UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

UNIVERSITÉ PANTHÉON-ASSAS – PARIS II
Droit – Économie – Sciences sociales
Année universitaire 2019-2020

Master 2 Sécurité et défense

INTELLIGENCE ARTIFICIELLE ET OPÉRATIONS DE MAINTIEN DE L'ORDRE :

Enjeux et perspectives d'une rupture technologique

Mémoire préparé sous la direction
du Général d'armée (2S) Marc WATIN-AUGOUARD

présenté et soutenu à distance
pour l'obtention du Master 2 Droit public, parcours Sécurité et défense

par

Aurélien BEAUGRAND

Lauréat du prix de mémoire recherche et réflexion stratégique
de la Gendarmerie nationale 2021

INTELLIGENCE ARTIFICIELLE ET OPÉRATIONS DE MAINTIEN DE L'ORDRE :

Enjeux et perspectives d'une rupture technologique

L'Université n'entend donner aucune approbation ni improbation aux opinions émises dans le mémoire ; ces opinions doivent être considérées comme propres à leur auteur.

RÉSUMÉ / *ABSTRACT*

Alors que les développements actuels en matière d'intelligence artificielle peuvent faire craindre un avenir à la *« Minority Report »*, il devient urgent de discuter de ses enjeux appliqués aux opérations de maintien de l'ordre. Qualifiée de technologie de rupture, l'IA apparaît comme un outil stratégique d'aide à la décision qui, par sa capacité de traitement et d'analyse massive des données en temps réel, permettra d'anticiper les situations à risque.

Entre utopie sécuritaire et protection absolue des libertés, le recours à l'IA dans les opérations de gestion des foules nécessite une réflexion pluridisciplinaire axée sur deux impératifs démocratiques : l'acceptabilité et la responsabilité. Il est donc indispensable de définir une stratégie globale associant décideurs politiques, juristes, citoyens, entrepreneurs et praticiens du maintien de l'ordre, en vue de garantir une IA à la fois opérationnelle et éthique.

Face au durcissement des manifestations et à leur infiltration par des groupes violents, l'intelligence artificielle devra être robuste par conception. Elle pourrait ainsi amorcer une révolution dans la pratique du maintien de l'ordre, pour une meilleure expression collective et pacifique des idées et des opinions.

While current developments in artificial intelligence may raise fears of a 'Minority Report' future, it has become urgent to discuss these issues as they apply to law enforcement operations. Often understood as a disruptive technology, AI promises to be a strategic decision-making tool which, through its capacity for massive data processing and real-time analysis, will make it possible to better anticipate risk.

Navigating between a securitarian utopia and absolute protection of liberties, the use of AI in crowd management operations requires multidisciplinary thinking focused on two democratic imperatives: acceptability and liability. It is therefore essential to define a comprehensive strategy involving decision-makers, lawyers, citizens, entrepreneurs, and law enforcement practitioners, in order to guarantee a use of AI that is both operational and ethical.

As protests harden and become infiltrated by violent groups, artificial intelligence will need to be robust in its design. It could thus initiate a revolution in the practice of order maintenance, to better enable the collective and peaceful expression of ideas and opinions.

TABLE DES ABRÉVIATIONS

AAI : Autorité administrative indépendante
ALICE : *Automatic Labelling for Image Collections Exploration*
BAC : Brigade anti-criminalité
BATX : *Baidu, Alibaba, Tencent, Xiaomi*

CASS : Cour de cassation
CE : Conseil d'État
CEDH : Cour européenne des droits de l'Homme
CHEMI : Centre des hautes études du ministère de l'Intérieur
CNCTR : Commission nationale de contrôle des techniques de renseignement
CNEFG : Centre d'entraînement des forces de gendarmerie
CNIL : Commission nationale de l'informatique et des libertés
CREOGN : Centre de recherche de l'École des officiers de la gendarmerie nationale
CRS : Compagnie républicaine de sécurité
CSI : Code de la sécurité intérieure
CSI : Compagnie de sécurisation et d'intervention

DARPA : *Defense Advanced Research Projects Agency*
DDHC : Déclaration des droits de l'Homme et du Citoyens
DINSIN : Direction interministérielle du numérique et du système d'information et de communication

EGM : Escadron de gendarmerie mobile
FED : Fonds européen de défense
GAFAMI : *Google, Apple, Facebook, Amazon, IBM*

IA : Intelligence artificielle
IMSI : *International Mobile Subscriber Identity*

LBD : Lanceur de balles de défense
LIL : Loi relative à l'informatique, aux fichiers et aux libertés
LOPS : Loi d'orientation et de programmation relative à la sécurité
LOPSI : Loi d'orientation et de programmation pour la sécurité intérieure
LOPPSI : Loi d'orientation et de programmation pour la performance de la sécurité intérieure

MRT : Méthode de raisonnement tactique
PI : Peloton d'intervention

R&D : Recherche et développement
RATP : Régie autonome des transports parisiens
RGPD : Règlement générale sur la protection des données
RGPP : Révision générale des politiques publiques

SNCF : Société nationale des chemins de fer français
SPI : Section de protection et d'intervention
UE : Union européenne

ZAD : Zone à défendre

SOMMAIRE

INTRODUCTION GÉNÉRALE

TITRE I – UNE TECHNOLOGIE À FORT POTENTIEL OPÉRATIONNEL

Chapitre 1 – Un outil stratégique valorisant l'action des forces de maintien de l'ordre

Chapitre 2 – Un cadre juridique à adapter aux modalités de mise en œuvre de l'intelligence artificielle

TITRE II – UN DÉVELOPPEMENT TECHNOLOGIQUE À ENCADRER

Chapitre 1 – Les prérequis structurants à une intelligence artificielle raisonnée du maintien de l'ordre

Chapitre 2 – Protéger des mésusages : les garanties juridictionnelles et non juridictionnelles

CONCLUSION GÉNÉRALE

INTRODUCTION GÉNÉRALE

À l'occasion d'une conférence, tenue en septembre 2017, réunissant des étudiants en nouvelles technologies, le président de la Fédération de Russie Vladimir Poutine affirmait que *« l'intelligence artificielle représente l'avenir non seulement de la Russie, mais de toute l'humanité »*. Puis d'ajouter que *« celui qui deviendra leader en ce domaine sera le maître du monde. Et il est fortement indésirable que quelqu'un obtienne un monopole dans ce domaine »*.

L'intelligence artificielle apparaît donc aujourd'hui comme un moteur de développement global, tant pour les États que pour les entreprises (Section 1). Pourtant, si les enjeux du maintien de l'ordre public et du développement de l'IA en France sont partagés et complémentaires (Section 3), leurs rapports sont complexifiés du fait de la contingence de leur définition (Section 2).

Section 1 – L'intelligence artificielle : un moteur de développement global

Cette préoccupation du gouvernant à l'égard de cette nouvelle technologie n'est pas une exception. Depuis de nombreuses années, les initiatives privées et publiques se sont multipliées en matière d'intelligence artificielle. Plus précisément, les États se sont vus pressés par les grandes entreprises technologiques et leurs avancées considérables en la matière. Dès 1997, l'entreprise américaine IBM a surpris le monde entier par la défaite infligée par son superordinateur, *Deep Blue*, au champion du monde en titre Garry Kasparov. Plus récemment en mars 2016, le programme informatique *AlphaGo* de l'entreprise britannique *Google Deep Mind* a remporté quatre victoires sur cinq parties jouées contre Lee Sedol, véritable célébrité coréenne du jeu de go et considéré comme le meilleur joueur mondial de la décennie. Ce faisant, la machine détrône un être humain à la première place du classement mondial, pour un jeu dont les combinaisons possibles sont supérieures au nombre d'atomes dans l'univers.

Si cette performance peut paraître bien éloignée de notre quotidien, l'intelligence artificielle n'en est pas pour autant étrangère. Les grandes entreprises américaines ont rapidement compris le potentiel démultiplicateur de l'IA dans le développement de leurs activités commerciales. Les fournisseurs de services en ligne emploient déjà des algorithmes pour améliorer notre quotidien. Les messageries électroniques filtrent les fameux « pourriels » en recourant à des algorithmes, parfois en licence libre, comme *TensorFlow*. Mieux encore, certaines proposent même des réponses-types, à l'image du logiciel *Smart Reply* de l'entreprise *Proxem*. Nos

réseaux sociaux favoris compilent l'ensemble de nos pages consultées afin de créer un fil d'actualité propre à chacun d'entre nous. Et les moteurs de recherche ne peuvent faire autrement que de recourir à l'IA pour indexer et hiérarchiser les résultats. Dans nos déplacements, les logiciels de navigation, qu'ils soient libres ou payants, identifient le meilleur chemin en fonction de nos centres d'intérêts, et sont en mesure d'adapter constamment l'itinéraire eu égard aux conditions de circulation en temps réel.

En outre, si ces applications semblent être purement désintéressées, et viser simplement notre « bien-être » (les applications médicales en termes de détection de cancer sont prometteuses), ce serait ignorer que ces géants de l'Internet scrute notre moindre signe d'intérêt pour tel ou tel élément qu'ils nous présentent. Jouant avec notre capacité d'attention sans cesse décroissante (elle était de 12 secondes en 2000 pour atteindre 8 secondes aujourd'hui), ces acteurs du marché cherchent à viser au plus juste en identifiant constamment nos besoins (le sont-ils réellement ?). Nos données sont inlassablement exploitées pour mieux nous connaître, et nous vendre toujours mieux, nous vendre toujours plus. C'est par ce même biais, et sous couvert d'une « meilleure expérience utilisateur », que des outils de traitement automatique du langage naturel ont fait irruption dans nos salons (*Siri* chez *Apple*, *Alexa* chez *Amazon*, *Google Home*), jusqu'à menacer notre intimité et violer notre vie privée.

Ainsi, selon une étude de l'entreprise américaine *Markets & Markets*, le marché de l'IA représenterait une valeur de 5,05 milliards de dollars pour 2020 (étude pré-crise Covid-19). Pour la banque d'investissement Bpifrance, les répercussions en termes d'emploi et de relations humaines pourraient être considérables. 16% des emplois seraient menacés dans le monde, et 85% des interactions avec les clients ne nécessiteraient plus d'intervention humaine. L'IA apparaît dès lors comme un outil de rentabilité.

Pourtant, devant cette fulgurance économique et malgré la publicité de plus en plus présente qui est faite à l'IA, elle n'est pas une nouveauté de ce millénaire. Dès les années 1950, une poignée d'ingénieurs s'activaient déjà dans l'ombre pour créer ce qui sera, sans aucun doute, *« l'enjeu du siècle »*[1]. Et les États économiquement avancés décèlent dans cette rupture technologique un potentiel de souveraineté. Leurs grandes administrations devinent un instrument de puissance, tant dans l'expédition de leurs affaires courantes que dans l'exercice de leurs missions régaliennes.

[1] Eric SADIN, *L'intelligence artificielle ou l'enjeu du siècle, anatomie d'un antihumanisme radical*, L'échappée, 2018

Néanmoins, si les applications commerciales semblent déjà toutes trouvées, l'intelligence artificielle est complexe dans son appréhension. Et, appliquée au domaine du maintien de l'ordre, l'émergence d'une doctrine est rendue difficile par la contingence de ces deux notions.

Section 2 – Des notions contingentes et évolutives

Intelligence artificielle et maintien de l'ordre sont deux notions en évolution. La première du fait de ses développements récents (A). La seconde, pourtant ancienne, est encore aujourd'hui source de débat et apparaît comme inachevée (B).

§1. L'intelligence artificielle : une technologie encore en construction

L'intelligence artificielle est une notion difficile à définir. Elle fait appel à un ensemble large de procédures techniques et de disciplines. L'expression même, « intelligence artificielle », est attribuée à John McCarthy, prononcée à l'été 1956 lors des conférences de Dartmouth. Avec Marvin Minsky, ces deux scientifiques américains sont connus pour être les pionniers de cette nouvelle technologie informatique. Le premier recevra d'ailleurs le prix Turing en 1971 pour ses travaux relatifs à ce domaine. Pour approcher la notion, Alan Turing propose dès 1950 dans sa publication *Computing machinery and intelligence* un test afin d'identifier le phénomène. À cette fin, il énonce le protocole suivant : mettre en individu en conversation avec un ordinateur caché de sa vue ; quand l'individu ne peut déterminer si l'agent conversationnel caché de sa vue est un homme ou un ordinateur, alors le logiciel qui équipe l'ordinateur valide le test. Aujourd'hui, ce genre de logiciel devient accessible au plus grand nombre, et permet à tout un chacun de réaliser son propre « hypertrucage » (*deepfake*). L'IA est désormais en mesure de créer de toute pièce un visage[2]. Pire encore, elle est capable de reproduire virtuellement le visage et l'expression faciale d'un homme politique, et d'y transposer un discours audio-visuel en temps réel.

Antoine Bordes, chercheur français employé par l'entreprise *Facebook*, soutient que l'intelligence artificielle est un *« ensemble de méthodes et d'outils développés afin de réaliser un ensemble de tâches de plus en plus complexes. On parle d'IA lorsque les tâches que l'on considérait uniquement réalisable par l'Homme le deviennent aujourd'hui par des machines »*.

[2] https://thispersondoesnotexist.com/

Le dictionnaire en ligne *Trésor de la langue française* donne quant à lui la définition suivante : *« Intelligence artificielle : recherche de moyens susceptibles de doter les systèmes informatiques de capacités intellectuelles comparables à celles des êtres humains »*. Aussi effrayant puisse paraître l'idée qu'une machine égale l'être humain, toute la nuance réside pour l'heure dans ce *« comparable »*. Car il faut dès maintenant distinguer l'IA dite « faible » de l'IA dite « forte ».

En effet, l'IA se fonde sur les sciences cognitives avec pour objectifs de reproduire et simuler la perception et le raisonnement humains. L'IA faible, qui nous intéressera à titre principal dans cette étude, tend à modéliser les idées abstraites pour ensuite les exploiter sous forme informatique : elle est programmée par l'Homme, qui la développe notamment par l'apprentissage statistique. L'IA forte serait capable d'écrire son propre code, donc potentiellement autonome. Cette IA forte s'inscrit depuis les années 2000 dans un débat sur la singularité, c'est-à-dire le moment à partir duquel la machine, consciente d'elle-même, développe ses propres normes. Elle devient un acteur à proprement parler, sorte de *« golem des temps modernes »*[3].

