variante éthiquement irréprochable met du temps à porter ses fruits ;
- 3b) Surtout, la nature même du système 1 offre elle-même des possibilités d'intervention efficace à plus court terme. En particulier, la phase d'« édition » des alternatives de choix, à laquelle on sait que la décision finale est sensible (e.g. la sous-estimation des risques est corrélative d'une édition centrée sur les gains et non sur les pertes), recèle des possibilités d'induire des changements de comportements. Ainsi, la littérature du domaine fourmille d'exemples montrant l'efficacité de l'intervention des options par défaut, dans laquelle le choix offert à l'agent reste identique, mais où l'on modifie l'option pour laquelle il doit explicitement se déclarer. Cette possibilité de proposer des « architectures de choix » appropriées (*nudges*), par lesquelles l'intervenant incite, sans l'y forcer, l'agent à adopter une certaine option, est aujourd'hui utilisée dans un nombre impressionnant de domaines

(conduite automobile, comportements alimentaires, addictions, comportements d'épargne et d'assurance, etc.). Cf Richard Thaler & Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press, 2008

En 2013, Lawrence Sherman, Professeur de criminologie à Cambridge, insistait sur l'intérêt de cette dernière perspective pour la prévention du passage à l'acte :

« La criminologie est comme une éponge. Nous faisons bon accueil aux disciplines scientifiques de base qui font ce qu'elles sont intéressées à faire dans notre domaine. Très souvent, c'est en établissant un certain type de prémisse théorique que les choses se passent. Les économistes étaient très intéressés à montrer que la punition fonctionne en conformité avec le modèle du choix rationnel. Mais Daniel Kahneman a complètement mis ce modèle à bas en étudiant la manière dont les gens prennent réellement des décisions, et son travail a beaucoup de pertinence pour la relation entre punition et conduite. Typiquement, c'est cette idée que vous pouvez travailler sur l'inertie avec laquelle les gens prennent des décisions, en mettant un point une sorte de contexte “nudge”, en modifiant les cases qu'ils ont à cocher pour agir d'une manière ou d'une autre, ou en leur adressant un message, de telle sorte que leur risque de payer pour leur crime soit accru. C'est ce qu'on appelle aujourd'hui “économie comportementale”, et ça fait absolument partie de la criminologie expérimentale, parce que ça nous donne des informations sur la manière de concevoir des interventions visant à ce que les gens respectent la loi, à ce que le système des punitions légales fonctionne de manière conforme et au moindre coût pour le contribuable, également à obtenir une société plus sûre et plus juste, tout en utilisant autant que possible la manière douce à cet effet, en se gardant d'utiliser la manière forte plus qu'il n'est réellement nécessaire dans des circonstances de ce genre. Nous ne considérerions pas les choses de cette manière, s'il n'y avait l'économie comportementale, la psychologie et d'autres domaines, que nous intégrons dans la criminologie expérimentale » (*Social Science Bites*, mai 2013).

### Applications de l'approche cognitiviste à la prévention du passage à l'acte

Jusqu'ici, ces applications ont été, pour l'essentiel, de deux types.

D'une part, les problématiques de Tversky et Kahneman ont directement inspiré la « criminologie expérimentale », domaine pour lequel le *Journal of Experimental Criminology* est la revue académique de référence – significativement

(*vide infra*), on ne trouve aucun Français dans la quarantaine de chercheurs internationaux qui constituent son comité éditorial). Ce type de criminologie a induit dans le monde anglo-saxon une assez large réforme des modes d'analyse et d'intervention de la police, dans la direction d'une stratégie d'ensemble davantage fondée sur les données.

D'autre part, mais de façon pour l'instant très sporadique, la problématique des *nudges* a été directement étendue aux stratégies d'intervention dans le domaine de la prévention de la délinquance.

### Applications aux modes d'analyse et d'intervention de la police

Le volume édité par Brandon Welsch & *alii*, *Experimental Criminology. Prospects for Advancing Science and Public Policy* [Cambridge, 2013] donne un paysage d'ensemble, complété depuis par les livraisons du *Journal of Experimental Criminology* pour des études de cas.

La présente note se limite aux innovations qui ont trait à la prévention du passage à l'acte délictueux et de sa récurrence.

Le contexte politique d'ensemble est l'encouragement appuyé donné, durant les années de la présidence Obama, à la fois aux sciences du comportement et à la recherche de politiques publiques plus efficaces.

On peut se référer au décret du 15 septembre 2015 installant à la Maison Blanche une équipe de spécialistes du domaine, la Social and Behavioral Science Team (SBST) : « *Les sciences du comportement contribuent notablement à des priorités comme l'emploi, l'espérance de vie en bonne santé, la réussite scolaire ou la transition vers les énergies décarbonées [...] Un gouvernement efficace et efficace doit refléter notre compréhension la meilleure du comportement humain et de la manière dont les gens s'approprient les politiques et les programmes, y participent et y répondent* ». (*Executive Order – Using Behavioral Science Insights to Better Serve the American People*<sup>9</sup>).

La définition de politiques publiques efficaces, c'est-à-dire efficaces à moindre coût, était dans les objectifs assignés à la SBST, qui a entrepris d'y travailler selon la méthodologie des expériences randomisées contrôlées.

Les expériences tentées dans le domaine de la prévention du passage à l'acte ou de la récurrence suivent la même méthodologie des expériences randomisées, avec des résultats probants en faveur d'un suivi moins intense pour les petits délinquants, permettant ainsi de dégager du temps et des moyens pour des tâches policières plus essentielles : le taux de délinquance reste identique dans le groupe moins suivi et dans le groupe auquel les normes précédentes continuaient d'être appliquées. Geoffrey C. Barnes & *alii*, « *Low-intensity community supervision for low-risk offenders: A randomized, controlled trial* », *Journal of Experimental Criminology*, 6-2, 2010, p. 159-189.

Dans une étude plus générale des perspectives offertes par la criminologie expérimentale (« *The Rise of Evidence-Based Policing: Targeting, Testing, and Tracking* », *Crime and Justice*, 42-1, 2013, p. 377-451, Sherman essaie d'articuler, à propos de la police elle-même, une distinction analogue à celle entre les deux régimes mentaux de Kahneman.

Il s'agit en somme d'articuler efficacement deux sources d'information : celle qui émane de la longue expérience « clinique » des policiers, qui ont le contact direct avec les délinquants et qui ont l'habitude de porter sur leur dangerosité des diagnostics et des pronostics intuitifs, rapides mais faillibles, et celle, « externe », qui peut émaner par *data mining* des larges bases de données disponibles. *Mutatis mutandis*, la première source fonctionne comme un Système 1, dont les résultats doivent être disciplinés et validés par un Système 2. Une articulation correcte entre les deux composantes est la clef de l'efficacité<sup>10</sup>.

En particulier, il doit être souligné que la mise en place d'une police inspirée par les principes de la criminologie expérimentale ne peut signifier le remplacement de la première composante par la seconde, et ce pour au moins deux raisons. D'une part, c'est aux policiers, non aux comportementalistes ou aux informaticiens, qu'incombe le soin de déterminer si l'individu considéré tombe ou non sous les catégories qui définissent le *cluster* auquel on le compare. D'autre part, il est essentiel qu'ils participent à la définition des descripteurs et de la nomenclature d'ensemble qui organisent les bases de données. La situation d'ensemble du problème est, à cet égard, tout à fait comparable à celle qui prévaut en

(9) Pour un bilan d'ensemble du recours de la puissance publique à la stratégie des *nudges* comme alternative à la réglementation ou à la taxation, cf. Benatzi (S.) & *alii*, 2017, « *Should Governments Invest More in Nudging?* », *Psychological Science*, 28-8, p. 1041-1055.

(10) Dans un autre registre, il a pu être considéré que l'articulation entre les « gourous » (i.e. les professionnels de la vie politique) et les *geeks* avait été la clef du succès de la première campagne d'Obama. Cf. Issenberg (S.), 2013, *The Victory Lab. The Secret Science of Winning Campaigns*, Broadway Books.

médecine, où la promotion d'une pratique *evidence-based* ne peut évidemment signifier la fin de la clinique et la « computérisation » d'ensemble de la discipline<sup>11</sup>.

### Applications directes à l'inhibition du passage à l'acte

On peut être ici beaucoup plus bref. La littérature ne contient guère, dix ans après la formulation de la théorie des *nudges*, qu'une contribution de débutants relative à l'efficacité du *nudging* pour la prévention du passage à l'acte chez les voleurs à l'étalage : Dhruv Sharma & Myles Scott Kigallon, «Nudge, Don't Judge: Using Nudge Theory to Deter Shoplifters», *11th European Academy of Design Conference* (2015).

### Applications au cas des actes terroristes

Bien que la plupart des criminologues<sup>12</sup> considèrent, avec quelque apparence de bon droit, que l'étude de ces actes relève de leur discipline, en tant qu'elle a trait à la totalité des actes délictuels et aux moyens de les réprimer ou de les prévenir, il faut reconnaître que la question posée est bien celle d'une extrapolation des méthodes et des résultats de la criminologie, plutôt que celle d'une simple spécialisation.

Parmi les traits qui expliquent cette situation, il y a d'abord, fort heureusement, la disparité numérique entre la catégorie des (petits) délinquants, à laquelle est consacré l'article de Barnes & *alii* cité plus haut, et la catégorie des terroristes : on serait bien en peine de réunir aujourd'hui, à propos de ces derniers, une base de données normalisée de plusieurs dizaines de milliers d'individus comme celle sur laquelle s'appuie l'enquête de Barnes.

À titre d'exemple, le chapitre de Fiona Brookman et Michele Wright, « “Deciding” to Kill: Understanding Homicide Offenders' Decision Making », qui fait le point sur la recherche relative au passage à l'acte individuel dans le récent *Oxford Handbook of Offender Decision Making* (2017), contient une analyse assez complète sur les mécanismes inhibiteurs et désinhibiteurs de la violence létale, mais ne dit rien de spécifique sur le terrorisme.

Aussi l'essentiel de la recherche en sciences cognitives sur le passage à l'acte terroriste lui est-il spécifiquement dédié.

Deux types de contributions émergent, l'une qui a trait à la perspective des neurosciences sur les massacres de masse, l'autre qui concerne les catalyseurs du passage à l'acte chez les prétendus « loups solitaires ».

### Travaux sur le « syndrome E »

Ce syndrome recouvre un ensemble de signes distinctifs tels qu'une perte d'affect et d'empathie, une excitation temporaire due aux actes violents, suivie d'une habitude où la violence devient banale, un effet de compartementalisation cognitive (on peut à la fois exterminer ou décapiter le matin, et vivre une vie de famille rangée le soir), et un effet de contagion de groupe.

Du point de vue neurologique, ces comportements correspondent à une hyper-activité d'une partie antérieure du cerveau, le cortex orbifrontal, provoquant un effet de « fracture cognitive » (l'hyper-activité de cette zone du cerveau inhibe les zones centralisant les informations, aussi bien que l'activité des neurones-miroirs, qui sont le support cérébral de l'empathie).

L'article séminal est : Itzhak Fried, « Syndrom E », *The Lancet*, 350 (Décembre 1997), p. 1845-1947.

### Recherche sur le passage à l'acte des « loups solitaires »

Le concept lui-même est notoirement problématique, hormis dans l'acception minimaliste qui en est proposée dans l'*Index International du Terrorisme Global* :

- agir de façon isolée dans l'exécution de l'attaque ;
- ne pas avoir d'affiliation directe avec un groupe ou une organisation terroriste ;
- ne pas suivre l'ordre direct d'un *leader* ou d'un groupe.

En particulier, la définition n'exclut pas que le processus de radicalisation soit conduit en interaction avec un groupe.