Tout l'enjeu d'une application de l'IA aux opérations de maintien de l'ordre réside donc dans la modélisation de l'ensemble du spectre de l'ordre public (du bon ordre au désordre). Ces modélisations ont lieu dans le cadre de méthodes dites d'apprentissage automatique (*machine learning*) et, à terme, d'apprentissage profond par réseaux de neurones artificiels (*deep learning*)[4]. Une intelligence artificielle est donc fondamentalement une combinaison d'un algorithme d'apprentissage, d'une puissance de calcul et d'une base de données. C'est à ce titre qu'intelligence artificielle et traitement massif des données (*big data*) sont liés : l'un est outil, l'autre le matériau.

[3] Joseph HENROTIN, « Les promesses de l'intelligence artificielle », *Le Collimateur*, IRSEM, 09/04/2019
[4] Voir Annexe III

§2. L'instabilité notionnelle du maintien de l'ordre

La notion d'ordre public en France est le fruit d'une lente construction juridique, encore aujourd'hui inachevée (A), dont les appellations diffèrent entre le juriste et le praticien (B).

A. Une construction historique de l'ordre public aujourd'hui inachevée

« L'ordre public est un hamac dans lequel il est permis de se balancer, mais sur lequel il est défendu de s'asseoir »

Charles Dumercy, *Paradoxes judiciaires*, 1899

L'ordre public est une notion qui irrigue le droit public français depuis plus de deux siècles. Qualifié de concept « à texture ouverte » en raison de la variété des éléments que l'on peut y intégrer, certains auteurs pensent que cette notion, au même titre que l'intérêt général, ne doit pas être définie. Pour le professeur Florian Poulet, *« ces notions doivent être contingentes et évolutives »* (…) *« pour les faire évoluer suivant la société »*[5]. Si donc aucune définition consensuelle ne saurait être formulée, on peut en trouver une énumération textuelle à l'article 73 de la Constitution de 1958, ou encore aux articles 10 de la Déclaration des droits de l'Homme et du Citoyen, et L2212-2 du code général des collectivités territoriales.

Au titre de ce dernier article, l'ordre public est caractérisé dans sa dimension municipale, et rassemble *« le bon ordre, la sûreté, la sécurité et la salubrité publiques »*. Il s'entend donc très largement. Appliqué à notre problématique des opérations de maintien de l'ordre, quelques dispositions de cet article nous intéressent particulièrement. On relèvera notamment *« ce qui intéresse la sûreté et la commodité du passage dans les rues, quais, places et voies publiques »*, *« les dépôts, déversements, déjections, projections de toute matière ou objet de nature à nuire, en quelque manière que ce soit, à la sûreté ou à la commodité du passage »*. Il est donc confié au maire un certain nombre de mission au nombre desquelles figurent notamment la répression des *« atteintes à la tranquillité publique telles que les rixes et disputes accompagnées d'ameutement dans les rues, le tumulte excité dans les lieux d'assemblée publique, les attroupements »*, et *« le maintien du bon ordre dans les endroits où il se fait de grands rassemblements d'hommes »*.

[5] Florian POULET, *Cours de politiques de sécurité publique*, Master 2 Sécurité et défense, 2019-2020

Cette notion fondamentale fait donc l'objet d'une conception extensive, à tel point que l'on a vu la juridiction administrative suprême l'étendre dans une dimension non plus seulement matérielle, mais également immatérielle. Le Conseil d'État a en effet ouvert l'ordre public à la dignité de la personne humaine[6]. Si le Conseil constitutionnel est lui-même venu consacrer cette dimension immatérielle – en reconnaissant les *« exigences minimales de la vie en société »* [7]–, elle n'entre pas dans le champ de la présente recherche. Pour autant, quel que soit sa dimension matérielle ou immatérielle, c'est en recourant au critère finaliste de l'ordre public que l'on identifie une mesure de police administrative. Cette dernière a en effet pour objet la prévention des atteintes et troubles à l'ordre public. Et c'est dans ce cadre qu'interviennent les opérations de maintien de l'ordre.

B. <u>De la sauvegarde de l'ordre public au maintien de l'ordre public</u>

Maintenir l'ordre public ne revêt pas la même signification du point de vue constitutionnel que du point de vue opérationnel.

Pour le Conseil constitutionnel, on constate qu'une dualité jurisprudentielle s'est installée dans son appréhension de l'ordre public. D'une part, il est un objet nécessaire à l'exercice des libertés. En témoignent les décisions de 1981 et 1985 dans lesquelles successivement le juge constitutionnel affirme que *« la prévention d'atteintes à l'ordre public, notamment d'atteintes à la sécurité des personnes et des biens »* est nécessaire *« à la mise en œuvre de principes et de droits ayant valeur constitutionnelle »*[8], puis ajoute que *« la conciliation nécessaire entre le respect des libertés et la sauvegarde de l'ordre public sans lequel l'exercice des libertés ne saurait être assuré »*[9]. D'autre part, il est également un moyen légitime de limitation de certaines libertés. Ce pendant négatif trouve son fondement dans l'obligation dégagée par le Conseil constitutionnel à partir du bloc de constitutionnalité à l'encontre du législateur, de concilier l'exercice des libertés avec l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public[10].

---

[6] Conseil d'État, assemblée, 27 octobre 1995, *Commune de Morsang-sur-Orge*, 136727
[7] Conseil constitutionnel, décision n°2010-613 DC du 07 octobre 2010, *Loi interdisant la dissimulation du visage dans l'espace public*
[8] Conseil constitutionnel, décision n°80-127 DC du 20 janvier 1981, *Loi renforçant la sécurité et protégeant la liberté des personnes*, cons. 56
[9] Conseil constitutionnel, décision n°85-187 DC du 25 janvier 1985, *Loi relative à l'état d'urgence en Nouvelle-Calédonie et dépendances*, cons. 3
[10] Conseil constitutionnel, décision n°82-141 DC du 27 juillet 1982, *Loi sur la communication audiovisuelle*

C'est donc avec un double objectif démocratique que le Conseil use de cette notion dans sa jurisprudence, à la fois moyen d'expression des libertés et motif de restriction. Ce faisant, le Conseil s'inscrit dans la lignée de la Cour européenne des droits de l'Homme pour qui des limitations à certains droits contenus dans la Convention sont toujours possibles si elles sont – selon la formule consacrée – *« nécessaires dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale »*.

Mais cette représentation juridique demeure bien éloignée de la réalité pratique du terrain. Et la définition municipale de la prévention des troubles à l'ordre public donne ici une illustration plus précise des conditions opérationnelles dans lesquelles sont employées les forces de l'ordre. Pour ajouter à celle-ci, le général de gendarmerie Bertrand Cavalier, auditionné devant la commission d'enquête présidée par le député Mamère en 2015, fait état que *« dans une acception large, le maintien de l'ordre est une fonction centrale destinée à garantir la cohésion de la Nation et la cohérence du corps social sur les fondements de nos valeurs communes. Il doit notamment permettre de régler les contentieux de façon négociée plutôt que par la violence »*[11].

Traditionnellement, la gestion des foules par les forces de l'ordre en France s'est d'abord construite sur un modèle de rétablissement de l'ordre. Pour l'historien Fabien Cardoni, le tournant du maintien de l'ordre en France se situe au XX^{ème} siècle. Jusqu'alors, ces opérations visaient à *« empêcher que la rue ne devienne une tribune, un forum et un acteur de la vie politique »*[12]. Les autorités publiques visaient avant tout la stabilisation du régime, face aux menées révolutionnaires qui essaimaient un peu partout. Le maintien de l'ordre que l'on connaît aujourd'hui naîtra dans les grandes manifestations sociales du début du XX^{ème}, pour devenir à l'aube du millénaire *« un point d'équilibre entre le désordre acceptable et l'ordre nécessaire »*[13]. Ces opérations de maintien de l'ordre concernent évidemment les grandes manifestations humaines à risques. Il ne s'agit pas des missions courantes de protection des populations, assurées quotidiennement par les forces de l'ordre dans le cadre de leurs patrouilles de sécurité publique.

[11] M. Pascal POPELIN, « Rapport d'enquête sur les missions et modalités du maintien de l'ordre républicain dans un contexte de respect des libertés publiques et du droit de manifestation », XIV^{ème} législature, 21 mai 2015, n°2794, p. 47
[12] Fabien CARDONI, *La garde républicaine d'une République à l'autre (1848-1871)*, PUR, 2008, p.211-256
[13] Philippe MASSONI, « Défense des libertés et ordre public à Paris », *Administration*, 1996, n°173, p. 55

L'intelligence artificielle se présente ainsi comme un outil d'optimisation des activités de maintien de l'ordre en manifestations. Il convient néanmoins de questionner son fonctionnement au regard de la protection des données personnelles, et contrôler les conséquences de son usage sur la vie privée du citoyen dans son expression sur la voie publique. Elle s'intègre dans le champ plus large de la police prédictive, outil d'aide à la décision, utilisée dans le cadre de la modernisation de l'action publique.

Section 3 – Enjeux partagés et complémentaires par l'IA et le maintien de l'ordre public

L'intelligence artificielle présente des enjeux tant au niveau international qu'au niveau national pour les États. À l'extérieur, la maîtrise de cette technologie en fait pour certains observateurs un indicateur de puissance[14]. Par les moyens humains et financiers que les États consentent à son développement et le haut niveau d'expertise nécessaire à sa conception, l'IA est un moyen de réaffirmer leur puissance face à des opérateurs économiques qui les concurrencent de manière croissante. À l'intérieur, les efforts en matière de modernisation de l'action publique font de l'IA un moteur d'optimisation des coûts de fonctionnements des administrations. Seulement, les défenseurs des libertés y voient également un moyen de confiscation du pouvoir, aussi bien par les autorités publiques que par l'outil en lui-même. Le niveau de connaissance nécessaire à sa compréhension semble l'éloigner du citoyen. L'IA fait donc partie, au même titre que l'informatique, de ces technologies dont les applications se sont démocratisées, sans que leur essence ne soit nécessairement démocratique. Or, c'est à la conception de l'outil que l'on en détermine les caractéristiques, donc sa conformité avec les usages que l'on en fera.

Face à l'avance des acteurs privés, et le regard tourné vers des applications d'intérêt national, les États se sont tardivement intéressés à l'IA. Animés par le double objectif de soutenir une économie nationale de pointe et conserver, voire rattraper, un retard souverain en la matière, ceux-ci ont rapidement saisi l'enjeu à long terme de l'IA. Il s'agit là bien plus d'une rupture que d'une simple mise à jour technologique, tant les réflexions quant à leur utilisation émergent au fil des mois. Les champs de la défense, de la sécurité et de la justice se sont ainsi rapidement intéressés aux nouvelles potentialités offertes par l'IA. Les premiers essais techniques se sont révélés plus ou moins fructueux. Les succès les plus immédiats ont eu lieu en matière de

[14] Cédric ABRIAT, « L'intelligence artificielle, nouvel indicateur de puissance ? », *Défense et sécurité internationale*, juillet-août 2019

maintien en conditions opérationnelles des matériels : grâce aux outils de maintenance prédictive développés par les industriels, les armées françaises ont anticipées des flux logistiques pour changer des pièces sur des matériels déployés en opérations extérieures. L'IA apparaît ici comme une solution de rationalisation des coûts. Mais ses promesses n'ont pas été tenues en matière d'assistance aux magistrats, au cours des essais qui se sont tenus dans les cours d'appel de Rennes et Douai en 2017. Il sera encore nécessaire d'améliorer le logiciel avant d'en tirer tous les bénéfices.

Matériellement parlant, il existe donc des matières dans lesquelles il est plus compliqué de modéliser les paramètres : le maintien du bon ordre en manifestation en est un. C'est par l'analyse fine d'une quantité immense de données enregistrées à l'occasion d'opérations de maintien de l'ordre que l'outil se façonnera. Des enjeux en termes de collecte, traitement et stockage de données recueillies sur la voie publique apparaissent donc, et laissent entrevoir une concurrence, déjà ancienne, de l'État par le secteur privé dans le développement de ces outils. Cette concurrence repose notamment sur des considérations économiques, mais aussi sur des considérations en matière de ressources humaines car l'État peine à recruter et fidéliser des spécialistes. Face à la puissance des universités et des grandes entreprises américaines et chinoises, l'IA nous permet d'entrevoir de nouvelles synergies. Car la France partage des intérêts communs avec ses partenaires européens en matière de sécurité et de justice. La création d'un Espace européen de sécurité, de liberté et de justice en est un des marqueurs forts, aboutissement – certes encore imparfait – d'une *« union sans cesse plus étroite »*[15].

Néanmoins, avant d'engager un dialogue approfondi, il faut déjà bien analyser les enjeux internes, c'est-à-dire ceux que nous identifions comme souverains. A cet égard, l'exécutif français a commandé, dès l'automne 2017, un rapport sur l'IA sous la direction du député et mathématicien Cédric Villani[16]. Dans son focus sur la sécurité et la défense, le rapport insiste sur le fait que la création d'une IA nationale devra, dès sa conception, intégrer le risque d'une *« itarisation »*[17]. Il s'agit avant tout d'éviter une préemption juridique américaine sur le développement d'une technologie, dont l'un des composants serait lui-même américain. Un tel abandon total de souveraineté ne serait pas permis, surtout au regard d'enjeux en matières de

[15] Article premier du traité sur l'Union européenne
[16] Cédric Villani, *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*, 2018
[17] *ITAR* ou *International Traffic in Arms Regulations* est une norme réglementaire d'application extraterritoriale, mise en place par les États-Unis d'Amérique, en vue de contrôler toute importation ou exportation d'un matériel lié à la défense. Elle fonctionne de manière rétroactive sur tout produit dont au moins l'un des composants de la chaîne de production a un lien avec les États-Unis.

libertés publiques inhérent à un tel outil régalien. Mais rien ne s'oppose *a priori* à un partage de souveraineté dans un cadre multilatéral, comme le propose l'Union européenne.

Au regard de ces éléments, l'IA marque donc une rupture technologique et ouvre la voie à ce que le rapport Villani appelle les *« imaginaires »*[18]. Ces derniers guideraient, implicitement mais réellement, le développement de l'IA. Les auteurs de science-fiction, dont les romans d'anticipation ne cessent de nourrir la recherche scientifique, en sont les pionniers, encouragés par les producteurs de l'industrie cinématographique. On citera notamment *1984* de George Orwell, *Minority Report* de Philipp K. Dick, ou encore *Equilibrium* de Kurt Wimmer. Entre opportunités réelles et dystopies, l'IA émerveille ainsi tout autant qu'elle fait craindre à certains le pire.