Il est en fait établi, d'une part, que la phase antérieure au passage à l'acte n'est jamais isolée (rôle des réseaux sociaux), d'autre part, que la commission d'autres actes terroristes joue un effet catalytique, lorsqu'elle en vient à être connue.

(11) Cf sur ce point. Sackett (D. L.) & *alii*, 1996, «Evidence Based Medicine: What it is and What it isn't? », *BMJ Clinical Research*, 312 (1996), pp. 71-72.

(12) E.g. Freilich (J. D.), Lafree (F.), 2015, «Criminology Theory and Terrorism: Introduction to the Special Issue», *Terrorism and Political Violence*, 27-1.

Parmi les travaux les plus signalés :

- 1) Le projet *Preventing, Interdicting and Mitigating Extremist events: Defending against lone actor extremism (PRIME)* financé dans le cadre européen de 2014 à 2017 – le site du projet contient la bibliographie des résultats de la recherche.

Deux remarques sur ce projet :

- le consortium réuni ne comporte, à nouveau significativement, aucun chercheur français ;
- c'est un projet financé dans le cadre du comité de programme « Sécurité », alors qu'il ne comporte aucune dimension technologique significative. Les négociations en cours relatives au prochain programme-cadre (FP9) laissent craindre une prévalence stricte, dans ce qui succédera à ce CP, des approches technologiques. La structuration de la recherche européenne, et *a fortiori* française, en matière de sécurité, demanderait pourtant le maintien d'une ouverture aux SHS et aux sciences du comportement.

Parmi les résultats obtenus dans PRIME : Malthaner, Stefan & Peter Waldmann. «The radical milieu: Conceptualizing the Supportive Social Environment of Terrorist Groups», *Studies in Conflict & Terrorism*, 37-12 (2014), p. 979-998.

Même si l'acte est le fait d'un individu isolé, les *drivers* sont partagés (il existe toujours un « milieu » au sein duquel le terroriste échange et partage ses convictions), et l'acte lui-même peut être déclenché par l'information selon laquelle un acte similaire a été commis (« contagion mimétique »). Cette circonstance, jointe au fait que les terroristes isolés sont peu préoccupés de leur propre sécurité, les rend vulnérables à la détection à des stades variés du processus de préparation de l'attaque ;

- 2) Travaux sur les terroristes de retour du terrain moyen-oriental, et sur leur probabilité de réengagement dans des actions extrémistes : David Malet & Rachel Hayes, «Foreign Fighters Returnees: An Indefinite Threat», accepté par *Terrorism and Political Violence* et publié en ligne le 27 juillet 2018 sur le site de la revue. L'article, concentré sur la question du délai d'attaque pour les extrémistes de retour (*Lags in Attack Times of Extremist Returnees (LATER)*), conclut, sur une base de 230 djihadistes de retour, que ce délai est généralement de moins d'un an, avec un délai médian de quatre mois, ce qui laisse entendre que les efforts de prise en charge et de suivi doivent se porter essentiellement sur les six premiers mois du retour.

Il convient enfin de noter qu'un certain nombre d'initiatives inspirées par les sciences du comportement ont été prises dans la période récente pour calibrer certaines opérations de « marketing viral anti-Daesh », sans pour autant que le bilan de ces opérations ait donné lieu à publication.

Tel a été le cas, en France, à l'initiative du Secrétariat à l'information du gouvernement (SIG), où des spécialistes de sciences cognitives ont collaboré à l'élaboration de « narratifs visuels » visant essentiellement à montrer qu'aucune des étapes du processus de radicalisation ne conduisait mécaniquement à la suivante.

## Conclusions

### Prévisions et prédiction pour le passage à l'acte

Même si les sciences du comportement ont fait progresser la question de l'identification des déclencheurs du passage à l'acte, la métaphore initiale de la décroissance de la radioactivité reste applicable et le demeurera.

Sur un plan épistémologique, la criminologie n'est pas logée à meilleure enseigne que la physique atomique ou la sismologie.

On peut faire des prévisions d'ensemble fiables, c'est-à-dire assigner de façon robuste des probabilités d'occurrence dans des délais déterminés (par exemple, indiquer la probabilité d'un séisme majeur autour de la faille de Sacramento dans un délai de 30 ans), mais on ne peut faire de prédictions, c'est-à-dire indiquer la date et le lieu précis de ce séisme.

En particulier, il ne saurait y avoir d'indicateur strictement prédictif de la date d'un passage à l'acte individuel : ni les techniques de profilage, ni, si l'idée en venait, le passage au scanner d'individus aux fins de détection du syndrome E de Fried, ne peuvent et ne pourront faire cet office.

En revanche, on commence aujourd'hui à être en mesure de faire deux choses, la première que la sismologie faisait mieux que la criminologie, la seconde que ni la physique atomique ni la sismologie ne feront jamais :

- affiner les prévisions au point de les rendre utiles au plan opérationnel, via la transition vers une criminologie *evidence-based* ;
- diminuer les probabilités d'occurrence en mobilisant les stratégies d'intervention que suggère la recherche scientifique.

## Systèmes de sécurité efficaces

Une idée souvent émise, pour améliorer la prévision du passage à l'acte, est de se fonder sur le seul « profilage » et de se rapporter aux bases de données disponibles pour examiner ce qu'il en a été par le passé des individus de profil le plus voisin en s'abstenant de toute spéculation causale.

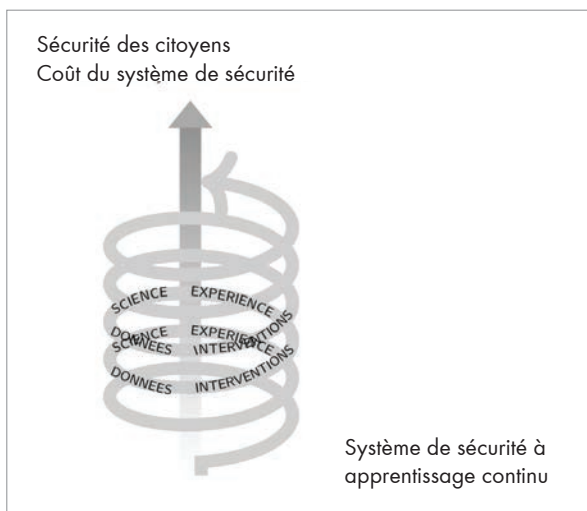
Il existe des limites aux approches de ce genre. Elles ont été étudiées en médecine, qui pose des questions à bien des égards semblables (rapport aux cas individuels, similarité entre l'intervention thérapeutique et l'intervention sécuritaire). Ces études ont conduit à proposer, en lieu et place du seul recours aux « données massives » et aux techniques de *clustering*, des systèmes qui font également une large place à l'investigation scientifique et à l'expérience pratique des intervenants, à savoir des « systèmes d'apprentissage continu » permettant une interaction entre les quatre composantes en jeu (expérience des praticiens, investigation scientifique sur les relations de causalité pertinentes, nature des interventions décidées, bases de données).

Dans le domaine de la médecine, deux références utiles<sup>13</sup> :

M. Smith & *alii*, *Best Care at Lower Cost: the Path to Continuously Learning Health Care in America*, National Academies Press, mai 2013 ;

*Accelerating Progress Toward Continuous Learning*, comptes rendus des réunions de la National Academy of Medicine, 29 juin 2017.

Le schéma général de tels systèmes peut être résumé dans la figure suivante :



Ce qui est visé n'est pas seulement l'efficacité des interventions, mais l'efficacité générale du système de sécurité (i.e. le ratio entre l'efficacité et le coût). L'objectif est donc non seulement d'identifier les interventions les plus efficaces, mais également de repérer celles dont on pourrait s'abstenir sans augmentation corrélative du nombre de passages à l'acte ou de récidives (*vide supra*, § 3.2.1).

L'édification du système des « données de sécurité » présente un certain nombre de difficultés, qui laissent planer un doute sur la possibilité (le mirage ?) d'une approche purement technologique-computationnelle des questions sécuritaires, dans laquelle la nature des interventions à conduire résulterait par simple *data mining* de la consultation des bases :

- absence de normalisation des informations. On est très loin d'avoir défini des protocoles de rapport stables et partagés assurant la commensurabilité mutuelle des informations détenues dans les différentes bases existantes, ce qui engendre notamment le problème classique des *Unknown Knowns* (on a l'information, mais on ne sait pas qu'on l'a) ;
- opacité épistémique. Les décisions d'intervention devraient pouvoir être motivées par des explications, or les « Big Data », et c'est une de leurs caractéristiques essentielles, n'en fournissent pas. On peut assurer par leur biais que telle ou telle configuration locale de température et de pression va donner des orages avec une haute probabilité, mais l'explication ne vient pas avec la simulation informatique. Les *Big Data* sont focalisés sur la corrélation et l'identification de *patterns*, non sur l'analyse causale. Dans le domaine humain (médecine, criminologie), la capacité à expliquer les décisions aux individus qu'elles concernent est, par contre, requise ;
- incomplétude. Ce trait est trop évident pour qu'on y insiste. Si l'on inclut dans ce qui devrait figurer dans de telles bases les passages à l'acte avortés (préparations interrompues par telle ou telle circonstance...), nous sommes loin du compte ;
- coût de constitution des bases. On évoque souvent le temps passé à des activités de *reporting* dont la finalité est peu clairement perçue. Si les personnels ne sont pas impliqués dans la définition et l'usage des bases,

(13) À ma connaissance (JD), il n'existe encore aucune proposition équivalente explicite dans le domaine de la sécurité.

	Beaucoup d'items	Peu d'items
Beaucoup de paramètres	Données « croisées »	Données de sécurité
Peu de paramètres	Données administratives	

on s'engage dans la mise en place d'une activité qui sera perçue comme – et donc qui sera, *simpliciter* – bureaucratique ;

- problèmes éthiques. Ils concernent les questions de la *privacy*, mais également le risque d'utilisation déviante par d'autres parties.

Par ailleurs, les bases relatives au passage à l'acte présentent des caractéristiques *prima facie* défavorables par rapport à certaines autres.

Les données pertinentes pour le passage à l'acte présentent les caractéristiques les plus défavorables de toutes, puisqu'on a affaire à la fois à un faible nombre d'items (il y a moins de délinquants que d'assurés à la Sécurité sociale) et à un nombre potentiellement considérable de paramètres<sup>14</sup>. Ce dernier point est de grande importance. Une fois indiqués les paramètres « canoniques » (âge, sexe (paix aux *gender theorists*...), etc.), la liste des descripteurs ou des paramètres pertinents pour le passage à l'acte est ouverte. De toute évidence, elle ne peut être établie que par la collaboration des praticiens et des scientifiques.

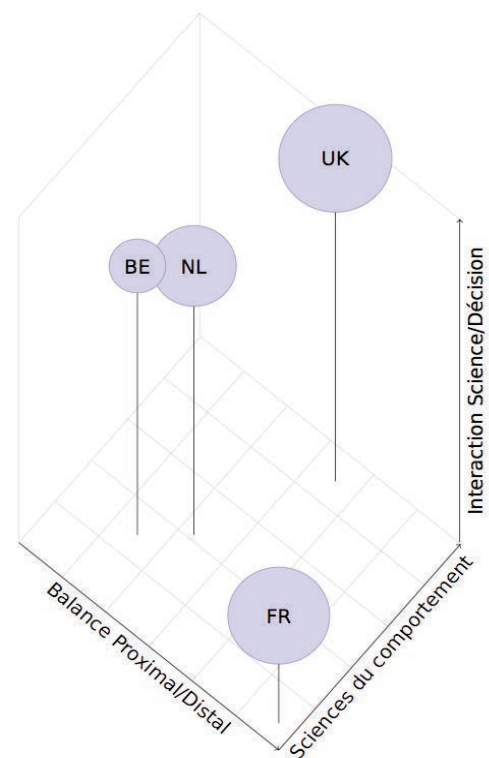
En conclusion sur ce point, l'idée selon laquelle l'amélioration de la prévision et de la prévention du passage à l'acte délictuel pourrait être assurée par le seul recours aux *Big Data* n'a pour elle que le *Zeitgeist*. Praticiens et scientifiques doivent demeurer (ou devenir, pour les seconds) des pièces essentielles d'un système de sécurité efficient.