C'est dans ce contexte clivant, voire anxiogène (65% des Français considèrent l'IA comme une menace pour l'humanité, selon une étude commandée par Bpifrance), qu'il convient d'étudier les rapports entre intelligence artificielle et opérations de maintien de l'ordre public.

Il s'agira donc de déterminer comment l'intelligence artificielle doit être pensée et construite en matière d'opérations de maintien de l'ordre, en vue de garantie leur efficacité tout en conciliant leur réussite avec le respect des libertés individuelles et collectives. Il s'agira également d'en mesurer les implications éthiques, juridiques, opérationnelles et humaines au regard des potentialités techniques.

Dans un premier titre, nous nous concentrerons le potentiel opérationnel qu'ouvre l'intelligence artificielle au service du maintien de l'ordre. Avant de considérer les modalités de son encadrement dans un second titre.

[18] Cédric VILLANI, *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*, 2018, p. 9

TITRE I – UNE TECHNOLOGIE À FORT POTENTIEL OPÉRATIONNEL

L'intelligence artificielle se présente comme une technologie de rupture dans le domaine du maintien de l'ordre. Aucun processus réel d'autonomisation n'existe pour l'heure dans le processus de planification et de conduite des opérations.

L'intelligence artificielle du maintien de l'ordre renouvelle les approches tant stratégique, qu'opérative ou encore économique. Elle s'invite dans les postes de commandement comme un outil stratégique d'aide à la décision qui, par sa capacité de traitement et d'analyse massive des données, permettra d'anticiper les situations à risque. Cette capacité de traitement inégalable amène à repenser l'organisation des ressources humaines aux fins d'assurer l'efficacité de cette nouvelle donne opérationnelle.

Par sa finesse d'analyse, elle se veut être un outil au service du déploiement d'un juste niveau de force, donc d'une dissuasion perfectionnée. En cela, l'IA du maintien de l'ordre se propose de révolutionner la gestion traditionnelle des foules.

L'IA se présente donc comme un outil stratégique de valorisation de l'action des forces de maintien de l'ordre (Chapitre 1). Néanmoins, la réussite d'une mise en œuvre durable de celle-ci nécessitera d'adapter et d'ajuster le cadre juridique aux capacités opérationnelles qu'elle apporte (Chapitre 2).

Chapitre 1 – UN OUTIL STRATÉGIQUE VALORISANT L'ACTION DES FORCES DE MAINTIEN DE L'ORDRE

L'engagement des forces de l'ordre dans ce type d'opérations vise à maintenir un ordre déjà établi. En cela, l'intelligence artificielle en manifestation se devra d'être un outil au service de la préservation et de l'expression des libertés publiques (Section 1). Grâce à sa finesse d'analyse, elle affinera la prise de décision opérationnelle. Ce qui nous amène à nous questionner sur un éventuel renouveau du maintien de l'ordre, et sa « déthéâtralisation » (Section 2). Enfin, le développement de cette technologie nécessite une stratégie nationale industrielle et de ressources humaines (Section 3).

Section 1 – Un outil stratégique en matière de préservation et d'expression des libertés publiques

Le maintien de l'ordre en France se fonde sur un équilibre entre liberté de manifester et ordre républicain. Trois piliers distincts ancrent la réflexion des parlementaires de la commission Mamère, et des experts qu'ils ont convoqués. Nous étudierons successivement l'exercice de la liberté de manifester, la garantie apportée à la préservation de l'ordre public et la spécialisation des forces formées à cet effet, au prisme des potentialités offertes par l'intelligence artificielle.

§1. L'intelligence artificielle au service de la liberté de manifester

Par la rupture technologique que représente en elle-même l'intelligence artificielle, elle bouscule l'approche traditionnelle et renouvelle l'appréhension même du maintien de l'ordre (B), au service d'une analyse dépassionnée des conditions d'exercice d'une liberté constitutionnellement garantie (A).

A. Une liberté constitutionnellement garantie

Avant d'entrer un peu plus dans le détail des opportunités ouvertes par l'intelligence artificielle, il convient de définir cette liberté, fondamentale pour toute démocratie affirmée.

Premier constat, la liberté de manifester n'est pas, en tant que telle, une liberté constitutionnelle. Réglementée par un décret-loi de 1935[19], c'est le pouvoir exécutif qui en a fixé les modalités d'encadrement, sans pour autant la définir. Désormais codifiée dans le code de la sécurité intérieure pour ce qui est de son régime, la liberté de manifester pourrait constituer, aux yeux de certains auteurs, un principe fondamental reconnu par les lois de la République. Il aura fallu attendre la décision LOPS du Conseil constitutionnel en 1995 pour qu'une timide protection constitutionnelle lui soit accordée en tant que *« droit d'expression collective des idées et des opinions »* [20]. Le Conseil ne lui aura pas donné expressément de fondement, mais des auteurs[21] identifient une correspondance avec l'article 10 de la Déclaration des droits de l'Homme et du citoyen. Ce n'est qu'à la suite de l'examen de la loi dite « anti-casseurs » qu'il lui sera donné une assise constitutionnelle en la faisant découler, cette fois-ci, de l'article 11 de la DDHC. Ce faisant, les sages de la rue Montpensier décrivent son exercice comme une *« condition de la démocratie, et l'une des garanties du respect des autres droits et libertés »*[22].

C'est finalement la chambre criminelle de la Cour de cassation qui en a explicité le plus clairement sa définition, qualifiant la manifestation de *« tout rassemblement, statique ou mobile, sur la voie publique d'un groupe organisé de personnes aux fins d'exprimer collectivement et publiquement une opinion ou une volonté commune »*[23].

B. Une approche renouvelée pour le décideur

L'intégration de la technique a toujours eu pour objet, quel que soit le domaine, d'éclairer le décideur. Appliqué au maintien de l'ordre, le déploiement progressif de moyen de vidéoprotection[24] à partir du milieu des années 1990 a ainsi permis aux pouvoirs publics d'être informés, en temps réel, de l'évolution des opérations de gestion de foules. Puis, par le développement des capteurs télévisuels de plus en plus perfectionnés (caméras embarquées sur des véhicules, hélicoptères, drones, caméras-piétons) et leur fusion instantanées dans les centres de commandements, ces mêmes pouvoirs publics ont vu s'affiner leur perception de la situation.

[19] Décret-loi *(abrogé)* du 23 octobre 1935 portant réglementation des mesures relatives au renforcement du maintien de l'ordre public
[20] Conseil constitutionnel, décision n°94-352 DC du 18 janvier 1995, Loi d'orientation et de programmation relative à la sécurité, cons. 16
[21] Voir notamment Étienne PICARD, *JCP G*, 1995, I. 155
[22] Conseil constitutionnel, décision n°2019-780 DC du 04 avril 2019, *Loi visant à renforcer et garantir le maintien de l'ordre public lors des manifestations*, cons. 8
[23] Cour de cassation, chambre criminelle, 09 février 2016, 14-82.234, bull.
[24] Voir not. la loi n°95-73 du 21 janvier 1995 *(modifiée)* d'orientation et de programmation relative à la sécurité

Néanmoins, il est bien question de perception, car le décideur ne visionne que ce qui lui est donné à voir. Deux écueils le guettent donc.

En premier lieu, il risque de subir une tunnelisation de l'information : l'image a le propre de fonctionner comme une dictature. Elle ne donne pas de choix, et fonctionne sur le principe de la persuasion. C'est finalement l'ouverture du champ focal qui lui apporte plus ou moins d'objectivité. À titre d'exemple on peut citer cette célèbre caricature[25] –non attribuée– parue lors de la campagne présidentielle américaine de 1988, montrant l'importance de la perspective et de la distorsion avec la réalité, entre le cadre de la caméra et la réalité de la scène entière. Elle trouve une illustration constante dans l'actualité, notamment à l'occasion de publications de vidéos montrant des violences, par ou à l'encontre de forces de l'ordre, lors de manifestations. Là encore, la perspective et le déroulé global des scènes sont importants, car seule l'analyse approfondie de l'ensemble des faits détermine la légalité ou non de l'emploi de la force. On citera, en exemple, la scène du dégainé par le policier de son arme de service alors qu'il était pris à partie par des manifestants lors de l'acte VI du mouvement des Gilets Jaunes.

En second lieu, la multiplication des capteurs peut amener le destinataire à une surcharge informationnelle. Et, en l'absence de moyens humains suffisants pour contrôler et analyser les images captées, le décideur s'expose à une « asphyxie », une noyade sous le flot continu et en temps réel des images. Dans un entretien accordé au journal en ligne la République des lettres[26], l'essayiste Paul Virilio soulignait que *« la surinformation était une autre manière, plus efficace encore que la censure, d'asphyxier l'opinion publique »*. C'est exactement le risque auquel toute personne en situation de responsabilité est aujourd'hui confrontée, avec pour conséquence finale d'affecter la qualité des prises de décisions opérationnelles.

Par son approche globale et dépassionnée, l'IA révolutionne donc non seulement la technique, mais aussi l'approche intellectuelle avec laquelle les décideurs pourraient appréhender les nouvelles opérations de maintien de l'ordre. L'IA fonctionne comme une mécanique froide et implacable, à laquelle plus il sera donné à voir, plus pertinente sera la finesse d'analyse. Le paradigme du traitement de la donnée est donc renversé, au profit d'une approche qui ne renie pas la qualité au profit de la quantité de charge informationnelle.

[25] Voir Annexe I
[26] La République des lettres, republique-des-lettres.fr/190-paul-virilio.php

Finalement, la technique repousse la notion de surcharge à une dimension purement matérielle. Il n'y a pas de risque à ce que la machine se « fatigue ». Car ce sont bien les capacités d'attention et de concentration qui sont les failles premières de l'humain. Et celles-là mêmes peuvent conduire à ignorer certains signaux faibles d'une part, et ne pas les corréler d'autre part. Par une capacité conjointe de traitement massif de l'information et de sélection de l'information pertinente, l'IA permet donc de prévenir le risque d'une possible double erreur du décideur. Il s'agit bien là d'une rupture technologique. L'outil d'intelligence artificielle permet ainsi une constance et une certaine fiabilité dans l'analyse dépassionnée des faits qui lui sont soumis. En cela, l'IA ajoute une garantie, certes implicite, mais ô combien réelle, à l'exercice de la liberté de manifester.

§2. Une garantie supplémentaire à la préservation de l'ordre public

L'intelligence artificielle s'inscrira, quoi qu'il advienne, dans le régime actuel de la déclaration préalable des manifestations. Si elle pourra faciliter l'application de ce régime (A), elle sera indéniablement un atout dans l'anticipation stratégique et la préparation opérationnelle (B).

A. Le régime actuel de déclaration : préalable à un exercice apaisé de la liberté de manifester

Curieusement, le régime ne se trouve pas dans une loi sur la liberté de manifester, mais dans le code de la sécurité intérieure, et plus précisément dans le livre II chapitre premier intitulé « Prévention des atteintes à l'ordre public lors de manifestations et de rassemblements » (Art. L211-1 et suivants du code de la sécurité intérieure). Pour certains auteurs[27], cette perspective sécuritaire serait liée à la dangerosité potentielle de l'exercice de cette liberté, et des conséquences graves et immédiates de son dévoiement (blessures graves et/ou mortelles, dégradations et destructions de biens meubles et immeubles). À cet égard, il est prévu un régime plus restrictif pour la manifestation que pour d'autres libertés publiques telles que la réunion, ce qui tient en premier, avant le risque de trouble à l'ordre public, à son exercice sur la voie public. Il faut néanmoins tout de suite nuancer ce propos car l'article L211-1 prévoit une *« obligation de déclaration préalable »* et non une obligation d'autorisation, mesure qui serait

[27] Voir notamment Olivier LE BOT, « La liberté de manifestation en France : un droit fondamental sur la sellette ? », *La liberté de manifester et ses limites : perspective de droit comparé*, Actes du colloque des 18 et 19 mars 2016

encore plus restrictive des libertés. Il est donc exigé des organisateurs une formalité administrative préalable à l'exercice de cette liberté, qui repose en pratique sur une information des autorités publiques au moins 72 heures avant la déambulation. Dans la pratique, les autorités municipales en sont régulièrement les dépositaires, et communiquent obligatoirement cette déclaration au préfet, qui pourra l'interdire dans les 24 heures précédant la manifestation. En l'absence d'une telle interdiction, le maire de la commune pourra toujours prendre un arrêté s'il a des éléments objectifs laissant penser que cette manifestation est de nature à troubler l'ordre public.

L'exercice de la liberté de manifester fait donc l'objet d'une négociation entre les autorités et les organisateurs. Et ce jeu de dialogue permet en pratique de discuter des modalités de cheminement, de dispersion en cas de contre-manifestations annoncées, ou d'une menace ponctuelle particulièrement grave d'atteinte à l'ordre public (risque terroriste avéré). Car il est rare que les organisateurs se voient interdits de manifester. Mais pour que ce dialogue ait lieu, encore faut-il qu'une telle déclaration ait préalablement existé. Le rapport Popelin[28] relatif à l'exercice des missions de maintien de l'ordre souligne à ce titre la difficulté croissante à apporter une réponse opérationnelle à l'augmentation des manifestations non-déclarées.

Au demeurant, une manifestation qui n'a pas été déclarée n'est pas en elle-même illégale. En effet, deux tempéraments sont à apporter ici. Le premier tempérament –légal– est celui des *« sorties sur la voie publique conformes aux usages locaux »*. Cette exception, prévue par le même article L211-1 du code de la sécurité intérieure, renvoie notamment aux processions religieuses, défilés à caractère festif et aux manifestations mémorielles. Le second tempérament est celui des cortèges n'ayant pas encore qualité d'attroupements. Il concerne les manifestations qui n'ont pas été déclarées, ou les manifestations interdites, pour lesquelles les forces de l'ordre n'ont pas encore ordonné la dispersion. Le professeur Le Bot estime ainsi que ce dernier tempérament est le fruit d'un risque de trouble plus important encore pour l'ordre public que celui résultant du non-respect de la loi. Il considère ainsi que cette pratique de non-dispersion immédiate est *« incontestablement un signe de libéralisme, que l'autorité publique laisse se dérouler ces rassemblements qui, de fait, ne se trouvent même pas soumis à l'exigence d'une déclaration mais relèvent du régime d'exercice des libertés le plus favorable, à savoir le régime répressif : la liberté s'exerce sans autorisation ni même déclaration »*[29].

[28] M. Pascal POPELIN, Rapport d'enquête sur les missions et modalités du maintien de l'ordre républicain dans un contexte de respect des libertés publiques et du droit de manifestation, n°2794, XIV[ème] législature, 21 mai 2015
[29] *Op. cit.* note 27, p. 21

Les récents mouvements « Gilets Jaunes » ont néanmoins légèrement changé la donne dans la marge de liberté octroyée par la puissance publique aux manifestations interdites. Et par ailleurs, on peut se questionner sur l'existence d'une décision d'acceptation implicite de l'autorité préfectorale, en matière de manifestation non-déclarée, en l'absence d'ordre de dispersion. Mais il est certain que l'intelligence artificielle jouera un rôle décisif dans le conseil aux autorités. Elle pourrait renforcer cette conception libérale par les analyses fines qu'elle tirera de l'environnement des manifestations annoncées et des données en accès libre.

B. L'intelligence artificielle : un atout dans l'anticipation stratégique et la préparation opérationnelle

Le régime de la déclaration préalable permet donc, par la temporalité qu'il impose, de laisser un temps de réflexion et d'analyse à la puissance publique. Ce délai est porté tout à la fois au bénéfice du préfet, que du ou des maires des communes sur le territoire desquelles la manifestation aura lieu. Si ces derniers ont d'ordinaire une bien meilleure connaissance de leur commune que le préfet, c'est bien ce dernier qui, par les moyens spécialisés dont il dispose, semble plus en mesure d'appréhender finement l'étendue d'éventuelles menaces qui pourraient surgir du dehors des communes. Il n'en demeure pas moins que rien n'empêche le maire, tout au contraire lui permet, de prendre des mesures plus restrictives que celles du préfet sur le territoire de sa commune, en vertu de ses pouvoirs de police administrative générale.

Si l'IA n'a pas vocation à remplacer les conseils ordinaires du préfet, elle pourrait dès à présent faciliter leur travail. À l'heure actuelle, ce conseil est fourni –pour la préfecture– par les services de police et de gendarmerie déployés dans les départements. On citera en particulier les services déconcentrés du renseignement territorial (ex-Renseignements généraux) qui sont en charge principale *« de la recherche, de la centralisation et de l'analyse des renseignements destinés à informer le Gouvernement et les représentants de l'État dans les collectivités territoriales de la République »* (…) *« dans tous les domaines susceptibles d'intéresser l'ordre public, notamment les phénomènes de violence »*[30]. Ces services particuliers pourraient alors voir leur capacité de travail démultipliée, dans l'aspect numérique tout au moins, par le recours au traitement algorithmique des données. Il est nécessaire ici de s'attarder sur la technique pour ouvrir le champ des possibles en matière d'anticipation.

[30] Article 21, Décret n°2013-728 du 12 août 2013 portant organisation de l'administration centrale du ministère de l'Intérieur et du ministère des Outre-mer

L'intelligence artificielle présente deux applications fonctionnelles particulièrement intéressantes pour le décideur. La première est la détection d'anomalies, qui permet à son utilisateur d'identifier des éléments dont les caractéristiques sortent de l'ordinaire, c'est-à-dire sortent de ce qui est commun à l'univers des éléments présentés à la machine. La seconde est l'aide à la décision, qui consiste à suggérer à l'utilisateur des actions, en fonction des paramètres de cet univers et des effets recherchés par le décideur sur celui-ci. Or, en permettant à un algorithme d'IA de traiter la masse considérable des données en libre accès sur Internet, les services en charge de la sécurité publique décuplent leur capacité d'analyse. Il ne s'agit pas de lancer un contrôle généralisé et systématique du flux Internet et de violer la vie privée des gens, mais d'exploiter en détail les données numériques rendues publiques afin de les corréler. On en dégage ainsi des grandes tendances qui permettront dans un premier temps d'affiner la connaissance des problèmes l'opinion publique, puis de nourrir la réflexion du décideur quant aux dispositifs à adopter en cas de manifestations. L'intérêt évident de cet usage, en matière de préservation de l'ordre public, est de faire ressortir les intentions de manifester. Deux corollaires peuvent en être déduits, l'un au service de la liberté de manifester, l'autre au bénéfice de la sauvegarde de l'ordre public.

En favorisant l'exploitation par l'IA des données numériques en libre accès, la puissance publique anticiperait au mieux les grands mouvements de populations, et s'assurerait d'une meilleure compréhension de l'opinion publique. En termes de gestion, l'IA permettrait ainsi à la puissance publique de mieux adapter les dispositifs policiers aux enjeux portés par telle ou telle manifestation à l'égard de la sauvegarde de l'ordre public. L'IA serait alors une garantie supplémentaire tant à la préservation de la paix publique, qu'au respect d'un déploiement nécessaire et proportionné de forces de l'ordre, ou qu'à la maîtrise de la dépense publique en résultant.

Il est à cet endroit des questions qui restent ouverte. L'intelligence artificielle aurait-elle pu « prédire » le mouvement des Gilets Jaunes, par l'analyse des données en libre accès sur les réseaux sociaux ? L'intelligence artificielle pourrait-elle aider la puissance publique à détecter par avance les manifestations qui ne ferait pas l'objet d'une déclaration ? *A contrario*, par sa capacité de traitement des données en temps réel, permettrait-elle de réduire les délais de déclaration ? Et, par un achèvement de ce mouvement, permettrait de réduire le nombre de manifestations non-déclarées ?

Le maintien de l'ordre en France fait aujourd'hui face à une mutation. Réels miroirs d'une société contrariée, les manifestations subissent des évolutions tant structurelles que conjoncturelles. Les conditions des troubles à l'ordre public ont évolué, et trois facteurs aggravants relevés par le rapport Popelin conduisent les forces de l'ordre à s'adapter.

En premier lieu, on constate une recomposition des acteurs principaux des manifestations tant que côté des forces de l'ordre que des manifestants. L'émergence de mouvements spontanés nés sur les réseaux sociaux prive la puissance publique d'interlocuteurs parmi les manifestants, ce qui pourtant à la base d'une préservation conjointe des libertés et de la paix publiques. Le lien et la confiance tissées depuis des années entre organisateurs et forces de l'ordre avait amené à une pacification des cortèges traditionnels (1er-Mai, défilés syndicaux). Mais depuis quelques années des infiltrations dans ces cortèges, notamment par des groupes structurés de casseurs de types *Black bloc*, ont conduit à une remise en question de la gestion des opérations de maintien de l'ordre. Ces individus encagoulés, tout de noir vêtus et issus pour la plupart des mouvements anarcho-libertaires, s'introduisent dans les manifestations avec la ferme intention de se confronter physiquement aux forces de l'ordre et de détruire tous les symboles de l'État et/ou du capitalisme (franchises internationales, banques, assurances). Ce constat n'est que la conséquence logique d'une part sans cesse décroissante des services d'ordre internes dans l'organisation des manifestations en France. Il en découle une moins bonne connaissance des acteurs en présence, et une dégradation logique de la concertation préalable à la manifestation entre ceux-ci. En parallèle de ce mouvement, les forces de police ont également à faire face à leurs propres dilemmes. La révision générale des politiques publiques a conduit à une nette diminution des effectifs de forces mobiles : la gendarmerie nationale a ainsi vu 15 de ses 123 escadrons de gendarmerie mobile être dissous. Dans les compagnies républicaines de sécurité, le nombre de personnels mobilisables sur le terrain est passé de 90-100 fonctionnaires à 70-80 fonctionnaires[31]. Cependant, les contestations n'ont pas diminué, ni en nombre, ni en volume ; et c'est ainsi que le très fort engagement des forces mobiles (chaque escadron de gendarmerie est déployé au moins 220 jours par an !) a conduit la puissance publique à revoir son dispositif. Pour continuer à garantir un niveau de présence opérationnelle et permettre d'assurer une formation continue minimale des effectifs mobiles, il a donc fallu recourir à des unités non spécialisées dans le maintien de l'ordre, au rang desquelles figurent notamment dans les grandes

[31] Audition de M. Éric MILDENBERGER, délégué général d'Alliance police nationale, devant la commission d'enquête sur les missions et modalités du maintien de l'ordre républicain dans un contexte de respect des libertés publiques et du droit de manifestation, n°2794, XIVème législature, 21 mai 2015

villes pour la police nationale les brigades anti-criminalité et les compagnies de sécurisation et d'intervention.

En second lieu, de nouveaux terrains de contestations sociales sont apparus, ils ne sont plus l'apanage des pavés des grandes villes. Des territoires ruraux accueillent désormais des manifestations, au sein desquels l'action des forces de l'ordre est compliquée tant opérationnellement que juridiquement. Les terrains en pleine nature sur lesquels la puissance publique est amenée à intervenir sont aménagés et occupés par une population très différente des cortèges traditionnels. Et ce n'est pas tant l'ordre public qui est troublée que l'occupation illégale de terrains privés : zones à défendre de Notre-Dame-des Landes et de Sivens.

Enfin, on note l'assignation d'objectifs complémentaires aux forces de l'ordre, couplée à une médiatisation croissante de ces enjeux de sécurité publique. Le rapport Popelin évoque ainsi la nécessité pour les forces de l'ordre de protéger les professionnels du journalisme face à des manifestants qui entretienne une défiance de principe à l'endroit des médias traditionnels. Une banalisation de la violence à leur encontre serait même en train d'émerger, ce qui conduit la puissance publique à mobiliser des personnels pour assurer leur sécurité. Le rapport souligne à cet égard, outre la protection des personnes, l'obligation à laquelle serait tenue cette dernière en vertu de l'article 11 de la Déclaration des droits de l'Homme et du citoyen. Défendre les journalistes dans l'exercice de leurs fonctions résulterait d'une double exigence : la première d'une obligation de protection de la vie, la seconde d'une obligation constitutionnelle de libre communication des pensées et des opinions. Cette mission particulière de protection des journalistes complique donc encore plus la mise en œuvre délicate des opérations de maintien de l'ordre, à une époque où l'hyper connexion donne tout à voir, tout de suite à l'opinion publique. Ce qui conduit logiquement cette dernière à abaisser son seuil de tolérance à l'égard de la violence déployée par certains manifestants. Corollaire de cet abaissement du seuil, la sanction pénale a fait l'objet d'un regain d'intérêt ; mais elle nécessite des moyens opérationnels particuliers afin d'interpeler et extraire de la foule des individus auteurs de faits délictueux ou criminels. Cette répression active, adjointe à l'attention particulière portée sur la sécurité des journalistes, dans un contexte de forte médiatisation amènent subséquemment les forces de l'ordre à modifier la nature et la gestion de leurs opérations de maintien de l'ordre.

Il s'agit donc désormais de développer et comprendre les dispositifs opérationnels auxquels l'IA pourrait apporter un effet majeur, et peut-être renouveler la manière dont ces opérations

nécessitant un savoir-faire particulier sont menées. Par les solutions techniques qu'elle promet, l'IA pourrait très rapidement apparaître comme un atout sérieux et incontournable d'une opération de maintien de l'ordre réussie.

Section 2 – L'outil du renouveau du maintien de l'ordre achevant sa « déthéâtralisation » ?

Dans son dernier rapport sur le maintien de l'ordre au regard des règles de déontologie, le Défenseur des droits soulignait que *« depuis une dizaine d'années, les règles et codes traditionnels de cette « théâtralisation » du maintien de l'ordre sont en déclin et régulièrement mis en cause, en particulier dans la capitale »*[32]. Les déploiements de forces spécialisées contre les dérives qui peuvent avoir lieu lors de manifestations ne remplissent plus leur objectif performatif. La démonstration des attributs de la force ne suffirait plus à dissuader certaines foules dans leurs dérives hostiles. Cette situation ne résulterait pas uniquement d'une perte de confiance de la population envers les forces de l'ordre, mais également d'une perte de légitimité tout à la fois des institutions policières et des manifestants. En effet, ces derniers n'hésitent plus à exercer des violences à l'encontre des forces de l'ordre, des journalistes et même des organisateurs de ces manifestations. Et la médiatisation croissante des interventions conduit l'opinion publique à penser que les opérations de maintien de l'ordre sont de plus en plus violentes. Il semblerait donc que la représentation et les symboles n'aient plus la même force dissuasive qu'on leur donnait jusqu'alors. Cependant est-il encore nécessaire que l'État dissuade par l'exposition des signes de sa puissance ? Lui qui, selon l'expression consacrée, revendique le *« monopole de la violence physique légitime »* (*Monopol legitimer physischer Gewaltsamkeit*)[33] ne s'affaiblit-il pas plus en exposant ses attributs de force qu'en expliquant clairement les modes de fonctionnement?

Au regard des promesses utilitaristes de cette nouvelle technologie, l'IA semble tout aussi bien trouver application au service d'une consolidation de la doctrine de maintien de l'ordre actuelle (§1), qu'ouvrir la voie à un renouveau de celle-ci (§2) dans laquelle la dissuasion ne se fonde plus uniquement sur une démonstration de la force armée.

[32] Rapport du Défenseur des droits, « Le maintien de l'ordre au regard des règles de déontologie », déc. 2017, p. 7
[33] Max WEBER, *Le Savant et le Politique*, 1919

§1. D'une consolidation du cadre actuel…

La doctrine française de maintien de l'ordre repose actuellement sur trois piliers : l'usage de forces spécialisées, le maintien à distance dans une posture dissuasive et le recours à la force en situation d'absolue nécessité et de manière proportionnée. Concernant l'IA, son usage par des forces spécialisées apparaît comme une garantie de l'efficacité de son emploi (A). De plus, elle propose de dissuader autrement en changeant la perspective d'encadrement des foules (B). Enfin, elle s'avère être un outil favorable par conception à cette logique de recours absolument nécessaire et proportionné à la force (C).