## La situation française en recherche sur la sécurité

Cette situation est particulière, et elle n'est pas particulièrement bonne.

D'une part, le développement des sciences du comportement, et surtout de leur application aux questions de sécurité et, plus largement, aux politiques publiques, est nettement plus modeste qu'il ne l'est à l'étranger. Pour ne citer qu'un exemple, la France est l'un des rares pays développés à ne pas avoir mis en place de dispositif comparable à la SBSIT américaine (*vide supra*, § 3.2.1) ou à la *Nudge Unit* britannique<sup>15</sup>.

D'autre part, les options prises en matière de recherche sur la prévention de la radicalisation sont nettement distinctes de celles qui ont été prises par nos partenaires européens, et manifestent des orientations qui sont peu appropriées à une articulation, en ce domaine, entre science et décision<sup>16</sup> :



(14) Sur les problèmes méthodologiques généraux posés par ce type de bases, cf. Shinha (A.) & alii, « Large Datasets in Biomedicine: A Discussion of Salient Analytic Issues », *Journal of the American Medical Informatics Association*, p. 759-767, notamment le § « High Dimensionality ».

(15) Cf. Halpern (D.), 2015, *Inside the Nudge Unit. How Small Changes Can Make a Big Difference*, Penguin.

(16) Dubucs (J.), 2016, *Recherche sur la radicalisation : les actions européennes. Benchmark international*, Rapport DGRI, janvier. NB. La taille des points est proportionnelle à la hauteur des financements.

Parmi les mesures qui pourraient être préconisées pour améliorer cette situation :

- intensification de l'interaction entre scientifiques et décideurs. Les modalités de cette intensification ne requièrent pas forcément que l'on fasse le tour du monde pour examiner la façon dont les choses se passent par ailleurs. Le séjour de chercheurs dans les instances de décision ou les agences gouvernementales dédiées pourrait faire office, à la condition naturellement que les chercheurs en question maîtrisent l'état de l'art international et qu'ils aient la capacité de l'expliquer ou de l'enseigner en termes simples et exotériques ;
- accès des chercheurs aux bases de données pertinentes. Il conviendrait pour cela d'utiliser les instruments déjà en place (e.g. l'EQUIPEX Centre d'Accès Sécurisé aux Données (CASD), qui a développé un dispositif d'anonymation rendant l'usage de ces bases compatible avec les normes en vigueur. Des mesures adéquates sont par ailleurs envisagées au sein du Conseil Scientifique sur les Processus de RADicalisation (COSPRAD) pour ouvrir à la recherche scientifique, sur appel d'offres, les bases de données les plus sensibles.

Pour le reste, c'est-à-dire la constitution en France d'une communauté de recherche interdisciplinaire performante dédiée aux questions de sécurité, les changements requis sont importants, nombreux, et dépassent de très loin le cadre de la présente note ■

# Côte d'Ivoire. Le phénomène des délinquants violents dits « microbes » et la réponse de la police et des acteurs informels de la sécurité (AIS)

Henry BOAH YEBOUET



Le phénomène des enfants dits « microbes », apparu au lendemain de la crise post-électorale, constitue aujourd'hui pour les populations abidjanaises une situation inextricable avec comme nœud gordien l'avenir de jeunes en danger physique et moral bien qu'ils soient eux-mêmes auteurs d'actes de délinquance d'une gravité certaine.

Les solutions trouvées par leurs victimes, en se référant aux acteurs informels de la sécurité, ouvrent une autre lucarne en montrant que la police n'est plus le dernier recours.

The phenomenon of the so-called microbes children appeared in the aftermath of the post-electoral crisis, constitutes today for the Abidjan populations, an inextricable situation with as Gordian knot the future of young people in physical and moral danger although they themselves are authors of acts of delinquency of a certain gravity. The solutions found by their victims, referring to the informal security actors, open a skylight that shows that the police are no longer the last resort in terms of protection of persons and property, for a certain category of population.

## Henry BOAH YEBOUET



Henry Boah Yebouet, criminologue, est directeur du LARESS (Laboratoire de Recherche Sécurité et Société) de

l'Université Félix Houphouët-Boigny.

**A**u premier trimestre de l'année 2011, en pleine crise post-électorale, les forces rebelles infiltrées dans la région d'Anyama (à la porte nord d'Abidjan) cherchent des moyens pour percer les lignes de défense gouvernementales à travers le dispositif militaire mis en place dans la commune d'Abobo.

Pour ce faire, elles vont s'appuyer sur de nombreuses complicités locales,

notamment des enfants de la rue qui seront leurs complices à travers les observations des mouvements de troupes ennemies et également de transport discret de matériels légers pour ceux-ci (munitions, armements démontés en pièce qu'il faut transporter d'un point A à un point B).

Trois mois après la fin de la crise, en juillet-août 2011, apparaît



un phénomène de bande de jeunes délinquants communément appelés « Phénomène des microbes », mais connu sous une autre appellation, peu usitée des populations, de « Vohon Vohon », terme désignant un insecte volant dont le bourdonnement dérange, perturbe la quiétude.

Le phénomène des microbes n'est pas un phénomène nouveau ; il rappelle la vie de Zé Pequeno, acteur principal du film brésilien « La Cité de Dieu ». D'autres formes du phénomène, qui ont fait l'objet d'études, ont porté sur la question des gangs, mais la réaction sociale face à ce phénomène a peu focalisé les chercheurs [Porto 2001, Salazar 2006]. Or, la réaction de l'État n'a pas été ferme au départ, elle a laissé s'installer un doute dans l'esprit des populations quant à sa capacité à les protéger surtout en cette période particulièrement criminogène. Analysant les effets de la lutte contre la forme locale des microbes, les « kulunas » à Kinshasa, Yalala [2013] a insisté sur les moyens importants déployés qui ont permis, à défaut d'y mettre fin, de le faire reculer par le recours aux armes à feu par les forces de police contre ces jeunes qui avaient fini par créer la psychose dans la capitale congolaise. Ces violences policières ont été également constatées par Audran (2014) dans le cas de la lutte contre les « foroques » à Diégo Suarez au Brésil. Les forces de police, appuyées occasionnellement par les forces spéciales, ont utilisé tous les moyens conventionnels pour lutter contre ce phénomène.

D'abord localisé à Abobo, dans les quartiers d'Avocatier, de Derrière-rail, de Kennedy, de Klouétcha et Carrefour N'Dotré, le phénomène va progressivement s'étendre à l'ensemble de la commune, puis à d'autres communes comme Yopougon et Cocody, où il aura du mal à s'implanter au regard de la résistance des populations et d'autres facteurs conjoncturels.

Face à ce phénomène, la réaction sociale s'organisera de prime abord autour des moyens régaliens de l'État, notamment la police et la gendarmerie, et à un degré moindre la justice. Mais, la prolifération des actes d'agression et de violence de la part de ces jeunes (avec, en apparence une incapacité des autorités à réagir promptement), va susciter un retour aux vieux réflexes vindicatifs chez les populations.

Selon les statistiques pour l'année 2011 de la police nationale ivoirienne, « l'activisme des jeunes de bande de rue nommés péjorativement "microbes" a fait 6 meurtres pour 252 blessés » chez leurs victimes [Houssou, 2014]. En termes d'activisme évoqué par Houssou, il faut plutôt entendre les activités ou actions criminelles de ces jeunes, qui

comme il est constaté, ne sont pas sans séquelles. En effet, au-delà des pertes matérielles pour les victimes, il y a aussi les homicides et les stigmates corporels, conséquences de la violence des « microbes ». Au cours de la même année, 122 jeunes sont mis aux arrêts, mais aucun ne fait l'objet de déferrement au regard de leur jeune âge. Le droit ivoirien en matière de délinquance des mineurs est très protecteur pour ceux-ci, les mesures préconisées étant, dans la majeure partie des cas, la remise aux parents ou des mesures de resocialisation.

Cette période de recrudescence des activités de ces jeunes délinquants coïncide avec un environnement sécuritaire délétère dans un pays où la justice des vainqueurs de la crise post-électorale et ses règlements de compte prospèrent.

Si les écrits évoqués, dans leur majeure partie, abordent sous différents aspects la question des gangs de rue en général, et celle des « microbes » en particulier, elles n'appréhendent pas la réaction des populations face au phénomène des jeunes délinquants violents dits « microbes ». Pour ce faire, cette contribution s'assigne comme objectif, au-delà de la revisite du phénomène lui-même, d'analyser les formes de réaction à la fois étatiques et informelles contre l'action de cette jeunesse criminalisée. Du questionnement autour de la réaction sociale découle l'hypothèse selon laquelle les populations ont choisi de résister aux activités des « microbes » à travers une organisation informelle de la sécurité. Parce que les forces de l'ordre n'ont pas été en mesure de rassurer les populations, celles-ci se sont organisées pour conserver leur quiétude.

La théorie retenue pour cette étude est celle de l'intimidation mutuelle de Cusson (1987). En effet, pour Cusson, « La sécurité peut être fondée sur la force, c'est-à-dire une force qui soit à la mesure de celle des rivaux ». Dans le contexte de la lutte contre les « microbes », la capacité de la riposte des populations, si elle est égale ou supérieure à celle des « microbes », aura pour effet d'équilibrer les forces et par conséquent de faire cesser les actes criminels de ces derniers. Cette réaction faisant suite à la réaction institutionnelle à travers les forces de l'ordre (police et gendarmerie) fera ensuite l'objet d'analyse.

Toutefois, avant d'en arriver aux résultats issus de cette étude, il importe de rappeler la méthodologie adoptée, à savoir le terrain d'étude, la population d'enquête choisie, les techniques de collecte et d'analyse des données.

## Note méthodologique

Le phénomène des microbes, sept ans après son apparition demeure un phénomène controversé. Ses origines, sa définition, le concept lui-même sont pour les chercheurs qui s'y intéressent, l'objet d'appréhensions diverses. Le phénomène étant relativement récent, chaque chercheur y va de son approche. Toutefois, il existe une convergence autour du fait qu'il s'agit d'abord d'une délinquance, voire d'une criminalité d'adolescents.

Dans le cadre de cette contribution, le phénomène ayant fait l'objet d'observations, des entretiens avec les acteurs, policiers, microbes, gros bras sont parus utiles pour appréhender le jeu de rôles de ceux-ci. L'échantillonnage non probabiliste par choix raisonné a permis de retenir des individus susceptibles de fournir les informations souhaitées, soit un total de 63 personnes dont 47 résidents et 16 agents des forces de l'ordre engagés dans la lutte. Les instruments de recueil de données utilisés sont l'entretien et la technique documentaire.

Le problème que l'étude appréhende, est celui de l'efficacité de l'action policière et de la réaction des populations à travers celle des groupes d'auto-défense et des gros bras face aux violences des microbes. Pour cela, l'analyse qualitative qui a été utilisée pour mettre en perspective les discours et informations de l'enquête dans divers quartiers de la commune d'Abobo a permis de vérifier la pertinence de la théorie retenue.

Cette étude porte sur les réactions de la société ivoirienne, à travers leurs opinions, attitudes et comportements, vis-à-vis du phénomène des « microbes ». Ainsi, pour mieux appréhender cet état de fait, les questions suivantes ont été posées : quelles sont les réactions institutionnelles et celles des populations abidjanaises ? Quelles en sont leurs logiques explicatives ? Ce questionnement a débouché sur l'hypothèse selon laquelle les réactions des populations abidjanaises face au phénomène des « microbes » sont la résultante de l'incapacité supposée ou avérée de l'État à ramener la quiétude au sein des populations et de l'extrême violence utilisée par les « microbes » lors de leurs agressions criminelles. Aussi, convient-il de rappeler que ce travail s'est appuyé sur la théorie de l'intimidation mutuelle de Cusson [1987] pour appréhender la réaction des populations face au phénomène des « microbes ». De ces travaux, il en résulte les résultats ci-après.

## Les microbes, un phénomène difficilement cernable

Le concept de microbe est apparu, dès le départ, difficile à cerner au regard de l'évolution multiforme du phénomène et d'une grille de lecture très diversifiée des chercheurs qui s'y sont intéressés [Sadia, 2014 Gaulithy, 2015]. D'ailleurs, assez récemment, Francis Akindès [2017], auteur du film documentaire *Paroles aux microbes*, lors de sa conférence publique n'a pas manqué de soulever les difficultés qu'une telle terminologie soulève.

Comme le constatait le doyen Carbonnier [1978] : « *L'évolution des mœurs donne naissance à des nouvelles formes de délinquance* ». Mais dans le contexte ivoirien, la crise militaro-politique ivoirienne (2002-2011), qui est une excroissance du multipartisme, ne relève en réalité d'aucune évolution, bien au contraire d'un recul démocratique au regard des choix d'accès au pouvoir de certains acteurs. Le phénomène des microbes qui apparaît comme une conséquence de cette période trouble – à la limite de l'anomie –, en référence à Merton, montre bien que s'il existe une économie de la guerre, il existe également des vestiges criminels de ces moments d'incertitude.

À l'apparition du phénomène, les acteurs avaient entre 8 et 15 ans, parfois 18 ans ; il s'agissait donc pour l'essentiel de mineurs au regard du droit pénal ivoirien, mineurs agissant en bande d'une dizaine de membres. La combinaison de ces caractéristiques (le nombre, la taille, l'âge et la rapidité d'action) a produit le nom de microbes<sup>1</sup> qui renvoie aussi, de façon imagée, « *au degré de nuisance ou de nocivité que les micro-organismes pathogènes (bactéries, champignons...) ont sur l'organisme humain* » [Gaulithy, 2015]. C'est donc cette capacité de nuisance et l'effet de groupe qui sont mis en relief à travers la dénomination « microbe ». Mais, si l'on s'en tient à de telles caractéristiques, les évolutions actuelles du phénomène obligent à revoir soit la dénomination, soit les caractéristiques. Car, peut-on dans ces conditions, être majeur et microbes ? Les controverses actuelles induisent à se limiter pour le moment à ne considérer comme microbes que les mineurs.

Les moyens d'agression sont pour l'essentiel des armes contondantes (bâtons, gourdins...) et des armes blanches (machettes et couteaux). Il s'agit une criminalité d'appropriation, sous-tendue par des actes de violences physiques qui font partie de la stratégie de terreur infligée aux victimes. En réalité, la finalité équivoque de ces

(1) Il ressort de nos investigations que l'appellation « microbes » vient des jeunes eux-mêmes qui se présentent comme des « des petits qui font mal », sous-tendus qu'ils sont certes jeunes, mais ayant une grande capacité de nuisance (entretien du 12/06/17 à Abobo « Derrière-rails »).

armes, qui ne sont pas interdites, complique d'éventuelles mesures de la prévention situationnelle dans la mesure où tout le monde peut posséder une machette, un gourdin, sans que cela ne soit source d'inquiétude pour autrui. La facilité d'acquisition de ces moyens rend encore plus anodine l'approche de ces jeunes et quasi imprévisible leur action, d'où l'impossibilité pour la police également de réagir promptement.

De ces constats, découle le questionnement suivant, à savoir quelles sont les entraves à l'action de la police ? Peut-on considérer la réaction des populations comme un retour aux vieux réflexes vindicatifs ? Les acteurs informels de la sécurité sont-ils les nouveaux remparts contre l'insécurité dans les quartiers « délaissés » par la force publique ?

L'organisation hiérarchique des microbes présente un style militaire : les bandes sont souvent parrainées par un Général. Il contrôle les troupes à travers ses lieutenants : les « devant-gbonhi » qui sont les chefs de bande. Ceux-ci sont en réalité les chefs opérationnels ; « *C'est rare que Général vienne sur le terrain. Moi, je lui rends compte des opérations et c'est lui qui gère les gains*<sup>2</sup> ».

Le mode opératoire utilisé de ces jeunes délinquants constitue également un élément d'identification. Il se caractérise par la violence et la rapidité des actions, l'effet de surprise est au cœur des actions. Certains « microbes » se font passer pour des petits mendiants avant de passer à l'acte. D'autres simulent des bagarres de rue ou des séances de démonstration de danse avant d'agresser les spectateurs du moment. « *On faisait un cercle avec des batteurs et un ou deux danseurs au milieu. Au fur et à mesure que les gens venaient nombreux assister, nous, on se retirait pour les laisser passer devant nous et lorsqu'on les avait bien encerclés, on agissait*<sup>3</sup>. » Lorsque cette approche a été écartée, les microbes ont choisi la technique de l'athlète qui consiste à pourchasser leurs cibles et malheur à celui qui se fera rattraper.

Lors de leur opération, la démarche utilisée est constante : rester en groupe et semer la panique pour profiter de l'effet de surprise chez leurs victimes dont les boutiquiers, les gérants de cabine téléphoniques, les passants et les vendeuses ambulantes font partie des cibles privilégiées. Il fallait éviter de se disperser pour devenir soi-même une cible de la vindicte populaire.



LES MOYENS D'AGRESSION SONT POUR L'ESSENTIEL DES ARMES CONTONDANTES (BÂTONS, GOURDINS...) ET DES ARMES BLANCHES (MACHETTES ET COUTEAUX). IL S'AGIT UNE CRIMINALITÉ D'APPROPRIATION, SOUS-TENDUE PAR DES ACTES DE VIOLENCES PHYSIQUES QUI FONT PARTIE DE LA STRATÉGIE DE TERREUR INFLIGÉE AUX VICTIMES. EN RÉALITÉ, LA FINALITÉ ÉQUIVOQUE DE CES ARMES, QUI NE SONT PAS INTERDITES, COMPLIQUE D'ÉVENTUELLES MESURES DE LA PRÉVENTION SITUATIONNELLE DANS LA MESURE OÙ TOUT LE MONDE PEUT POSSÉDER UNE MACHETTE, UN GOURDIN, SANS QUE CELA NE SOIT SOURCE D'INQUIÉTUDE POUR AUTRUI.



Relativement à l'étiologie du phénomène, des facteurs structurant le délitement constant de la cohésion sociale et nourrissant les dynamiques de violence impliquant les jeunes défavorisés peuvent être retenus. Il s'agit entre autres<sup>4</sup> de la recomposition des structures de la famille et l'apparition de nouveaux modèles de réussite sociale ; la quête du gain facile et la « valorisation » des nouveaux riches qui ont produit de nouveaux schèmes de réussite fondés non pas sur l'effort, mais sur le résultat, celui de la réussite sociale ; du délitement du système scolaire avec des programmes d'enseignement peu adaptés...

Ces facteurs, que l'on peut rattacher à l'évolution de la société ivoirienne et de ses incidences sur la criminalité d'une manière générale, ne peuvent seuls expliquer le phénomène des microbes. La crise de l'emploi est un facteur important du désespoir de la jeunesse ivoirienne. En effet, le secteur informel est le principal créateur d'emploi avec des revenus très bas malgré la croissance économique annoncée depuis 2012. Or, si la maîtrise de l'économie du secteur informel est telle qu'il est difficile statistiquement de faire des projections en termes de création d'emplois et de revenus, sa dimension informelle

(2) Entretien avec Kass, *Devant Gbonhi* du Général Hamed, un chef des « microbes » du quartier Kennedy (Abobo), le 21/06/2017.

(3) Djonh, 2<sup>e</sup> *devant Gbonhi* du Général Hamed, le 21/06/2017.

(4) Pré-rapport des ONG Interpeace et Indigo publié par le PNUD, l'UNICEF et l'ONU en 2015.

démontre toute son instabilité sociale. En outre, « la redistribution des richesses est faible, voire inexistante et ne contribue pas à éradiquer la pauvreté » [Akindès, 2017]. Toutefois, si un seul facteur devait être retenu relativement au phénomène des enfants dit « microbes », on citerait la crise militaro-politique et ses conséquences en termes de perte de repères moraux et de quête d'argent facile. La longue crise et les tensions sociales qu'elle a développées ont conduit les autorités à ne se soucier que de la survie de l'État ; les aspects passant au second plan.

En 2015, l'indice de développement humain classait la Côte d'Ivoire au 172<sup>e</sup> rang sur 187 selon le PNUD<sup>5</sup> avec 46,3 % de la population vivant sous le seuil de pauvreté<sup>6</sup>. En 2018, la Banque africaine du développement (BAD) estimait qu'en Côte d'Ivoire, « le taux de chômage se situait entre 70 % et 90 % de la population était en situation de chômage » [BAD, 2018].

Le phénomène des microbes concerne des jeunes originaires de milieux défavorisés, habitant des quartiers précaires, mais qui ne sont pas forcément des enfants de la rue. L'on dénombre généralement trois types de parcours de ces jeunes :

1. ceux issus des rangs des anciens combattants (enfants soldats) lors de la crise post-électorale de 2011. Ils sont considérés comme les plus dangereux, car ayant vécu les affres de la guerre. Ce sont eux qui sont soit les généraux ou les « devant gbonhi » ;
2. ceux qui étaient informateurs pendant ladite crise. Ce sont les acteurs opérationnels parce que connaissant bien l'espace, ils y opèrent avec plus de facilité ;
3. ceux qui ont intégré ces bandes, juste par suivisme et plus récemment. Victimes pour l'essentiel de l'effet d'imitation, ils ont rejoint les vétérans auprès de qui ils font office de novices, de stagiaires. Blumstein *et al.* [1998] et Mc Gloin [2007] montrent que c'est un phénomène d'initiation où les pairs cherchent à élargir leur capital humain en engageant les plus jeunes par une initiation.

Cette précocité de la trajectoire de la délinquance juvénile influence durablement les diversifications criminelles. La culture de la violence de ces adolescents, rappelons-le, est inspirée de la crise de 2002 à 2011 et elle semble répondre

pour eux à un besoin de « se recomposer en l'absence d'une autorité parentale réelle et de se construire en s'inspirant de modèles d'autorité et de réussite qu'offre la rue ». La violence devient donc banale et quotidienne, un moyen d'exister, de survivre dans un « univers où la marginalisation devient une expérience sociale partagée<sup>7</sup> ».

## La police, une réponse institutionnelle en mal d'adaptation

La police sera envisagée ici dans une assertion sociopolitique en référence à l'institution policière, c'est-à-dire la police nationale, la gendarmerie nationale, prise exclusivement dans le contexte de la lutte contre le phénomène des microbes [Loubet Del Bayle, 1993].