A. Un usage de l'IA par les forces spécialisées, garantie d'une efficacité de son emploi

La police de gestion des foules a fait l'objet d'une réelle maturation à partir de la fin du XIX^{ème} siècle et des grandes grèves minières qui ont secoué la France et la Grande-Bretagne. Progressivement, le maintien de l'ordre a fait l'objet d'une institutionnalisation que certains ont qualifié de paramilitarisation des fonctions policières. Le britannique Tony Jefferson définit cette paramilitarisation comme *« l'application d'un entraînement, d'une philosophie et d'une organisation (quasi) militaires de la police, que celle-ci soit organisée de manière centralisée ou non »*[34]. Il s'agit en fait bien plus d'une militarisation des chaînes de commandement qu'une militarisation des personnels policiers, qui s'exprime à la fois dans la continuité de la chaîne de commandement et dans la subordination de ces personnels à une discipline plus stricte[35]. Or cette discipline est au fondement d'un usage raisonné et raisonnable de la force. Si pour le sociologue américain Egon Bittner le policier au sens général est celui qui met en œuvre la force en recourant à son intuition face aux situations qui surgissent devant lui[36], le criminologue québécois Jean-Paul Brodeur lui oppose la nécessité d'une centralisation et d'une militarisation du commandement comme clef de voûte de l'efficacité de l'intervention policière face à des violences collectives[37]. Le succès d'une opération de maintien de l'ordre, et donc l'abaissement du seuil de violence, résident donc dans une dépossession de l'initiative personnelle du policier au profit d'une action globale maîtrisée. Cette dernière est le fruit d'une décision centralisée,

[34] Tony JEFFERSON, *The case against paramilitary policing*, Open university press, 1990, p. 16
[35] Peter WADDINGTON, « Toward paramilitarism ? Dilemnas in the policing public order », *British Journal of Criminology*, 1987
[36] Egon BITTNER, « Florence Nightingale à la poursuite de Willie Sutton. Regards théoriques sur la police, *Déviance et Société*, vol. 25, n°3, 2001, p. 277
[37] Jean-Paul BRODEUR, « Le travail d'Egon Bittner, une introduction à la sociologie de la force institutionnalisée », *Déviance et Société*, vol. 25, n°3, 2001, p. 316

répercutée par la voie hiérarchique, et mise en œuvre sereinement grâce à la confiance qui unit les uns aux autres.

Le mouvement des Gilets Jaunes a particulièrement mis en lumière les failles qui existaient dans le recours à des unités de police non spécialisées, déployées à l'occasion des opérations de maintien de l'ordre, et dont la participation a été rendue nécessaire par le surengagement en d'autres points du territoire des compagnies républicaines de sécurité et des escadrons de gendarmerie mobile. C'est à cet égard que l'on constate une corrélation triple entre ce recours à des unités non préparées, la hausse du nombre de tirs de lanceurs de balles de défense (LBD) et la hausse du nombre de blessures graves causées par son emploi. Entre le 17 novembre 2018 et le 05 février 2019, près de 90% des tirs de LBD ont été effectués par la police nationale dans son ensemble (unités spécialisées ou non), contre 10% par les seules forces de gendarmerie mobile[38]. Ce recours massif au LBD par la police nationale n'est pas tant celui des CRS que celui des unités de la BAC et des CSI. Et pour les sénateurs, ces dernières unités, appelées en renfort, n'en ont pas fait usage dans un cadre défensif collectif sur décision du commandant d'unité, mais bien dans le cadre de la protection individuelle de ses membres exposés. Les conséquences qui ont pu découler d'un tel recours à des unités non spécialisées pour appuyer les unités de maintien de l'ordre apportent une lumière crue sur la réduction des effectifs engagée par la puissance publique avec la RGPP.

On le comprend, la militarité revendiquée par les forces mobiles, et particulièrement celles de la gendarmerie nationale[39], a une influence sur la manière dont il est fait usage de la force, toujours dans le respect des lois ; c'en est même l'un de ses marqueurs. Elle est donc un terreau favorable au déploiement de moyens particuliers comme pourrait l'être l'IA. Bien sûr l'intelligence artificielle n'a pas en elle-même de pouvoir de coercition, mais sa mise en œuvre par des structures hiérarchisées pourrait être une garantie de son emploi à bon escient, eu égards aux enjeux en matière de libertés. Il est donc d'abord ici question d'une confiance à accorder en priorité aux unités spécialisées, à ces professionnels du maintien de l'ordre qui ont fait des libertés publiques leur cœur de métier.

Leur connaissance approfondie de ces opérations permettra ainsi aux ingénieurs de développer un algorithme « intéressant », c'est-à-dire conforme aux réalités du terrain vécues par les

[38] Rapport législatif du Sénat, Proposition de loi visant à interdire l'usage des lanceurs de balles de défense dans le cadre du maintien de l'ordre et à engager une réflexion sur les stratégies de désescalade et les alternative pacifiques possible à l'emploie de la force publique dans ce cadre, 20 février 2019

[39] Général Marc WATIN-AUGOUARD, « Sauvegardons la militarité de la gendarmerie », *Le Journal du Dimanche*, 08 juin 2019

personnels policiers. Cette exigence est d'autant plus pertinente qu'en parallèle de l'institutionnalisation du maintien de l'ordre, la dynamique dans lequel s'inscrivent les casseurs est également à la « professionnalisation ». Si cette professionnalisation n'est à entendre ni au sens organique, ni au sens structurel, elle consiste plus en un *modus operandi* et des techniques de communication élaborées pour déjouer la surveillance des services de renseignement[40]. Là se joue donc l'avenir du renseignement en matière d'ordre public lors des manifestations, et nécessite l'expérience de ces forces de l'ordre spécialisées – au fait de ces techniques quasi-insurrectionnelles – pour mieux en décrypter les éléments précurseurs et affûter l'algorithme de détection.

Enfin, affirmer l'usage de l'intelligence artificielle dans une chaîne de commandement « militarisée », c'est garantir la responsabilité de l'autorité politique. En effet, la hiérarchisation stricte assure le contrôle de l'action au politique, en premier et dernier ressort. Si l'analyse des résultats fournis par l'algorithme incombera au premier chef à ces spécialistes du maintien de l'ordre, la mise en œuvre de l'action policière par ces derniers n'est que l'aboutissement d'une stratégie négociée entre ceux-ci, les manifestants et les représentants de l'autorité politique (préfets). La responsabilité de l'action est en revanche portée par l'ensemble de la chaîne décisionnelle, donc au plus haut lieu par l'autorité politique elle-même. Intégrer l'IA dans une chaîne de commandement militarisée, c'est donc en soi se prémunir d'une déresponsabilisation des décideurs en cas de mésusage.

B. D'un encadrement de la foule à son accompagnement : dissuader autrement

« De toutes les manifestations du pouvoir,
celle qui impressionne le plus les hommes, c'est la retenue »

Thucydide, *Histoire de la guerre du Péloponnèse,* V^e^ siècle av. J.-C.

Le premier enjeu de toute opération de maintien de l'ordre est la maîtrise de l'espace. C'en est même un élément fondamental à tel point que pour Peter Waddington, les polices de gestion des foules disposent aujourd'hui d'une expertise non pas tant dans le contrôle des

[40] Jacques BAUD, *La guerre asymétrique ou la défaite du vainqueur*, Éditions du Rocher, 2003, p. 110-114 : *« Contrairement à une opinion largement répandue – et aux affirmations de certains services de renseignement – le black bloc n'est ni une structure, ni une organisation, ni un réseau, ni une idéologie. Elle représente une fonctionnalité au sein d'une manifestation, associée à une stratégie d'action de nature asymétrique. »*

interactions physiques que dans l'évitement préalable de la confrontation. Cette expertise repose à la fois sur une analyse de l'environnement dans lequel les foules vont évoluer (1), et sur une compréhension de leurs mouvements (2).

1. Adapter la gestion du maintien de l'ordre à l'environnement : l'IA des objets

L'excellence d'une opération de maintien du l'ordre réside pour partie dans l'appréhension de l'environnement dans lequel la manifestation va avoir lieu. Bien évidemment, cette analyse commence au moment de la déclaration de la manifestation. Le décideur public va dès lors valider, ou non, le parcours que va emprunter le cortège, en fonction des zones identifiées comme étant particulièrement à risques au regard des circonstances (hôpitaux, commerces, lieux de culte, continuité de la circulation à moteur) ou impraticables (chantier en cours sur la voie publique). À ce titre, il ne faut pas oublier que l'exercice d'une manifestation impose pour d'autres des sujétions et restrictions aux libertés. La liberté de manifester peut ainsi constituer une entrave à la liberté d'aller et venir des individus, mais aussi une atteinte à la liberté du commerce et de l'industrie pour les commerçants qui estiment que le défilé du cortège risque de leur causer des dégâts, et qui préfèrent donc baisser le rideau. Par conséquent, il y a en premier lieu une analyse de l'environnement au niveau politique, par l'autorité préfectorale en charge de la préservation de l'ordre public. L'intelligence artificielle profiterait ici largement dans l'appui à la décision. L'intégration des données relatives à la cartographie et à la configuration des lieux, la présence de points d'intérêts, et la fusion de données accessibles en sources ouvertes (comme l'organisation concomitante d'événements en plein air, ou privés à proximité) permettraient d'offrir à l'autorité préfectorale une plus large vision des éléments en présence susceptibles d'interférer dans la gestion des foules manifestantes.

Mieux encore, l'intégration et le traitement de données de masse en sources ouvertes permettraient de garantir aux autorités policières en charge des opérations une analyse plus fine au regard des forces à mobiliser. À cette fin, l'analyse des pages publiques de réseaux sociaux permettrait de dégager des tendances, non pas seulement à partir de la visibilité de la page et de son succès en terme de consultations et d'abonnements, mais également à partir de leur occurrence, voire même du contenu des messages postés publiquement. Car entre les sympathisants d'une cause et ses membres actifs, l'appréciation de l'ampleur d'un mouvement semble actuellement plus relever de l'intuition des services de renseignement que de réels

critères scientifiques. L'IA se propose ici comme un outil de rationalisation de l'action publique appliquée aux opérations de maintien de l'ordre.

Par-delà l'aspect anticipation, l'IA des objets semble prometteuse dans plusieurs domaines. S'appuyant sur son réseau de plus de 9000 caméras de vidéoprotection dans les gares franciliennes, la SNCF se montre précurseur en la matière. Grâce à sa plateforme de test PREVIA, la société de transport propose d'ores et déjà à des opérateurs privés de mettre en œuvre leurs logiciels d'intelligence artificielle avec des données réelles issues de ce réseau. Ces démonstrateurs permettent donc dès aujourd'hui d'avoir un aperçu des applications imminentes de l'IA dans le domaine de la gestion de foules, sous la dérogation à des fins expérimentales explicitement autorisée par la CNIL. Avec la création de cette plateforme commune à tous les candidats fournisseurs de service, la SCNF les évalue de manière équitable, et valorise ainsi son flux vidéo aujourd'hui largement sous-exploité pour détecter et prévenir les situations à risques.

Au premier rang, on trouve la détection d'objets et la détection de personnes. Si la détection par l'IA d'un bagage abandonné ne fonctionne pas encore, les opérateurs travaillent à corréler le comportement des usagers avec leurs objets. La détection de personnes exclut aujourd'hui la reconnaissance faciale, car cette dernière nécessiterait l'intégration de données biométriques à l'algorithme. Or, la fourniture de ce type de données qualifiées de hautement sensibles par les autorités publiques, qui plus est à des opérateurs privés, n'est encore ni leur intention ni celle de la loi. L'IA travaille donc à l'heure actuelle uniquement à partir de la tenue vestimentaire et des accessoires portés par les personnes. Pour exemple, la RATP développe actuellement sous le contrôle de la CNIL un logiciel de vidéoprotection intelligente, qui détecte les individus à partir de la masse et des pixels de couleurs rendus à l'image, et facilite leur suivi dans les couloirs de la station Châtelet – Les Halles. On peut d'ores et déjà imaginer la transposition d'une IA des objets dans les opérations de maintien de l'ordre qui, à partir du flux vidéo capté en temps réel par tout type de sources (vidéoprotection sur la voie publique, caméras-piéton, caméras-véhicule, drones, hélicoptères), permettrait l'identification d'objets considérés comme dangereux. Il faudrait pour cela en premier lieu orienter l'apprentissage sur les objets légalement considérés comme des armes[41], puis étendre l'apprentissage aux armes par destination telles que la jurisprudence pénale les identifie. À cet égard, le projet ALICE

[41] Le code de la sécurité intérieure prévoit dans son livre III titre premier une police administrative spéciale relative aux armes et munitions. Voir notamment les articles L311-2 et suivants qui prévoient une catégorisation des armes ainsi que les conditions dans lesquelles elles peuvent être détenues, et l'article R311-1 donnant les définitions.

(*Automatic Labelling for Image Collections Exploration*) développé par la Gendarmerie nationale dans le cadre de son plan stratégique « Recherche & Innovation », permet déjà d'automatiser la recherche, le tri et l'identification d'images exposant des armes à feu, des stupéfiants ou du contenu pédopornographique ; à ceci près qu'il ne concerne pour l'heure que les réseaux criminels[42].

L'intérêt n'est évidemment pas pour l'IA de mettre sous les yeux du décideur l'ensemble des objets comportant un risque d'utilisation malfaisante, mais d'associer ce risque à un type de manipulation ou un comportement qui ne laisse que peu de place au doute. La matière pénale a d'ailleurs une appréciation extensive de la notion d'arme, ce qui complexifierait inutilement la tâche du décideur si tout devait en permanence lui être présenté. Dès lors, si dans la phase anticipation de la manifestation, l'IA détecte du mobilier urbain particulièrement sensible par son amovibilité ou du matériel de chantier sur le cheminement, une première alerte pourra éveiller l'attention du décideur. En outre, et la période actuelle y est propice, il sera décisif d'identifier les objets pouvant représenter un danger pour les manifestants eux-mêmes, en dehors des éléments « communs » que l'on peut trouver en manifestation. Rien ne permet d'écarter l'idée que des terroristes décident de s'en prendre violemment à des individus à l'occasion de manifestations, qui constituent par essence de grands rassemblements de personnes. Cette hypothèse n'est pas uniquement celle d'une attaque violente directe, mais pourrait prendre le tour d'un colis ou d'un objet piégé[43]. L'IA pourrait à cet égard mettre en surbrillance les éléments qu'elle identifie comme présentant un intérêt sur les écrans présentés au décideur.

D'ailleurs, ces éléments d'intérêt pourraient diriger les attentions des décideurs sur les personnes qui se trouveraient en difficulté au sein du cortège. Cela pourrait concerner les personnes qui se trouvent mêlées malgré elles au cœur des cortèges, ou bien les personnes qui présenteraient une particulière vulnérabilité en raison de l'âge, d'une grossesse ou d'un handicap physique visible qui conduirait les forces de l'ordre à adapter leur plan d'action. À cet égard, l'intelligence artificielle permet d'apporter une analyse plus fine de la situation, nécessaire à une action des forces de l'ordre guidée par la souplesse.

---

[42] Plan stratégique « Recherche & Innovation » disponible en version PDF : https://erewerra2.files.wordpress.com/2018/07/plan-stratc3a9gique-de-la-recherche-et-de-linnovation-1.pdf

[43] Ce mode opératoire, courant au Moyen-Orient, a déjà eu son précédent en France, à l'occasion de l'attentat préparé par un commando de jeunes femmes, et déjoué à Paris le 04 septembre 2016. Une berline, dans laquelle se trouvaient cinq bonbonnes de gaz et trois bidons de gasoil, avait alors été garée près de la cathédrale Notre-Dame par les suspectes avant qu'elles ne tentent d'y mettre le feu. Si au demeurant aucune manifestation n'avait lieu, la rue accueillant à ce moment de très nombreux touristes, dans ce quartier fréquenté de la capitale.