Dans la commune d'Abobo, aux premières lueurs du phénomène, furent les actions timides de la gendarmerie nationale pour l'endiguer, la première plainte n'ayant été portée qu'au premier trimestre 2012. Ces actions se sont heurtées à la fois à la méconnaissance du phénomène et aux dispositions relatives à la minorité pénale qui les empêchaient de mener des opérations répressives. Ainsi, chaque fois qu'un microbe était appréhendé, dans les 48 heures, parfois même dans la mi-journée, il était libéré, rendant ainsi inefficace toute action policière<sup>8</sup>.

La police nationale n'a pas non plus échappé à de telles frustrations. D'ailleurs, la mise en place de la brigade anti-microbes (BAM) en 2014, si elle a permis de spécialiser la lutte au sein de l'institution, n'a pas empêché sa prolifération vers d'autres communes comme Adjamé, Attécoubé et Yopougon. Le phénomène étant devenu dynamique et mouvant, avec parfois de nouveaux acteurs, issus de ces quartiers.

En outre, Abobo étant la commune la plus peuplée de la capitale économique Abidjan, avec plus de 2 millions (RGPH 2014), le dispositif policier est insuffisant pour réguler les pratiques délinquantes. Avec seulement sept commissariats et deux brigades de gendarmerie et un total d'environ 300 agents de la force publique, il est difficile de garantir un maillage suffisant de la commune avec un ratio extrêmement faible (1 agent pour 6 667

(5) Ministère des Affaires étrangères de la République française : présentation de la Côte d'Ivoire, France Diplomatie, 13/01/2017.

(6) « Côte d'Ivoire, population sous le seuil de pauvreté », *Actualitix*, 10/01/2016.

(7) Kouamé (Y. S.) & Moltes (A.), 2015, *Obstacles à la cohésion sociale et dynamique de violence impliquant les jeunes dans l'espace urbain*, Rapport de recherche participative, Interpeace & Indogo, Abidjan, Juillet.

citoyens). Par ailleurs, la situation des enfants qui est au cœur de la campagne de l'ONG de l'épouse du chef de l'État (Fondation Children of Africa), et la recherche de solutions des enfants en situation de difficulté en lien avec la crise post-électorale, ont longtemps entravé les actions des forces de l'ordre qui se retrouvaient sous une pression politique importante.

À ce sujet, en Janvier 2016, le chef de l'État ivoirien (Alassane Ouattara) puis son ministre de l'Intérieur et de la Sécurité d'alors (Hamed Bakayoko) ont invité l'opinion à ne plus qualifier ces jeunes de « microbes » mais simplement de « désœuvrés ». Pour les autorités ivoiriennes, l'expression « enfants microbes » tend à stigmatiser ces jeunes qui ont plutôt besoin d'un soutien. La ministre de la Solidarité, Yao Euphrasie, reprenant le combat du Gouvernement, préfère utiliser le concept juridique d'enfant en conflit avec la loi<sup>9</sup>.

Pour ces autorités, l'expression appropriée est donc celle de mineurs en conflit avec la loi. En réalité, il ne s'agit pas d'une innovation ; cette notion proposée par la doctrine française est connue depuis une vingtaine d'années. Seulement, dans cette expression qui est une composante du concept « d'enfant en contact avec le système judiciaire », on retrouve certes les mineurs en conflit avec la loi (ex-mineurs délinquants), les mineurs témoins, les mineurs en danger physique et moral et les mineurs victimes. Or, on y distingue les *pickpockets*, les voleurs à la tire ou à la roulotte... et les enfants dits « microbes » qui sont un type particulier qui se distingue des autres enfants en conflit avec la loi par les caractéristiques précédemment décrites. D'ailleurs, ils peuvent ne pas être confondus aux jeunes délinquants au regard de la gravité de leurs actes ; certaines de leurs victimes ayant trouvé la mort, il s'agit de cas d'homicides avec toute l'incidence au plan juridique (cour d'assises des mineurs). En clair, l'enfant microbe est un mineur en conflit avec la loi, mais le mineur en conflit avec la loi ne se résume pas à l'enfant microbe.

Une autre controverse, qui est née avec le temps, est celui des « microbes » mineurs qui sont devenus majeurs. La difficulté est de savoir s'ils peuvent continuer à être considérés comme des « microbes », puisque l'une des caractéristiques retenues est l'âge de la minorité pénale avec toutes les conséquences judiciaires qui en découlent. Si le mode opératoire n'a pas changé, les moyens utilisés non plus, l'âge, qui constitue un élément déterminant, ne permet plus de leur conserver cette appellation. Le

microbe s'évaluant à l'échelle du plus petit, le plus grand ne saurait être un microbe. Au-delà de la minorité (18 ans), leurs actes doivent être analysés au regard du droit commun.

Sur le plan des actions de lutte, les opérations se sont succédé : de l'opération « Baygon », qui visait en 2014 une répression vigoureuse des « microbes » [Ouattara, 2014], on est arrivé à l'opération « Épervier » en 2016, qui avait une connotation toute préventive cette fois-ci, avec de vastes coups de filet policiers effectués dans les fumoirs de drogue et autres zones criminogènes suspectes. En novembre 2018, la 4<sup>e</sup> opération avait lieu avec les mêmes objectifs :

- ratisser les quartiers cibles des microbes ;
- détruire les « fumoirs » et confisquer aux fins de sa destruction la drogue saisie ;
- saisir les armes diverses dont certaines à feu.

Avec les résultats très mitigés de l'action policière, la quasi-totalité des actions institutionnelles actuelles vise la rééducation et la réinsertion sociale des « enfants microbes ». Ainsi, une section spéciale pour la réinsertion sociale des « microbes » est créée au sein du centre de rééducation de Dabou en Décembre 2014 par l'Agence du désarmement, démobilisation et réintégration (ADDR). Sa mission consiste à former les jeunes aux métiers de la mécanique, de la menuiserie et de la couture avec, en soutien, des cours d'éducation civique et de secourisme. L'État procède également en Novembre 2016 à la réhabilitation du centre de Saliakro (M'Bahiakro – Bouaké) pour la mise en place d'un programme de réinsertion pour microbes. La création de la direction de la Protection judiciaire de la jeunesse et de l'enfance (DPJJE) vient renforcer la prise en charge socioéducative de l'enfant<sup>10</sup>. Outre ces actions, des campagnes de sensibilisation sont lancées à l'endroit des familles, tout en sollicitant la collaboration des populations (coopération et dénonciation des « microbes »). Mais ces actions, dont l'impact sur le phénomène n'est pas très prégnant, sont perçues par les populations comme des actions d'éclat, de la communication politique, orientées davantage vers les partenaires internationaux. En effet, dans la réalité, le phénomène demeure inquiétant et l'incidence de ces activités est perceptible.

(8) Cdt Yoboué : « La loi et les ONG nous ont lié les bras face aux microbes », entretien du 03/0482017.

(9) <https://www.google.com/yao+euphrasie+et+le+phenomene+des+microbes>, consulté le 14/8/2017.

(10) <https://observers.france24.com/fr/20150817-microbes-abidjan-centre-reinsertion-dabou-enfants-mineurs-cote-ivoire>, consulté le 30/01/2019.



À L'HEURE D'UN BILAN À MI-PAROURS, LA RÉACTION INSTITUTIONNELLE EST CELLE DES AUTORITÉS À TRAVERS LES DIFFÉRENTES STRUCTURES ÉTATIQUES, AVEC DEUX VOILETS : UN VOILET RÉPRESSIF ET UN VOILET PRÉVENTIF. À CE NIVEAU, LE TAUX DE RÉINSERTION EST FAIBLE À CAUSE DU MANQUE D'OPPORTUNITÉ ET DE LA CRAINTE DES ENTREPRISES. ON POURRAIT MÊME PROCLAMER L'ÉCHEC DE LA LUTTE, CAR, EN MATIÈRE DE PRISE EN CHARGE, CE NE SONT PAS LES ACTIONS D'ÉCLAT OU LES BREFS SÉJOURS EN CENTRE DE RÉÉDUCATION D'À PEINE TROIS MOIS QUI PERMETTRONT UNE RESOCIALISATION DE CES ADOLESCENTS QUI SE SONT FORGÉS DANS LA DÉLINQUANCE.



Dans la commune d'Abobo, « entre 2013 et janvier 2015, ce sont 196 microbes qui ont été interpellés et 20 autres lynchés à mort. Ils ont agressé 192 personnes dont 7 ont perdu la vie<sup>11</sup> ».

À l'heure d'un bilan à mi-parcours, la réaction institutionnelle est celle des autorités à travers les différentes structures étatiques, avec deux volets : un volet répressif et un volet préventif. À ce niveau, le taux de réinsertion est faible à cause du manque d'opportunité et de la crainte des entreprises. On pourrait même proclamer l'échec de la lutte, car, en matière de prise en charge, ce ne sont pas les actions d'éclat ou les brefs séjours en centre de rééducation d'à peine trois mois qui permettront une resocialisation de ces adolescents qui se sont forgés dans la délinquance.

Face à la persistance du phénomène des « microbes » continuant à sévir dans les quartiers, il importait pour les populations de trouver des solutions alternatives comme le recours aux acteurs informels de la sécurité tels des groupes d'auto-défense et « gros bras ».

## Les solutions « populaires », les gros bras et les groupes d'auto-défense

Les réactions communautaires relatives aux actions des « microbes » s'exercent avec l'appui des groupes d'auto-défense et des gros bras. Il s'agit d'une forme de *policing* non étatique que Bruce Baker [2008 et 2010] désigne par l'expression « *non-state policing* » que l'on peut traduire littéralement par « sécurité informelle ». Ces acteurs apparaissent comme le dernier recours lorsque l'État n'a pas pu répondre aux besoins des populations, parce que le ratio d'un agent de la force publique pour un citoyen est une chimère<sup>12</sup> et que les populations d'Abobo notamment y ont déjà eu recours. Les acteurs informels de la sécurité (AIS) que l'on pourrait assimiler en référence à Jean Paul Brodeur [2003] aux « *nouveaux visages de la police* » sont apparus pour assumer la fonction de garant de la sécurité dans leur environnement social ; ce pour quoi ils sont sollicités contre rémunération. Pour Hernando de Soto [2000], la principale caractéristique de cette économie informelle est l'extra-légalité ; l'action des AIS allant au-delà de la loi sans s'inscrire pour autant dans l'illégalité. Leur champ d'action couvre un domaine d'activités auxquelles la police ne se serait pas livrée : faire de la médiation, rassurer les populations, servir d'escorte... Dans la sphère extralégale, la fonction principale des acteurs informels de la sécurité (AIS) est de protéger les possessions précaires de populations déjà démunies, mais également de les protéger contre les agressions inutiles des « microbes ».

Si l'on n'est pas retourné aux anciennes époques de la vengeance privée, les voies trouvées dans les quartiers pour freiner, à défaut d'endiguer le phénomène, n'en sont pas si éloignées. Le recours aux groupes de vigiles ou d'auto-défense et aux gros bras s'apparente, à cet égard, à des solutions expéditives, outre les cas de lynchages populaires. Ces réactions des populations sont le reflet d'une société orientée de plus en plus vers la violence comme solution aux problèmes qu'elles rencontrent. Cela ne sous-entend pas qu'elles soient violentes par nature, mais elles ont recours à l'usage de la force chaque fois que de besoin au regard de l'absence d'une réaction régalienne. Ces actes de violence qui se traduisent par des lynchages, ont occasionné la mort de plus d'une trentaine de « microbes » supposés ou réels dont le plus célèbre est

(11) Quotidien *Le patriote* : « Criminalité : bientôt un "vaccin" contre les "microbes" », 04/06/2015.

(12) Et si elle existait, elle transformerait toute société en État policier.

Mamadou Traoré dit « Zama », chef de gang à Attécoubé, décapité le 14 avril 2015<sup>13</sup>.