Plus précisément encore, la détection de personnes conduit inévitablement à l'étape d'après, qui est celle de leur traçage dans la foule. Il n'est évidemment pas question d'un point de vue légal et éthique, ni même nécessairement intéressant d'un point de vue opérationnel, de tracer l'ensemble des manifestants individuellement. Mais la capacité de l'IA à suivre un individu qui présenterait les signes précurseurs d'un comportement violent, identifiés par l'algorithme au fur et à mesure de son balayage, serait une plus-value patente. Sans aller jusqu'à interpeler préventivement l'individu, une meilleur anticipation des comportements individuels anormaux permettra d'ajuster le dispositif en fonction de ceux-ci : faire suivre l'individu par des équipes discrètes dans la foule ou aux abords uniquement, déployer des éléments mobiles d'intervention en prévision d'une interpellation si des voies de fait étaient commises, etc… Cette proposition prend un tour particulier, à l'heure où, pour des motifs tenant à la santé publique, la CNIL a validé l'usage du traçage de contacts pour téléphones intelligents par l'intermédiaire de l'application StopCovid. Cette application mobile respecte les dispositions relatives à la vie privée, et notamment le consentement car son installation demeure à la discrétion de l'utilisateur.

D'une certaine manière, si d'aucuns peuvent considérer que IA viendrait à renverser le paradigme classique selon lequel « le terrain commande », il est plutôt raisonnable de penser que c'est l'adaptation à celui-ci qui en sortira largement renforcée. En revanche, il est bien un paradigme qui change avec l'IA, c'est le passage d'une logique de stock à une logique de flux.

2. <u>D'une logique de stock à une logique de flux : une nouvelle appréhension des opérations de maintien de l'ordre facilitée par l'intelligence artificielle</u>

Il est ici question de l'interaction qui opère entre l'IA et le second pilier qui fonde la doctrine de gestion policière des foules en France : le maintien à distance dans une posture dissuasive. Force est de constater que c'est sans doute ce pilier qui est le plus sujet à effritement. Avec le mouvement des Gilets Jaunes, les grandes manifestations traditionnelles ont laissé place à des phases d'intense confrontation des manifestants avec les forces de l'ordre. Celles-ci s'expliquent notamment par l'absence de porte-parole pour représenter l'action manifestante, qui s'est traduite par un manque de concertation et de négociation pour l'adaptation des dispositifs policiers. Et l'action a, par la suite, été compliquée par la greffe de groupes très politisés au mouvement. Ainsi selon le professeur Jacques de Maillard, pour la seule journée du 1er décembre 2018 (acte III), les échauffourées ont conduit à dénombrer 400 interpellations,

125 blessés dont 25 parmi les forces de l'ordre, et près de 1000 grenades de désencerclement jetées (soit plus que sur toute l'année 2017 !)[44].

Pourtant, il était de coutume de penser que la police disposait d'acquis solidement ancrés et imperturbables. Il était même admis que *« la police, en matière de manifestation, « joue à domicile » (home-ground advantage), et dispose d'un monopole du savoir et de l'expertise qui lui permet d'orienter, de guider, de manipuler les protestataires en exerçant sur eux un ascendant dans la préparation de la manifestation qui élève considérablement les coûts de la protestation violente »*[45]. Face à l'émergence de mouvements nouveaux, diffus et parfois même spontanés[46], les forces de l'ordre doivent donc s'adapter. La simple présence policière et l'exposition des attributs de la puissance républicaine ne sont plus suffisantes pour dissuader les foules à mener des actions violentes. Et police comme gendarmerie doivent identifier les leviers tant psychologiques qu'opérationnels qui lui permettront à nouveau d'encadrer sereinement ces manifestations, qui se dérouleront vraisemblablement de plus en plus selon ces nouvelles modalités.

L'intelligence artificielle trouve à cet égard une application majeure dans la réduction de l'incertitude pour le décideur, dans les phases de conception et de conduite globale de la manœuvre. Là où il est aujourd'hui nécessaire d'avoir une appréhension compartimentée du terrain afin de séquencer l'opération de maintien de l'ordre en une succession de missions intermédiaires plus facilement réalisables, l'IA modélise l'environnement dans son entièreté et en temps réel, grâce à sa capacité de traitement massif des données. Cette approche est particulièrement intéressante car elle permet une prise de recul instantanée du décideur, face à au risque de surexposition à l'information qui le guette. Cette capacité de synthèse déléguée à l'algorithme permet ainsi une plus grande souplesse dans le conditionnement de l'action globale. Dès lors, l'IA réaffirme son rôle stratégique dans la conduite des opérations, particulièrement dans les opérations de maintien de l'ordre en zone rurale, comme l'ont pu être Sivens ou Notre-Dame des Landes. Ces ZAD qui, par essence, ne se prêtent pas un

[44] Jacques de MAILLARD, « Relations police-population », *DéfiS*, n°9, décembre 2018
[45] Fabien JOBARD, « La militarisation du maintien de l'ordre, entre sociologie et histoire », *Déviance et Société*, vol. 32, n°1, 2008, p. 104
[46] On pense ici notamment au phénomène des zones à défendre (ou ZAD), qui agrègent des populations issues d'horizons divers, dont les combats intellectuels rapprochent les actions, et qui se manifestent en particulier par des occupations illégales du domaine privé, afin de s'opposer à des projets publics d'aménagement du territoire.

compartimentage efficace et pertinent, d'une part exposent plus les forces de l'ordre face à des manifestants beaucoup plus mobiles[47] et d'autre part complexifie la fluidité des ordres.

Cet aspect stratégique trouvera également à s'appliquer dans l'identification et la prévention des mouvements de foule. Ces derniers, entendus largement, peuvent être dissociés en mouvements intérieurs (radicalisation violente d'un groupe qui se détache du lot ordinaire manifestant ; ou sur un tout autre registre peur panique dans la foule due à événement interne ou externe à la manifestation) ou extérieurs (rassemblement d'une contre-manifestation). Là encore, l'IA décuple la capacité d'analyse des forces de l'ordre, en appréciant la manifestation de manière décompartimentée. Cette IA des foules n'est pas uniquement un moyen de prévention et de répression des actes malveillants, mais également un moyen de prévenir les risques inhérents à un trop grand rassemblement de personnes. Si peu d'exemples ont marqué l'histoire des mouvements françaises, on ne peut que se remémorer le drame de la *love parade* de Duisbourg. Cette manifestation musicale organisée en juillet 2010 avait rassemblé près de 1,4 millions de participants dans cette commune d'Allemagne ; un mouvement de foule avait conduit à la mort de 19 personnes et plus de 500 blessés, dont deux succomberont des suites de leurs blessures. En l'espèce, les conditions n'étaient pas manifestement pas réunies pour accueillir autant de monde, puisque les organisateurs n'attendaient que 250 000 personnes. Mais l'idée qu'un algorithme détermine le seuil à partir duquel, selon la configuration des lieux, les risques deviennent trop importants permettrait aux forces de l'ordre de dissiper progressivement et sereinement ces lieux particuliers d'exposition aux risques.

L'IA permettrait de renforcer la capacité des forces de l'ordre à assurer le maintien à distance des manifestants tout en restant dans une posture dissuasive. Ce maintien à distance est traditionnellement conçu comme un principe fondamental tant que l'action des forces de l'ordre n'est pas nécessaire pour mettre fin à des infractions graves d'atteintes aux personnes. Le mouvement des Gilets Jaunes a d'ailleurs questionné l'opinion publique sur ce qui apparaît comme une absence de réaction face aux atteintes contre les biens, dont les seules dégradations contre des biens privées étaient déjà évaluées par la fédération française de l'assurance à près de 170 millions d'euros[48] après l'acte 18. Il s'agit pour le décideur d'être éclairé sur les situations potentiellement crisogènes, et d'en prévenir leur réalisation. La vraie question opérationnelle est celle du délai d'analyse de la convergence des événements avec une situation

[47] Audition du général Bertrand CAVALLIER devant la commission d'enquête sur les missions et modalités du maintien de l'ordre républicain dans un contexte de respect des libertés publiques et du droit de manifestation, n°2794, XIV[ème] législature, 15 janvier 2015

[48] « La somme exorbitante des dégradations causées par les Gilets jaunes », *Capital*, 19/03/2019

à risque, afin de permettre un plan de réaction temporellement réalisable. On imagine bien que si l'IA détecte une situation à risque dont la réalisation est à trois minutes, encore faut-il disposer des moyens à portée pour intervenir sur zone.

Malgré tout, il est indéniable que l'IA apportera une souplesse dans le commandement. Mais la dissuasion n'est que rarement suffisante dans les opérations de maintien de l'ordre, et la nécessité d'intervenir n'est jamais loin. Là aussi l'IA s'inscrit dans une logique de continuité avec la doctrine actuelle de maintien de l'ordre.

C. Un outil favorable, par conception, à un usage proportionné et gradué de la force

La doctrine française est fondée sur le respect du droit à la vie, tel qu'il est énoncé par l'article 2 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales : c'est-à-dire le recours à la force comme *ultima ratio*. La puissance publique peut donc faire usage de moyens de coercition lorsqu'il y a dégénérescence dans l'exercice de la liberté de manifester sur la voie publique. En effet, il s'agit pour l'autorité de disperser les manifestants qui n'auraient pas déclaré leur intention de manifester, ou n'y mettraient pas un terme lorsqu'arrive la fin prévue de la manifestation, et par voie de conséquent qui constitueraient des attroupements[49].

En plus du cadre commun à tout citoyen concernant le recours à la force (article 122-4 à 122-7 du code pénal intégrant l'état de légitime défense, et l'état de nécessité) et du cadre particulier d'usage de la force prévu par l'article L435-1 du code de la sécurité intérieure, deux hypothèses permettent aux policiers et gendarmes déployés en opérations de maintien de l'ordre de recourir à la force. Explicitement mentionnées à l'article L211-9 du code de la sécurité intérieure, elles permettent, du fait de leur gravité, de s'affranchir des deux sommations réglementaires. Il s'agit en premier lieu des *« violences et voies de faits »* exercées à leur encontre. Et en second lieu de la défense des terrains qu'ils occupent.

Quel que soit le cadre du recours à la force, deux principes cardinaux issus de cet article 2 de la CEDH s'appliquent en toutes circonstances : absolue nécessité et proportionnalité. Policiers et gendarmes n'emploieront donc la force que selon un schéma de gradation[50].

[49]Art. 431-3, Code pénal : *« Constitue un attroupement tout rassemblement de personnes sur la voie publique ou dans un lieu public susceptible de troubler l'ordre. »*
[50] Voir Annexe IV

C'est à cet égard que l'intelligence artificielle montre à nouveau l'étendue de son intérêt. L'État a tout à perdre dans une opération de maintien de l'ordre qui dégénère : exposition de ses personnels à des risques de blessures, impact médiatique dans la presse, perte de confiance de ses citoyens, préjudice économique. Oui, l'État est en première ligne dans la réparation des *« dégâts et dommages résultant des crimes et délits commis, à force ouverte ou par violence, par des attroupements ou rassemblement armés ou non armés, soit contre les personnes, soit contre les biens »*[51]. La loi rend ainsi l'État civilement responsable, et sans faute, de tous les préjudices liés à des opérations de maintien de l'ordre, qui ne parviendraient pas à leur objectif. Par l'analyse fine des comportements qu'elle devra démontrer, l'algorithme pourra proposer au décideur les modalités d'un déploiement du juste niveau de forces mobiles en des points particuliers du cheminement : ceux qui seraient menacés par un développement soudain d'actions violentes dans un temps rapproché par des manifestants.

Une nouvelle fois, l'IA apparaît comme un outil de rationalisation des dépenses publiques, tout à la fois dans la prévention des atteintes aux biens et aux personnes, que dans l'économie des forces nécessaires à la réussite de ces opérations. Il ne s'agit toujours pas de déléguer à la machine la conduite des manœuvres, mais bien d'en tirer une appréciation situationnelle objective sur l'ensemble du cortège. Néanmoins, rien n'empêche à l'heure actuelle d'intégrer à l'algorithme les cadres d'intervention classiques retenus par les EGM et les CRS, afin que celui-ci propose un ou des schémas qui, au vu des éléments présentés, paraissent le mieux atteindre l'objectif de pacification.

§2. … à un renouveau de la doctrine du maintien de l'ordre à la française

À la lecture de ces éléments, on comprend que l'intégration d'un tel outil d'aide à la décision dans le champ des opérations de maintien de l'ordre conduirait à bien plus qu'une simple évolution. Il s'agit bel et bien d'une révolution car plus que commander un système numérique il devient nécessaire pour le chef opérationnel de commander avec lui. Il faut donc se questionner sur l'émergence d'un processus de codécision (A). Parallèlement, la discussion sur l'usage d'algorithmes à l'occasion de manifestations doit permettre d'en soulever les applications en amont de celles-ci, et à leurs abords immédiats le jour J : c'est la question du

[51] Art. L211-10, Code de la sécurité intérieure

contrôle de la « profondeur stratégique » (B). Enfin, face à la judiciarisation des opérations de maintien de l'ordre, l'IA parachève-t-elle ce mouvement ?

A. L'apprentissage de la codécision

Développer de nouvelles capacités conduit irrémédiablement à repenser les techniques de travail. La plasticité des technologies numériques doit permettre au chef d'en explorer toutes les fonctionnalités, avant qu'il puisse mettre en œuvre ce système en situation opérationnelle. Cet entraînement doit également lui permettre de penser autrement, c'est-à-dire de profiter de la simulation pour sortir des cadres traditionnels et confronter ses perspectives à la réalité virtuelle. Cet exercice d'imagination que l'IA va démocratiser auprès de tous les tacticiens du maintien de l'ordre est un fondement, que d'aucuns qualifieraient de devoir[52], dans l'adaptation d'une doctrine aux évolutions sociétales. L'IA devra donc intégrer cette dimension éducative, et servir de bac à sable pour tester la solidité des modèles. À la différence d'un algorithme de simulation classique qui pour une série d'actions identiques proposées par l'utilisateur répondra toujours la même chose, l'IA s'adaptera en proposant des *scénarii* toujours plus réalistes.