Si dans le contexte d'une réaction sociale vigoureuse avec des erreurs et autres bavures parfois inévitables, les gardiens, veilleurs de nuit, gros bras sont sollicités, il n'en est pas de même des « vieux pères », car les microbes ne dialoguent pas, ils agressent et disparaissent. Or, les vieux pères connus dans leur sphère sociale comme des « sages » ne peuvent être d'une utilité face à ces jeunes délinquants. Leur arme favorite étant une démarche constructive de conciliation, elle ne peut prospérer dans un environnement où le dialogue n'a pas sa place. D'ailleurs, les quelques actions entreprises vers eux se sont soldées par des échecs<sup>14</sup>.

Aujourd'hui à Abobo, tous les quartiers de la commune touchés par le phénomène disposent de leurs propres AIS. Pour l'essentiel, il s'agit de jeunes gens recrutés sur place et ayant un enracinement local. Ceux-ci sont généralement bien informés des activités des « microbes » et des besoins et attentes des populations. Parfois, ces groupes se constituent en dehors de toute sollicitation parce qu'il s'agissait pour eux de sécuriser leur propre quartier. Cette action coïncidant avec les attentes sociales fait d'eux les derniers recours, de véritables héros.

Au départ, reposant sur du bénévolat, leurs actions n'étaient pas rémunérées dans certains quartiers. Mais avec le temps, les habitants se sont organisés pour leur verser des cotisations à la hauteur de leur bourse. Les contrats qui s'établissent ainsi sont généralement verbaux. Il s'agit d'un accord tacite fondé sur la confiance entre les parties. Cette évolution de l'offre transforme la sécurité informelle en activité mercantile.

L'existence et l'importance de ces acteurs informels de la sécurité sont une réponse aux insuffisances des pouvoirs publics : la police ivoirienne ne parvenant pas à assurer la sécurité des personnes dans ces quartiers défavorisés. Les AIS interviennent ainsi dans des domaines qui ne sont pas pris en charge par l'institution policière. En effet, les actions de la police relèvent du domaine de la loi, les insatisfactions de la population, au regard de la réactivité de la police jugée procédurière, la conduisent à solliciter les AIS (Yoro 2015).

## Conclusion

Les principaux résultats issus de cette recherche mettent l'accent sur le fait que la réaction sociale face au phénomène des « microbes » est à appréhender sous deux aspects : d'une part, la réaction institutionnelle et celle des populations, d'autre part. Pour y parvenir, la réaction institutionnelle s'est bâtie autour de deux orientations. Le volet préventif a consisté en la mise en place de programmes de sensibilisation à l'endroit des parents des présumés « microbes » ainsi que toutes les communautés résidant dans ces communes, de même que des programmes de réinsertion sociale confiés à la Cellule d'exécution du programme de protection des enfants et des adolescents vulnérables (PPEAV). Outre le volet préventif, une autre phase, répressive, a été confiée aux acteurs de la sécurité publique. Elle a porté sur la mise en route d'opérations coup de poing à travers des opérations « Baygon » et « Épervier ». Pour ce qui est des réactions des populations, le recours aux AIS s'est avéré le dernier rempart contre un phénomène qui se présente de plus en plus comme un serpent de mer, difficile à maîtriser, car l'hydre renaît chaque fois que l'on croit l'avoir vaincu.

La réponse des AIS, qui fait appel à la force, a conduit à la conclusion selon laquelle la violence qu'elle manifeste, à travers les actes de lynchage, n'est qu'une expression de la libération des instincts agressifs à la suite des agressions subies. Ainsi, face la frustration créée par l'incapacité des autorités policières à assurer la sécurité des populations, celle-ci répond par l'agression. Cet état de fait peut être mis en rapport avec la théorie de frustration-agression de John Dollard. Par ailleurs, la violence (lynchage) envisagée par les populations comme réponse aux agressions des « microbes », face à l'inefficacité des autorités compétentes, a également été appréhendée par Breteau et Zagnoli [1980] puis par Cusson [1987]. Pour Breteau et Zagnoli [*op. cit.*, p. 49], « *en se vengeant, on apporte la preuve de sa capacité à réagir. Cette capacité confirmée constitue une menace pour tout offenseur éventuel et remplit donc une fonction dissuasive* ».

En définitive, une forme de substitution sournoise dans les quartiers délaissés de la police s'opère par l'action des AIS, créant ainsi une nouvelle forme d'organisation autour d'une organisation non régaliennne de sécurité. Si la psychose qui règne dans le district d'Abidjan eu égard aux actes criminels commis par les « microbes » semble compréhensible, il n'en demeure pas moins qu'à l'évocation

(13) <https://www.ivoireactu.mondoblog.org/2015/04/15/zama-un-chef-des-microbes-tue-par-la-foule>, consulté le 17/04/2015.

(14) Un jeune imam (ex-combattant), qui nous raconté avoir tenté vainement d'amener les « microbes » de son quartier à renoncer à ces pratiques, s'est résolu à « les affronter avec les jeunes du quartier, jusqu'à ce qu'un camp gagne ». Leur détermination à ne pas se laisser faire a convaincu la bande de microbes à migrer vers d'autres lieux plus favorables. Entretien avec l'imam Ladjji Cissé, Abobo BC, le 23 /06/2017.

du terme « microbes », les réactions observées laissent interrogateur. Aujourd'hui, où le phénomène semble s'essouffler, peut-on attribuer le seul ou grand mérite aux AIS ? Certes, s'ils n'y sont pas étrangers, l'action de tous les acteurs, même de l'État, ne peut être occultée. En outre, la répression ne saurait être une solution durable, encore moins les discours moralisants. Il faut donc

infléchir l'option répressive en réduisant le « poids » des AIS par la mise en place dans ces quartiers des services de police communautaires, c'est-à-dire associer les citoyens à la police pour la gestion de leur propre sécurité. Une reconversion de ces jeunes est encore possible à travers une prise en charge mieux organisée avec en finalité des perspectives d'emploi ■

## Bibliographie

- AKINDÈS (F.), 2017, *Engagement des adolescents et jeunes dits « Microbes » dans la violence à Abobo*, Rapport de recherche participative, ONG Interpeace & Indigo, Abidjan.
- AUDRAN (M.), 2014, « Le problème de la délinquance juvénile », émission diffusée le 13/03/2014 par Radio France International (RFI).
- BRETEAU (C. H.) & ZAGNOLI (N.), 1980, « Le système de gestion de la violence dans deux communautés rurales méditerranéennes : La Calabre méridionale et le N.E. Constantinois », in VERDIER (R.) (ed), *La vengeance* (42-73), Paris, éditions Cujas/CNRS.
- BRODEUR (J. P.), 2003, *Les nouveaux visages de la police*, Montréal, Les Presses de l'Université de Montréal.
- CARBONNIER (J.), 1978, *Sociologie juridique*, Paris, PUF.
- CUSSON (M.), 1987, *Pourquoi punir ?* Paris, Dalloz.
- CUSSON (M.), DOUMBIA (Y.), YEBOUET (B.), 2017, *Mille homicides en Afrique de l'ouest : Burkina Faso, Côte d'Ivoire, Niger et Sénégal*, Montréal, Les Presses de l'Université de Montréal.
- DIDR/OFPPRA, 2017, *Les groupes de « microbes » à Abidjan. Fonctionnement des gangs et politique de lutte des autorités*, Didr/Ofpra.
- GAULITHY (K. G.), 2015, « Les Gangs de « microbes » à Abidjan », *Revue internationale de criminologie et de police technique et scientifique*, 68 (4), p. 406-422.
- LOUBET DEL BAYLE (J. L.), 1993, *La police, approche socio-politique*, Paris, Montchrestien.
- MPFFPE, 2016, Atelier de réflexion sur le thème : « Situation des enfants dits « microbes » : stratégies de prise en charge incluant les familles et les communautés ».
- PORTO (M. S. G.), 2001, « Exclusions sociales et violence : le cas du Brésil », *Sociologie et sociétés*, 33 (2), p. 49-66.
- SADIA (M.-A.), 2014, « Environnement, personnalité et violence chez les mineurs incarcérés : cas de 5 « microbes » d'Abidjan », *Revue Africaine de Criminologie*, 14, 56-67.
- SALAZAR (G.), 2006, « Politiques des enfants de la rue au Chili », *Anthropologie et sociétés*, 30 (1), 75-96.
- Articles de journaux
- A.S., 2015, « Lutte contre l'insécurité à Abobo : 200 fumoirs détruits, 250 microbes arrêtés et déférés », *Le Mandat*, n° 1774 du 17 décembre, p. 8.
- F.C., 2014, « Nous voulons éradiquer le phénomène », *Le Nouveau Réveil*, N° 3758 du 14-17 août, p. 3.
- HOUSSOU (A.), 2014, « Une fusillade entre policiers et « microbes » fait plusieurs morts », *L'Intelligent d'Abidjan*, n° 3161 du 19-20 juillet, p. 2.
- O.I., 2016, « Ne les appelons plus « microbes », mais enfants en conflit avec la loi », *L'Intelligent d'Abidjan*, n° 3656 du 21-22 mai, p. 7.
- OUATTARA (M.), 2014, « La police lance l'opération « Baygon » », *Nord-Sud Quotidien*, n° 2724 du 05/08/2014, p. 8.
- K. E., 2015, « Criminalité : bientôt un « vaccin » contre les « microbes » », *Le patriote*, 4 juin.
- TANO (R.), 2015, « « Enfants microbes » la psychose grandit ! », *Nord-Sud Quotidien*, n° 3027 du 18 août, p. 7.
- TANO (R.) & M.T., 2015, « Peut-on régler définitivement la question des « microbes » à Abidjan ? », *Nord-Sud Quotidien*, n° 3032 du 24 août, p. 6.



TOURÉ (Y.), 2015, « *Tout sur le phénomène des “microbes”* », L'Expression, n° 1704 du 28 avril, p. 6. <https://www.google.com/yao+euphrasie+et+le+phénomene+des+microbes>, consulté le 14/8/2017

YALALA (M.), 2013, « La guerre est déclarée contre les réseaux du banditisme urbain, le phénomène des “kuluna” à Kinshasa », publié le 20 novembre dans le journal en ligne *Le Potentiel*, consulté le 26/03/2015. <https://www.ivoireactu.mondoblog.org/2015/04/15/zama-un-chef-des-microbes-tue-par-la-foule>, consulté le 17/04/2015.

#### Sites internet

<http://www.atooci/2017/11/08/pr-francis-akindes-propose-discrimination-positive-phenomene-de-microbes/>, consulté le 15/01/2019

<https://www.ivoiresoir.net/exclusif-cote-divoire-taux-de-chomage-entre-70-et-90-voici-le-vrai-rapport-de-labad/>, consulté le 15/01/2017

# Relations police- population et *community* *policing* : le paradoxe sud-coréen

Éric MEYNARD

La Corée du sud est un pays bien mal classé au regard de la confiance qu'expriment les poliçables à l'endroit de leur force publique, la police nationale.

La police nationale sud-coréenne au reste ne s'en cache pas puisqu'elle publie régulièrement l'index de confiance à l'égard des forces de l'ordre établi par l'OCDE. Sur l'ensemble des pays, la Corée du sud se retrouvait systématiquement au 27<sup>e</sup> rang de 1991 à 2003 sur 30.

## Eric MEYNARD

Éric MEYNARD est diplômé en criminologie et titulaire d'un master 2 en sécurité publique, il a occupé des postes de directeur d'hôpital et de sous-préfet. Il a publié en 2014 *Criminalité, police et sécurité publique en République d'Irlande* aux éditions de L'Harmattan.