Plus précisément, l'IA doit permettre au décideur d'identifier les conséquences immédiates et à long terme des ordres qu'il donne. Elle pourrait dès lors jouer un rôle majeur dans la prévention des erreurs tactiques. Par la capacité d'analyse et de comparaison probabiliste avec des situations passées, l'IA doit mettre le décideur à l'abri de situations sans issues. L'exemple le plus parlant est celui d'une succession d'ordres mineurs pour l'organisation de la manœuvre qui conduirait *in fine* à la création d'une nasse, sans échappatoire pour les manifestants. Cette dimension anticipationnelle ne devra d'ailleurs pas rester une exclusivité de son application éducative. Adjoindre un tel outil d'alerte à l'IA opérationnelle est même une nécessité pour réaménager un plan initial de manœuvre, qui s'avère en pratique irréalisable ou dangereux. Les militaires ont pour coutume de dire que le plan est la première victime de la bataille. Il faut donc permettre au tacticien de s'adapter au plus vite face à une situation que l'on pourrait qualifier de convergente, et lui garantir un délai optimal pour réagir et diverger de la situation à risque.

Au demeurant, la formation des cadres de la police et de la gendarmerie nationales, qu'elle soit initiale ou continue, n'est pas extensible à l'infini. Il faut dès lors que l'apprentissage du

[52] Rémy HÉMEZ, « Tactique : le devoir d'imagination », *RDN*, n°704, 2008, p. 50-56

fonctionnement soit aisé et que sa mise en œuvre soit rapide et peu coûteuse. Comme le fait remarquer le général Marc de Fritsch à l'égard des applications d'appui à la décision militaire[53], l'intégration de la symbologie et des modes d'actions couramment utilisés par les opérationnels sera un élément structurant de la compréhension des schémas proposés par l'IA. Il n'est toujours pas question de déléguer à l'IA une quelconque autonomie sur la mise en œuvre d'un schéma d'intervention, mais bien de l'associer au processus décisionnel. Cette association prend donc le tour d'une codécision qui est porté par le seul décideur opérationnel, et par voie de conséquent l'ensemble de la chaîne hiérarchique. Il est ainsi question d'une confiance, ou non, dans la capacité de l'algorithme à fournir des éléments d'anticipation, nous reviendrons plus en détail dans cette étude sur l'explicabilité d'un tel processus de codécision.

B. Prendre le contrôle de la « profondeur stratégique » ?

Cette notion de profondeur stratégique, chère aux militaires, permet de porter le combat loin du sanctuaire (le territoire national) s'il devait advenir malgré les efforts pour le prévenir. Le nerf de toute opération est le renseignement. À cet égard, il convient de déterminer dans quelles limites la captation de ce dernier pourrait s'effectuer dans le cadre des opérations de maintien de l'ordre.

Nous l'avons observé un peu plus haut dans cette étude, la recherche de renseignement en amont des manifestations est un enjeu stratégique. Elle l'est en vue d'une éventuelle interdiction de manifester si des éléments réels et objectifs viendraient à questionner l'autorité préfectorale sur sa capacité à assurer le respect de l'ordre public. Mais elle l'est tout autant afin d'ajuster au mieux le dispositif policier qui accompagnera la foule. Cette recherche de renseignement est donc prévisionnelle, et le traitement massif de données numériques accessibles en sources ouvertes semble être une voie, il faut le reconnaître, relativement peu intrusive au regard des libertés publiques et individuelles. En revanche, il faut se questionner sur la captation de données au moment de la manifestation, et qui serait susceptibles d'une analyse en temps réelle ou différée par un algorithme d'apprentissage.

Il est ici finalement question du périmètre à l'intérieur duquel les données seront captées par l'IA dans le cadre unique d'une opération de maintien de l'ordre. Au regard de la jurisprudence actuelle, il semble dangereux de vouloir connecter l'IA aux données des réseaux exclus du

[53] Marc de FRITSCH, Ariane BITOUN, « Commander avec l'IA, une aide à la conception et à l'évaluation des modes d'action », *RDN*, n°820, 2019, p. 81-85

périmètre de la manifestation. L'IA appliquée aux manifestations devra rester cantonnée aux manifestations. Dès lors, si un individu suspect quitte le cortège et que son suivi s'avère nécessaire, il devra l'être par les moyens numériques ou physiques que l'on connaît actuellement. Qu'en est-il des cortèges qui en viendraient à se disperser volontairement ou involontairement hors de l'itinéraire prévu ? Il serait également juste de ne pas transposer l'IA sur les réseaux ordinaires de captation d'images de sécurité publique.

Dans son aspect numérique, le contrôle de la profondeur stratégique semble finalement être une capacité d'action raisonnable que la représentation nationale pourrait accorder à l'exécutif. Bien plus en tout cas que cette profondeur physique de terrain qui couvrirait les abords des cortèges, et dont les limites seraient sources intarissables de discussions au regard des libertés collectives et individuelles des autres citoyens extérieurs à ces cortèges.

C. Vers une gestion individualisée des foules, affirmation d'une judiciarisation du maintien de l'ordre ?

« Le maintien de l'ordre est une opération policière
qui se joue à l'avant-scène d'une tension autour du principe de représentation »

Fabien Jobard, *Le Monde Culture & Idées*, 07 février 2015

Une telle question nous amène à reconsidérer le modèle qui jusqu'alors avait guidé les politiques françaises de maintien de l'ordre, et qui prend racine dans les travaux de Gustave Lebon. Dans son ouvrage *Psychologie des foules* paru en 1895, l'auteur distingue la foule d'un simple agrégat d'individus pour la considérer comme une unité propre. Celle-ci dispose, de son propre fait, de leviers d'influence sur l'individu présent en son sein, au rang desquels on trouve sa déresponsabilisation, sa suggestibilité et par conséquent sa *« contagion »* aux passions qui la traversent et qui s'exprimeront plus violemment en lui. Il y a pour l'auteur une dissolution de l'individualité au profit d'une âme commune, guidée par une morale et des passions propres. Lebon y exprime aussi l'idée selon laquelle sans meneurs, la foule ne peut garder sa cohérence longtemps ce qui l'expose à la désagrégation.

Pour maîtriser cette entité considérée comme unique, les forces de l'ordre ont donc développé un ensemble de techniques préventives (médiation, limitation des mouvements autour de points

sensibles) et répressives (barrages fixes, bonds offensifs, charges). Ces méthodes visent à canaliser et orienter les flux de personnes dans le cadre d'une gestion globale de la foule.

Or, face à l'émergence croissante *« d'individus violents animés, peu ou prou, par la seule volonté de troubler l'ordre public, de commettre des exactions (y compris contre les manifestants eux-mêmes) ou de se confronter aux forces de sécurité »*[54], il convient de rappeler que l'objectif premier des opérations de maintien de l'ordre est de permettre un exercice apaisé de la liberté de manifester par les foules, donc d'en extraire les individus qui en alimentent la violence. Depuis les émeutes urbaines de 2005, EGM et CRS ont ainsi détaché respectivement des pelotons d'intervention (PI) et des sections de protection et d'intervention (SPI) qui, appuyés par des groupes de police judiciaire extérieurs au maintien de l'ordre, procèdent aux interpellations. Cette évolution des attentes a complexifié la mission traditionnelle des forces mobiles qui selon l'adage se résume à « tenir et subir, collectivement ». Car il s'agit avant tout pour ces forces d'assurer une gestion démocratique des foules, et non d'interpeler (mission qui nécessite une posture moins figée, ce que le rapport Popelin rappelle à juste titre). Et c'est le débat dans lequel l'intelligence artificielle s'inscrira nécessairement, encore qu'elle pourrait bien réconcilier ces deux positions.

En effet, la multiplication des capteurs, qui permettent d'affiner l'identification des fauteurs de trouble, est utilisée par les défenseurs de cette judiciarisation du maintien de l'ordre comme un moyen de plus en plus sûr d'imputabilité des infractions commises. Dans le même temps, l'intégration d'une IA aux images collectées en temps réel pourrait permettre un déploiement rapide et visible de ces PI et SPI – voire même d'agents en uniforme dans les foules comme les *Konfliktmanagement Polizei* en Allemagne – sur les zones où des individus se préparent à commettre des infractions. L'idée n'est évidemment pas de déployer ces unités de manière furtive pour tenter un flagrant-délit à tout prix, mais bien de se préserver d'un dérapage qui appellerait à d'autres violences.

L'intelligence artificielle des foules permettrait donc d'améliorer l'efficacité de ces unités d'interpellation. Cette efficacité se traduira fatalement en une plus grande dissuasion que les forces de l'ordre pourront opposer aux manifestants velléitaires. On change ainsi de modèle de représentation. Les forces de l'ordre ne seraient plus ces digues sur lesquels des vagues humaines mécontentes et déferlantes viendraient se jeter dans une gerbe d'écume, mais une plage accueillant la marée humaine pacifique, ponctionnée de la houle des violents.

---

[54] *op. cit.* note 11, p. 12

Ce changement des apparences théâtrales du maintien de l'ordre permis par l'IA ne serait ainsi pas sans rappeler le système allemand de gestion des foules. La souplesse de déploiement des unités de types SPI/PI en des points particulièrement à risques tout au long des cortèges, et pour des durées limitées, n'en serait donc pas moins efficace. Mais pour que cette nouvelle entreprise du maintien de l'ordre fonctionne, encore faut-il qu'elle soit expliquée aux manifestants : avant la manifestation (par voie de presse ordinaire), et surtout pendant son déroulé par l'usage de panneaux lumineux ou par voie de mégaphone par exemple.

Il pourrait à cet égard être envisagé des messages préenregistrés qui seraient émis régulièrement. Il ne s'agit pas évidemment pas d'infantiliser les manifestants en leur indiquant comment ils doivent manifester, mais des messages particuliers pourraient être diffusés automatiquement pas l'IA, après validation par les autorités préfectorales, en fonction des réactions de la foule. D'une certaine manière, il pourrait se nouer une interaction plus directe avec l'ensemble de la foule, en fonction des réactions de celle-ci interprétées par l'IA. Est-ce à créer un dialogue entre la machine et la foule ? C'est en tout cas une hypothèse intéressante.

Le réel point sensible d'une IA d'analyse des foules, doctrinalement et éthiquement parlant, réside dans un heurt avec les libertés individuelles. Couplée à des outils numériques de détection faciale, des intelligences artificielles peuvent d'ores et déjà détecter des émotions pour prédire et anticiper les réactions des usagers de transports publics, à l'image de la solution proposée par la *start-up* française *Two-i* dans le tramway de Nice. Il faut ici insister sur la distinction entre détection faciale et reconnaissance faciale. Si l'analyse d'une expression faciale relève d'une détection faciale, il en est tout autrement de la reconnaissance qui nécessite une comparaison numérique entre la détection d'un visage, en temps réel ou différé, avec une base de données biométriques. Et si la détection faciale est déjà une atteinte certaine à l'intimité et à la vie privée, il en est d'autant plus au sujet de la reconnaissance faciale. La question juridique qui pourrait survenir est celle de l'entraînement d'algorithmes à la seule détection de visages par des opérateurs privés. C'est un sujet qui de toute façon nous concerne depuis bien longtemps, à raison des applications mobiles pour smartphones que nous téléchargeons quotidiennement (services de communications de type *Instagram, Snapchat*), et qui depuis déjà quelques années ont appris non pas seulement à nous détecter mais à nous reconnaître (service reconnaissance faciale pour déverrouiller les téléphones de marque *Apple*). Les grandes entreprises détiendraient finalement déjà plus de données sur nous-mêmes que ce que nous sommes prêts à en consentir à notre propre État, à se demander si ces « services » n'asservissent pas plus qu'ils ne servent ?

Est-ce à dire que dès demain cette solution de la détection, voire de la reconnaissance faciale à l'occasion d'un état d'urgence par exemple, sera appliquée en temps réel aux images collectées lors de manifestations ? C'est un point à ne pas écarter, et il faut dès à présent poser les bases d'une discussion juridique et éthique à ce sujet. Plus que détecter un comportement qui sort de « l'ordinaire » d'une manifestation, il s'agit pour l'algorithme de détecter les émotions à partir des expressions faciales et gestuelles. Par-delà la détection, la vraie question est celle de l'analyse qui est en est faite. Quelle pertinence peut être accordée à l'interprétation d'une émotion ? Un visage qui se ferme, synonyme d'un mécontentement, peut-il s'assimiler à une volonté de révolte ? Ou est-ce simplement l'expression d'un désarroi à défiler toute une après-midi alors que le vent se lève et que les nuages se montrent de plus en plus menaçants ?

L'intelligence artificielle se présente donc comme un formidable démultiplicateur pour le décideur, et une inextricable source de conflits avec les libertés collectives et individuelles. Elle se propose de pousser les situations aux extrêmes afin de mesurer les effets d'une décision, elle apporte non pas une garantie mais des éléments d'appréciation supplémentaires au décideur. À l'autre bout du spectre, elle se présente comme un moyen supplémentaire de gestion démocratique des foules, en s'efforçant d'apporter des solutions respectueuses de la proportionnalité, en prévenant les confrontations directes en forces de l'ordre et manifestants. Enfin, elle se promet d'affranchir le décideur des difficultés inhérentes au milieu dans lequel son opération se déroule, en le libérant d'un compartimentage parfois contraignant.

Section 3 – Une stratégie nationale industrielle et de ressources humaines à développer

Une telle stratégie de moyens devra s'appuyer sur une base industrielle et technologique forte et « souveraine » (§1), avec laquelle les pouvoirs publics pourront construire un travail en plateau et s'ouvrir éventuellement à une interopérabilité européenne (§2). Néanmoins, ils ne devront pas négliger le développement et le maintien de compétences techniques en interne (§3).

§1. La nécessité de s'appuyer sur une base industrielle et technologique forte et « souveraine »

La France et l'Union européenne ont pris tardivement conscience de l'enjeu que représentait l'intelligence artificielle. Quelques jours après la parution du rapport Villani en 2018, le Président de la République a annoncé un plan massif d'un montant de 1,5 milliards d'euros alloué spécifiquement à l'IA. Des priorités émergent, dans la droite lignée du rapport Villani, et portent notamment sur la recherche, l'ouverture des données et les enjeux éthiques, au travers d'appels à projets sur la durée du quinquennat 2017-2022. Le ministre de l'Enseignement supérieur, de la Recherche et de l'Innovation, et le secrétaire d'État au numérique ont présenté dans la foulée une stratégie nationale de recherche en IA, qui vise à *« faire de la France un leader mondial de l'intelligence artificielle »* en permettant de *« consolider notre expertise de niveau mondial et d'attirer les meilleurs talents »*[55].