Ce déficit de « confiance », voire de défiance, à l'endroit de la police nationale génère au fond deux types de conséquences : elle conduit aussi bien à ce que la police aujourd'hui n'a que peu de prise sur le corps social, mais inversement, la population à tendance à mépriser sa police, et plus largement un certain esprit civique.

Cette situation doit s'appréhender dans le cadre d'une histoire politique, économique et sociale qui s'est singulièrement accélérée depuis le début des années 1990. En 1991, la population sud-coréenne fait le choix de la révolution démocratique, mettant ainsi un terme à la dictature militaire qui installa son règne à la fin de la Seconde Guerre mondiale. La perception d'une police politique à la discrétion du pouvoir perdura bien après la période de la dictature.

En outre, la période de l'occupation japonaise avait également, dès 1910, contribué à une vision très négative de la police, à la solde d'un envahisseur tant honni.

À partir de l'avènement de la démocratie en 1991, la police nationale s'évertua à conjurer une image déplorable en multipliant les initiatives de nature à tisser un lien de confiance avec les Coréens.

## Une police qui n'a pas la confiance de ses poliçables

En 2000, une enquête de victimation fut conduite selon le même protocole de l'*International Crime Victim Survey* (ICVS) en retenant treize infractions : le cambriolage, la tentative de cambriolage, le vol simple, le vol de véhicule, le vol à la roulotte, la détérioration de véhicules, le vol de deux roues, et de bicyclettes, les agressions sexuelles, les agressions et les menaces de coups et blessures, les infractions au droit de la consommation et la corruption.

Avant l'année 2000, l'enquête de victimation menée par la police nationale coréenne ne reprenait pas les mêmes critères que l'ICVS, ce qui limitait les comparaisons.

En même temps, l'harmonisation des deux enquêtes n'exclut pas tous les biais, d'ordre culturel et sociétal, notamment dans le rapport des citoyens à la délinquance en particulier, et avec la déviance en général.

La comparaison établie par Jang en 2000<sup>1</sup> apporte quelques éclairages intéressants. Sur les bases de ces données, la Corée du sud apparaît comme un des pays les plus sûrs au monde en matière de vols et d'atteintes aux personnes. En revanche, le taux de victimisation en matière de cambriolage était le plus élevé des pays de l'OCDE, à l'exception de l'Australie. Si l'on procède à une comparaison dans le temps, un auteur comme Hwang<sup>2</sup> montre que le taux de victimisation baisse de manière continue à partir des années 1990 jusqu'à la fin des années 2000.

Cette tendance est pour le moins singulière au regard d'autres pays qui ont connu une phase de croissance économique et de modernisation qui génère systématiquement un accroissement de la délinquance. Les changements sociaux liés notamment à l'industrialisation et à l'urbanisation galopante n'ont pas provoqué une montée de la délinquance, et cela peut être attribué, à l'instar d'autres sociétés asiatiques comme le Japon, à l'homogénéité culturelle de la société coréenne et son fort système de contrôle social informel.

Parallèlement à cette « sous-criminalité » relative, les Coréens ne montrent que très peu de considération et de satisfaction à l'égard de leur force publique.

L'étude de Jang dans le cadre de la *Korean Crime Victimization Survey*, menée en 2000, met en exergue un taux de satisfaction calamiteux comparé à ceux des autres pays occidentaux, figurant dans l'*International Crime Victimization Survey*, conduite sous la direction de Van Kesteler<sup>3</sup>.

Alors que les pays de l'Europe du nord (Danemark, Finlande, Suède, Pays-Bas) ainsi que les pays « neufs »

(Canada, Australie), mais aussi la Catalogne, affichaient des taux de satisfaction de plus de 70 %, la Corée du sud se singularisait par un taux de satisfaction de 16,8 % en 2000.

Cette insatisfaction, voire défiance, à l'égard de la police peut également être appréhendée à la lumière du très faible taux de reportabilité des délits, 21,9 % en 2000, c'est-à-dire plus de deux fois moins que la moyenne des pays occidentaux.

L'enseignement qu'en tire Jang mérite réflexion : «*These low rates mean that people are much likely to be reliant on the police authority in South Korea, and that they are less satisfied with the performance of their police officers, regardless of the high level of security*»<sup>4</sup>.

Ce faible taux de reportabilité est, selon une étude de Tak, lié à différents facteurs, par exemple que l'infraction soit suffisamment grave selon la victime pour être déclarée ou l'impact de délit sur la réputation sociale de la victime, la relation au voisinage, l'âge ou encore le sexe de la victime<sup>5</sup>.

D'autres études<sup>6</sup> ont démontré que les victimes sont rétives à l'idée de porter à la connaissance des autorités les délits associés à la plus forte opprobre sociale, comme les agressions à caractère sexuel. L'enquête KCVS a recherché les raisons pour lesquelles les victimes ne s'adressaient pas à la police : 37,7 % invoquaient le caractère mineur de l'infraction, mais 23 % des répondants invoquaient le fait qu'ils ne faisaient pas confiance aux policiers pour prendre en compte et traiter leur demande.

Ce dernier aspect renvoie à la conviction que la police est efficace dans son travail. Or, là encore, la police sud-coréenne se singularise par un score des plus médiocres selon l'étude de Jang menée en 2000.

Seulement 37 % des répondants estiment que la police est efficace pour lutter contre la criminalité, à comparer aux 87 % exprimés par les États-Uniens, 85 % par les Canadiens, 70 % par les Finlandais.

(1) Jang (J.O.), 2000, *International Crime Victimization Survey*, Korean Institute of Criminology.

(2) Hwang (J.), 2009, «Critical comparison of official statistics to victimization data: explaining the reduction of the victimization rate», *Korean Criminal Review*, 1, p. 249-283.

(3) Van Kesteler (J.P.), Mayhew (P.), Nieuwbeerta (P.), 2000, *Criminal victimization in seventeen industrialized countries*.

(4) Jang, *op.cit.* p. 275.

(5) Tak (J.), 2010, «Reporting theft and fraud victimization in Korea», *Criminological Review*, 21 (3) : 53-75.

(6) Baumer (E.) et Lauritsen (J.), 2010, Reporting crime to the police, 1973-2005: A multivariate analysis of long-term trends in the national crime survey and national crime victimization survey, 48 (1) : 131-185.

## Les conséquences du déficit de confiance

Cause ou conséquence, il n'en demeure pas moins que la faiblesse de l'esprit civique vient renforcer la faiblesse du lien de la force publique à la population. Certains observateurs ne manquent pas de souligner que «*South Koreans often bear unfavorable opinions regarding the fairness of their nation's law and they have weak commitment to the abiding of such laws are considered inconvenient*»<sup>7</sup>.

Yi et Lew, dans une enquête publique publiée à partir d'un échantillon de plus de deux mille personnes, montraient que plus de 58 % des répondants ne s'estimaient pas tenus au respect des lois, en invoquant leur caractère autoritaire et non démocratique.

De la même manière, une enquête menée par la police nationale<sup>8</sup> publiée en 2012, corrobore cette faible observance des lois et règlements, notamment ceux relatifs au Code de la route, aux enquêtes judiciaires ou encore à l'ordre public. S'agissant de ce dernier aspect, ce n'est pas tant leur illégitimité perçue que la faiblesse des sanctions prévues qui incline à leur faible observance. La plupart des contrevenants sont souvent remis en liberté contre caution.

Au fond, la faiblesse de l'esprit civique couplée à la défiance à l'égard de la police, encourage les comportements non coopératifs avec les agents de la force publique.

## Le Community Policing comme solution : de l'évidence au paradoxe

Le *Community Policing* a été, à l'instar d'autres pays, considéré comme la doctrine susceptible de juguler une criminalité qui a eu tendance à croître pendant les « années FMI », mais également comme solution à la crise de légitimité de la police sud-coréenne.

La mise en place de cette police de proximité fut introduite dans un élan réformiste en 1999, sous le slogan aux accents volontaristes « Operation Grand Reform 100 Days ».

(7) Jinsi (P.), Julak (L.), *op.cit.*, 2016.

(8) Korean National Police Agency, 2010, Séoul.

(9) Moon (R.), Choo, 2004. «The politicization of police in South Korea: a critical review», *Policing: An International Journal of Police Strategies and Management*, Vol. 27 n° 1, p. 517-59.



LE *COMMUNITY POLICING* A ÉTÉ, À L'INSTAR D'AUTRES PAYS, CONSIDÉRÉ COMME LA DOCTRINE SUSCEPTIBLE DE JUGULER UNE CRIMINALITÉ QUI A EUTENDANCE À CROÎTRE PENDANT LES « ANNÉES FMI », MAIS ÉGALEMENT COMME SOLUTION À LA CRISE DE LÉGITIMITÉ DE LA POLICE SUD-CORÉENNE.

LA MISE EN PLACE DE CETTE POLICE DE PROXIMITÉ FUT INTRODUITE DANS UN ÉLAN RÉFORMISTE EN 1999, SOUS LE SLOGAN AUX ACCENTS VOLONTARISTES « OPERATION GRAND REFORM 100 DAYS ».

ELLE DOIT S'APPRÉHENDER DANS LA DYNAMIQUE LANCÉE PAR LE GOUVERNEMENT DE KIM DAE JUNG, DONT LA PRIORITÉ ÉTAIT LA CONSTRUCTION D'UN RÉGIME POLITIQUE DÉMOCRATIQUE ET LIBÉRALE AINSI QU'UNE FORTE PROMOTION DES DROITS ET LIBERTÉS FONDAMENTALES.



Elle doit s'appréhender dans la dynamique lancée par le gouvernement de Kim Dae Jung, dont la priorité était la construction d'un régime politique démocratique et libérale ainsi qu'une forte promotion des droits et libertés fondamentales.

Pour la police, cela se traduit par la mise en place d'une police de proximité en lieu et place d'une police d'ordre, résolument tournée vers la demande de sécurité des Sud-Coréens.

Cette doctrine a, d'autant plus facilement, pu se mettre en place que la Corée conservait un système de monoplice, fortement centralisé. Le pays revenait de loin : la police coréenne fut l'instrument d'une féroce répression sous l'occupation japonaise, puis celui d'une dictature militaire impitoyable<sup>9</sup>.

Frappé de cette tare ontologique d'illégitimité, le gouvernement avait pour principale préoccupation de changer l'image de la police, comme le soulignait fortement la police nationale : «*change citizens' perceptions of the police and lessen citizens'sustained distrust and anger toward the police*<sup>10</sup>».

Une enquête majeure menée par trois universitaires en 2012<sup>11</sup> a remis en cause cette relation *a priori* d'une évidence doxique, bien que parfois nuancée par certaines études, d'une relation univoque entre *Community policing*, plus grande proximité à la population et diminution du sentiment d'insécurité.

Au moment où le gouvernement de Kim Dae Jung se lança dans son ambitieuse réforme en 1998/1999, peu d'évaluations existaient à ce moment permettant de juger de l'impact de la police communautaire sur le sentiment d'insécurité.

Or, le passage d'une police d'ordre à une police de sécurité publique, c'est-à-dire tournée vers le policable et non plus vers la souveraineté de l'État, ne disposait donc pas des critères d'évaluation adéquats<sup>12</sup>. Les objectifs n'étant pas les mêmes, la manière de les évaluer ne pouvait être identique. En effet, l'impact de la police de proximité nécessite des critères d'évaluation principalement qualitatifs, comme la réduction du sentiment d'insécurité, la satisfaction des citoyens et l'amélioration du quotidien des citoyens en mettant en avant le concept de «*quality of life crime*<sup>13</sup>».

Par ailleurs, la proximité à la population, qui renvoyait à une police du renseignement et de répression politique, n'était pas tant le problème que la nature de celle-ci, et donc de la légitimité politique qu'elle servait<sup>14</sup>.

En effet, les Coréens étaient habitués à cette proximité de la force publique à travers le maillage des postes de polices (*substations*). Cette association de la police et de la population s'organisait à travers les «*Crime Prevention Advisory Committee* », dont la fonction n'était pas tant

de collaborer à la politique de sécurité publique que d'être le simple réceptacle des discours policiers à l'endroit de la société civile.

Une des premières mesures mises en place consista à mettre un terme aux patrouilles planifiées par la hiérarchie policière sans considération pour les besoins locaux.

La police prit également l'initiative d'ouvrir les portes de ses commissariats et postes de police aux citoyens et des représentants d'associations des habitants furent désignés pour participer à des réunions et débats publics.

La réforme de la police se voulait également proactive, au travers de campagnes de porte-à-porte, de questionnaires afin de mieux cerner la demande sociale de sécurité des Sud-Coréens.

Par ailleurs, la police s'évertua à ajuster au mieux sa «*prestation* » auprès non seulement des communautés de quartiers, mais aussi des foyers, à travers par exemple le projet de «*Vacant Houses Reporting Program*» qui consistait à surveiller des logements laissés inoccupés en l'absence de leurs propriétaires pendant leurs vacances.

Le dispositif 122 Service Corps fut spécifiquement établi aux fins de répondre à toutes les demandes des habitants, sécuritaires, en termes de tranquillité publique, voire environnementale, au travers de «*Voluntary Patrol Organisations*» et des «*Crime Patrol Organisations*».

## Appréhender le sentiment d'insécurité en Corée du sud

La question du sentiment d'insécurité n'a jamais véritablement été considérée en Corée du Sud. La première étude est celle de Hwang<sup>15</sup> dont l'objet fut d'examiner les impacts à Séoul de la mise en place de la police de proximité sur le sentiment d'insécurité. Cette

(10) Korean National Police Agency, *White Paper*, 2000-2001.

(11) Roh (S.), Kwak (D-H), Kim (E.), *Community Policing and fear of crime in Seoul: a test of competing models*, *Policing: An international Journal of Police Strategies and Management*, Vol. 36 No. 1, 20013, p. 199-222.

(12) Silverman (E.B) et Della-Giustina (J.), 2001, «*Urban policing and the fear of crime*», *Urban Studies*, Vol. 38 N° 5-6, p.941-57.

(13) Xu *et alii.*, 2005, «*Discovering the impact of community policing: the broken windows theories, collective efficacy and citizens' judgement*», *Journal of Research in Crime and Delinquency*, Vol. 42, n° 2, p. 147-86.

(14) Moon *et alii.*, 2005, «*Korean police officers' attitude toward the efficacy of mini-police stations*», *Journal of Criminal Justice*, vol.33 N° 5, p. 441-49.

(15) Hwang (E.), 2006, «*A multilevel test of fear of crime: the effect of social conditions, perceived community policing activities, and perceived risks of victimization in a megalopolis*», *Doctoral Dissertation, Dissertation Abstracts International*, vol. 67, n° 3990, 2007, Michigan State University, East Lansing, MI.

enquête montra l'aspect très limité d'une police de proximité attendu que : «*Confucianism, Korean society, the community integration factor may exert a limited influence on the people's fear of crime*<sup>16</sup>»

Roh *et alii*.<sup>17</sup> au terme de leur enquête auprès d'un échantillon représentatif des habitants de Séoul aboutissent à des conclusions habituelles d'une relation positive entre police de proximité et sentiment d'insécurité. À l'inverse, celui-ci ne décroît pas lorsque celle-ci est mise en oeuvre.

Selon ces auteurs une première explication tient au fait que lorsque la police a été réformée sur la base du *Community Policing* en 1999, la police n'accorda que peu d'importance au sentiment d'insécurité. La mise en œuvre de la police de proximité avait avant tout pour but de valoriser l'image de la police en la rendant plus visible sur le terrain.

Dans son rapport annuel en 2001, la police nationale indiquait que la réforme de l'institution se trouvait à un moment critique dans la mesure où elle n'avait pas encore su dépasser son image de police d'ordre, répressive et autoritaire.

Par ailleurs, le sentiment d'insécurité était quelque chose de peu ressenti aussi bien du côté de la police que des policiers. La raison en est tout simplement que la société coréenne a toujours connu un faible niveau de criminalité, et ce niveau n'a pas progressé pendant les années de boom économique et de l'urbanisation galopante. Roh *et alii*.<sup>18</sup> annoncent l'hypothèse selon laquelle l'homogénéité socioculturelle de la société coréenne a joué le rôle d'un véritable « amortisseur » des effets sociaux et sociétaux de la période de modernisation du pays.

Même si pendant les années dites du « FMI », consécutives à la grave crise asiatique de 1997, les indicateurs macro-économiques se dégradèrent : hausse du chômage, des inégalités, et sur un plan sociétal, entrée en crise du modèle familial. Le taux de criminalité n'augmente que de 13,2 % en 1997 et de 18,8 % en 1998.

Par ailleurs, si la mise en place de la police de proximité n'a pas eu prise sur le sentiment d'insécurité, par ailleurs négligeable, c'est que les Coréens et Coréennes ne considèrent pas la délinquance comme un problème local mais national.

Il existe donc bien un véritable « paradoxe sud-coréen » en que ce le *Community Policing* développé pendant les années 2000 n'a que peu contribué à la fois au renforcement du lien police-population et à la diminution du sentiment d'insécurité.

Au contraire, cette relation est aujourd'hui toujours aussi compliquée, une des priorités du gouvernement étant de lutter contre les oppositions et obstructions de la police par les policiers dans l'accomplissement de leur mission<sup>19</sup> ■

(16) *Ibid.*, p.17

(17) Roh (S.) et Oliver (W.M.), 2007, «Effects of policing community upon fear of crime: understanding the causal linkage», *Policing. An International Journal of Police Strategies & Management*, vol 28, n° 4, p.670-83.

(18) Roh *et alii*, 2010, «Crime victimization in South Korea: a multilevel approach», *Journal of Criminal Justice*, vol. 38, n° 1, p. 301-10

(19) Yoon Hac-Sung, Han Min-Kyung, *Obstruction of Police's Performance of Official Duties*, Korean Institute of Criminology, Research Reports II, 2015-2016.

# Le jeu des 8 familles d'atteintes à la sécurité économique et ses 48 fiches thématiques

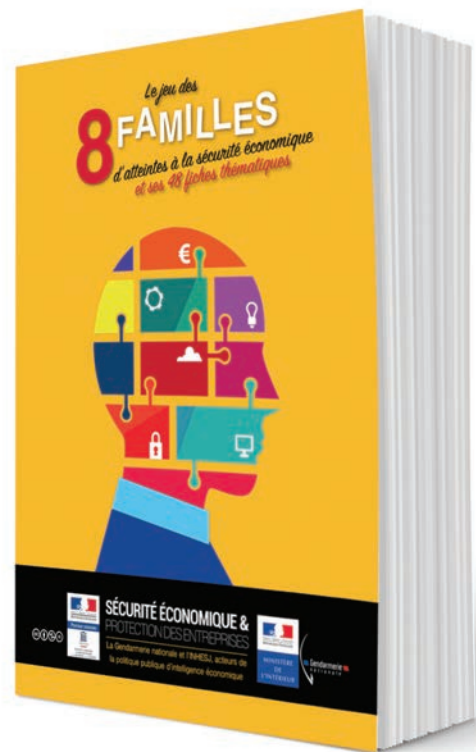
Les entreprises évoluent dans un monde complexe et incertain. Pour faire face à la multiplication des risques et des malveillances, elles doivent mettre en place une véritable culture de sécurité/sûreté et d'intelligence économique. L'analyse de l'environnement global de l'activité des entreprises démontre ainsi que l'intelligence et la sécurité économiques constituent un enjeu majeur pour l'ensemble des acteurs économiques. Si les nouvelles technologies offrent des solutions adaptées à certaines situations, la sensibilisation des personnels de l'entreprise reste la mesure la plus efficace.

Soucieux d'apporter leur contribution à un tel enjeu, l'Institut national des hautes études de la sécurité et de la justice (INHESJ) et la Direction générale de la Gendarmerie nationale (DGGN) ont décidé de coordonner leurs efforts pour sensibiliser aux atteintes à la sécurité économique par la création, en 2019, d'un kit de sensibilisation créé à cet effet.

Ce kit de sensibilisation est composé de :

- 48 fiches thématiques organisées en huit familles : atteintes physiques sur site, fragilisations/désorganisations, atteintes aux savoir-faire, intrusions consenties, risques financiers, risques informatiques, fragilités humaines, atteintes à la réputation ;
- un jeu de 48 cartes correspondant à chacune des fiches, pour une approche ludique et didactique.

Le jeu de cartes peut être commandé gratuitement auprès de l'INHESJ (commandes individuelles uniquement - dans la limite des stocks disponibles).



## Le livre

### NOUVEAU PRÉCIS D'HISTOIRE DU FBI

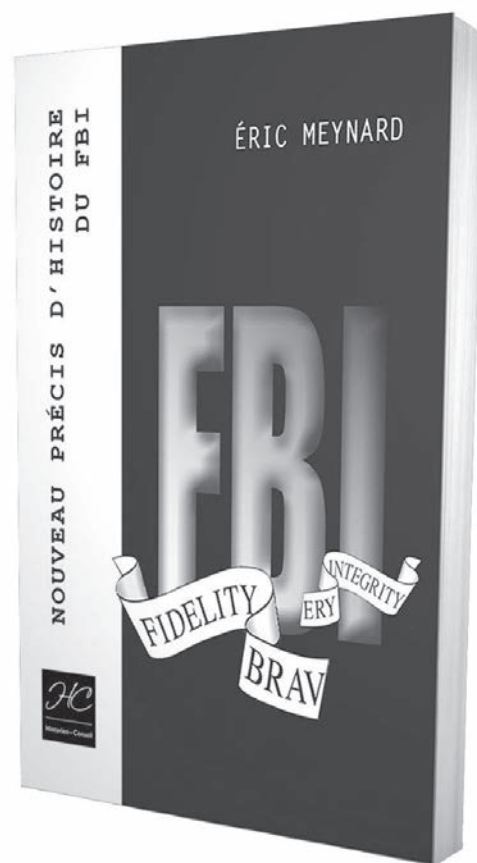
Éric MEYNARD

Entre affaires politiques fracassantes et soupçon de police secrète, le *Federal Bureau of Investigation* a atteint le statut de mythe absolu dans l'histoire du XX<sup>e</sup> siècle. Sujet d'innombrables films, séries et ouvrages plus ou moins documentés, il a, depuis un siècle, été investi par chacun de ses propres fantômes. Mais que cache réellement cette sombre légende ?

Pour faire le point en toute objectivité, voici une synthèse claire et concise sur l'histoire du *Bureau*, afin de comprendre non seulement ce que fut son rôle réel dans un certain nombre d'affaires retentissantes, mais aussi de décrypter les logiques qui ont présidé à sa création puis à sa mise en oeuvre dans le contexte mouvementé de l'histoire des États-Unis.

## Pour en savoir un peu plus sur l'auteur

Éric Meynard, diplômé en criminologie et titulaire d'un master en sécurité publique, a occupé plusieurs postes dans la haute fonction publique ; il a notamment été sous-préfet. Il a publié en 2014 *Criminalité, police et sécurité publique en République d'Irlande* et écrit régulièrement pour les *Cahiers de la sécurité et de la justice* et la *Revue française de criminologie*.



Editeur : Historien-Conseil

Parution : mars 2020

Pagination : 150

Format : 12x18 cm

Prix : 12,50 euros