La volonté affichée est donc de rattraper un retard en la matière car il est vrai qu'en 2016 : 3,2 milliards d'euros était investis dans l'IA en Europe, contre près de 12,1 milliards d'euros pour la seule Amérique du nord et 6,5 milliards d'euros pour l'Asie[56]. À cet égard, et avec le retrait du Royaume-Uni qui contribuait massivement à gonfler cette enveloppe, l'Union européenne a sorti hâtivement en février 2020 un livre blanc sur l'IA, afin de déterminer des orientations stratégiques tenant compte des risques inhérent aux utilisations de cette technologie. La Commission veut conserver une approche *« axée sur la régulation et l'investissement »*, car l'aide d'État ne doit pas être effectivement la seule voie de l'investissement en matière d'IA. La France a bien saisi l'enjeu et vise à long terme, par sa stratégie nationale, la captation des capitaux d'investissement privé et l'attrait de chercheurs et d'étudiants, notamment en facilitant l'octroi de visas dits « technologiques ». Pour Floran Vadillo, docteur en science politique et

[55] *Stratégie nationale de recherche en intelligence artificielle*, 2018
[56] *Livre blanc sur l'intelligence artificielle : une approche européenne sur l'excellence et la confiance*, p. 4

enseignant à Sciences Po, trois pistes de réflexion permettent de comprendre le retard pris par la France dans le développement de sa base industrielle et technologique.

Le premier, et le plus fondamental, est le manque d'anticipation des industriels. Effectivement, les grands industriels sont les moteurs des innovations et fédèrent autour d'eux des synergies en s'appuyant sur le tissu des petites et moyennes entreprises. Les jeunes pousses (*start up*) génèrent bien souvent l'innovation mais n'ont pas nécessairement les moyens économiques et financiers d'assurer immédiatement une montée en puissance. C'est par une association avec de grandes entreprises bénéficiant d'un plan de charge et d'une plus grande visibilité qu'elles pourront dynamiser leurs productions. Conséquence logique et seconde piste avancée par l'enseignant : il n'existe pas d'offre industrielle ayant atteint une masse critique. Par « masse critique », on peut entendre la capacité à générer ou capter une quantité suffisante de données pour développer l'algorithme. Il est clair que les États-Unis d'Amérique, Israël et la Chine bénéficient à cet égard d'une considérable avance avec leurs entreprises du numériques, les fameux *GAFAMI* (*Google, Apple, Facebook, Amazon, IBM*) et *BATX* (*Baidu, Alibaba, Tencent, Xiaomi*), mais aussi avec les moyens colossaux qu'ils allouent pour leur défense et leur sécurité.

Grâce aux données générées par leurs utilisateurs et clients, ces entreprises disposent de bases de données considérables qu'elles utilisent soit à des fins mercantiles soit à des fins d'apprentissage-machine, quand elles ne sont pas réquisitionnées par leurs gouvernements respectifs. On peut également entendre par « masse critique » la capacité de ces entreprises à évoluer sur le marché. On constatera que seules quatre jeunes pousses européennes figurent parmi les cent meilleures mondiales dans le domaine de l'IA. Comme le note la société de conseil *McKinsey & Company*, cela ne contribue donc pas à augmenter le *« rythme de la diffusion et des investissements »* en Europe. La nécessité de consolider la base industrielle et technologique de sécurité française se fait d'autant plus pressante que les services de l'État sont parfois contraints d'acheter leurs outils à l'étranger. Tel a été le cas de la direction générale de la sécurité intérieure qui, à l'été 2016, a conclu un contrat avec la société américaine *Palantir Technologies*[57]. Ce contrat temporaire aurait dû prendre fin en octobre 2018 avec l'arrivée du *Cluster Data Intelligence* développé par le groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres (GICAT). Mais en raison des retards pris sur le programme et face à la difficulté à trouver un intégrateur français en capacité d'unir les

[57] *Palantir Technologies* est une entreprise américaine spécialisée en science des données. Elle fournit des solutions techniques pour l'analyse et le traitement massif de données. Elle a reçu le soutien financier du fonds *In-Q-Tel*, détenu par la *Central Intelligence Agency* (CIA), dès le début des années 2000.

solutions sur la même plateforme, le marché avec *Palantir* est en passe d'être reconduit. Si l'on peut imaginer que le logiciel *Palantir* est sous la surveillance des services français, à l'affût de la moindre porte dérobée, sa mise en fonctionnement sur un réseau informatique, même fermé n'est pas une garantie totale, dans la mesure où une opération de maintenance effectuée par l'opérateur américain peut amener une fuite massive des données exploitées. Troisième et dernier élément avancé par l'enseignant, le cadre juridique français applicable au recueil de données offre moins de latitudes que les pays précités. Mais si cette exigence au regard des données personnelles retarde temporairement l'Europe, c'est le prix à payer pour sauvegarder nos libertés individuelles.

L'idée de souveraineté nationale peut paraître un peu restrictive en matière de maintien de l'ordre. Si effectivement on ne peut pas faire abstraction des doctrines nationales d'emploi des forces de l'ordre, rien n'empêche une entente des États pour le développement d'une IA commune. Cette IA pourrait faire l'objet d'un programme entre États européens, dans un cadre qui pourrait être initialement un cadre interétatique. Il permettrait une plus grande souplesse avant une intégration plus large, voire une communautarisation. Néanmoins, un tel programme ne peut réellement prendre forme que si une stratégie nationale est déjà en place. La France pourrait saisir l'opportunité d'ouvrir les débats et fédérer autour d'elle ses partenaires européens.

Une fois bien appréhendés ces éléments, il faut créer au plus tôt les conditions d'un dialogue entre industriels et puissance publique nationale. Plus précisément, ce dialogue doit être tripartite et continu puisqu'il doit convier tout à la fois les industriels, les donneurs d'ordre et les opérationnels. Ces derniers ont toute leur place car en tant qu'utilisateurs finaux il est nécessaire qu'ils participent au développement de la technologie. Ils sont d'ailleurs également les plus légitimes au retour d'expérience technique.

§2. L'exigence d'un travail en plateau, protection et ouverture à une interopérabilité européenne

La coopération entre ces trois acteurs est donc primordiale, au bénéfice d'un outil mûri et efficace. De la précocité du projet dépend également sa réussite. En effet, si le succès se construit sur la durée, c'est en posant rapidement la réflexion que l'on réduit les coûts d'un projet. Là où une modification, même mineure, peut entraîner une remise en cause globale du système lorsque celui-ci est arrivé en phase finale de production ; déterminer une doctrine

d'emploi au plus vite permet d'en faciliter la faisabilité technique auprès de l'industriel. Cette phase de conception est à différencier de la phase d'expérimentation en conditions réelles et de la phase de mise en œuvre opérationnelle, au cours desquelles une incrémentation et une mise à niveau du système sont toujours nécessaires. Le dialogue se doit donc d'être continu, et dépasse largement la seule phase de développement. Le travail en plateau est donc une garantie pour l'État afin d'optimiser le produit final, mais aussi de constamment garder la main pour éviter toute dérive de l'opérateur privé.

Ce genre de coopération prend un tour particulier à la lumière des conséquences de l'épidémie de coronavirus qui sévit en 2020. Deux grands mastodontes américains des technologies, *Google* et *Apple*, sollicités par l'appel général des gouvernements à faire émerger rapidement une solution, ont décidé d'unir leurs efforts pour développer une application de traçage des téléphones mobiles. Cette application, bien qu'éloignée de l'IA, sous-tend néanmoins les enjeux en termes de données personnelles et de respect des libertés fondamentales, puisqu'elle consiste en la collecte des données de géolocalisation et de co-localisation des mobiles entre eux. L'idée, louable, est d'identifier *a posteriori* les personnes avec qui l'individu porteur du virus a pu être en contact dans les jours passés. Le problème de cette initiative est le poids de ces acteurs privés dans la définition des critères techniques. Les solutions clefs en main proposées par ces industriels excluent les États du protocole de fonctionnement de l'application, des éventuelles applications connexes qui n'auraient pas nécessairement de lien avec la lutte anti-coronavirus, mais aussi du contrôle juridiques des données sauvegardées dont on peut penser qu'elles soient ensuite soumises à la juridiction américaine. On le comprend aisément, les États sont actuellement dans une situation complexe où, face à la crise d'ampleur qu'ils traversent, ils ne sont pas spécialement puissants dans la négociation. C'est dans ce genre de crise que l'on mesure la rivalité que les grandes entreprises technologiques opposent désormais aux États, pourtant souverains. La France a, pour sa part, pressé l'Institut national de recherche en informatique et en automatique de développer une application nationale, plus transparente pour la vie privée des Français, au regard des enjeux considérables de souveraineté numérique liés à une externalisation vers les États-Unis.

Le problème qui se pose donc est celui de l'exploitation de données par des acteurs privés. La question sous-tendue est celle de la protection de la vie privée, dans la mesure où les données obtenues sur la voie publique sont précieuses pour développer les algorithmes. Face à cette nécessité d'ouvrir l'accès à des opérateurs privés, il convient d'en préciser les contours. S'agissant de la production d'une IA comportementale, le premier élément relatif à la vie privée

est l'image permettant d'identifier un individu en un temps et en un lieu déterminés sur la voie publique. Mais en l'absence de fourniture de données biométriques au secteur privé, rien ne permet *a priori* d'identifier la personne. Et, à moins de considérer que la démarche comportementale est un élément de la vie privée, ces données font donc l'objet d'une certaine anonymisation. Tout l'enjeu est donc de fournir aux entreprises privées un matériau objectivisé, le plus respectueux des libertés publiques.

Très concrètement, en prenant l'exemple de la reconnaissance comportementale, on peut illustrer les bénéfices d'une telle coopération tripartite. Le donneur d'ordre (l'État représenté par le ministère de l'Intérieur) détermine, avec ses membres opérationnels issus des compagnies républicaines de sécurité et des escadrons de gendarmerie mobile, un cahier des charges portant sur les objectifs techniques et les exigences juridiques au regard du cadre légal et des libertés publiques. Cette première base de travail va permettre à l'industriel d'imaginer et proposer des solutions techniques. Et de là s'engage un dialogue entre les besoins des opérationnels et les possibilités techniques, sous le contrôle attentif du donneur d'ordre. En l'espèce, l'enjeu pour l'opérationnel est d'identifier les mouvements

Par conséquent, en jetant les bases d'une coopération tripartite, l'État peut espérer tirer le maximum économiquement parlant. Premièrement, il se préserve au mieux d'un dérapage des coûts en coordonnant le dialogue des acteurs dès la naissance du projet. Deuxièmement, il participe à son propre « retour sur investissement » dans la mesure où les financements consentis en amont aux jeunes pousses, vont créer les conditions d'un terreau favorable à leur initiative en matière de marchés publics. À cet égard, il faut préciser la difficulté que représentent les marchés publics de la sécurité et de la défense pour les entreprises. En effet, ils sont souvent étroits et nécessitent des investissements bien plus importants en matière de recherche et développement. Or, ces entreprises vivent et investissent sur leurs chiffres d'affaires, et deux solutions s'offrent à elles. Soit elles recourent à la *« dualisation de technologies civiles »*[58], c'est-à-dire qu'elles trouvent une application commerciale « tout public », ce qui pourrait intéresser des grands groupes privés particuliers tels que la SNCF dans sa mission de sécurisation des gares (la SNCF expérimente d'ailleurs à l'heure actuelle un algorithme d'IA pour détecter, grâce à la vidéoprotection, des colis ou bagages laissés sans surveillance). Soit ces entreprises proposent leurs produits à l'exportation, ce qui n'est pas sans poser problème lorsque les technologies en jeu sont considérées comme souveraines. Au

[58] Nicolas MAZZUCCHI, « Intelligence artificielle et industrie de défense, le grand défi », *R.D.N.*, n°820, 2019

demeurant, dans le cadre de l'IA appliquée aux opérations de maintien de l'ordre, cette souveraineté est à relativiser. L'exportation vers un pays partenaire du projet serait à la base de cette coopération. Cette dernière pourrait même s'appréhender dans un échange « données contre algorithme ». Il permettrait d'amorcer un cercle vertueux pour améliorer toujours plus le système algorithmique.

Une autre voie se dessine pourtant, à l'instar du ministère des Armées qui se doit de conserver ou d'acquérir de nouvelles capacités par le biais de programmes parfois longs et coûteux. En s'appuyant sur la direction générale de l'armement, les militaires expriment leurs des besoins opérationnels pour les traduire en spécifications techniques, synthétisées dans le cahier des charges. Face à l'inexorable accroissement des coûts en équipements militaires, l'État français peut formuler depuis 2017 des demandes de soutien financier auprès du Fonds européen de la défense (FED). Cette initiative permet de financer les projets communs entre pays de l'UE en matière de défense. Un tel fonds européen en matière de sécurité intérieure existe (FSI), mais il concerne surtout la protection des frontières extérieures et la coopération policière en termes d'échange de renseignement. Il pourrait être intéressant de le faire évoluer en le dotant de crédits d'investissements en R&D. Il permettrait ainsi de financer des solutions en IA au bénéfice de l'ensemble des pays contributeurs. Ici aussi la France pourrait mener les discussions quant au développement de ces projets. Quelle que soit la solution retenue, là encore se pose le problème de la fourniture de données à une entité privée.

On l'aura compris, la donnée est devenue l'enjeu essentiel de ce siècle. Face au phénomène de sa commercialisation, les États semblent être les mieux placés pour les protéger. Par leurs pouvoirs de régulation et de sanction, les États sont les plus à même de garantir leur préservation, notamment par le contrôle du juge. Plus en amont, il s'agit de se questionner les conditions juridiques dans lesquelles les donneurs d'ordres publics vont fournir des données au secteur privé pour l'entraînement d'algorithmes régaliens. Cet obstacle n'est pas, en fait, chose nouvelle ; et l'État s'en accommode d'ores et déjà très bien. En effet, il a de longue date saisi l'opportunité patrimoniale que représentaient les données qu'il collecte auprès des citoyens. Depuis la loi LOPPSI 2, l'État commercialise officiellement auprès de sociétés privées, les données personnelles de ceux qui immatriculent leurs véhicules. Selon le quotidien Le Parisien[59], la manne financière qui en résulterait s'élèverait à environ quatre millions d'euros par an. Cette commercialisation des informations contenues dans le fichier des cartes grises a

[59] http://www.leparisien.fr/week-end/l-etat-aussi-vend-vos-donnees-19-05-2015-4784563.php

soulevé fin 2013 des questions au Sénat à l'occasion de l'examen de la loi de finance 2014. Un amendement avait même été déposé, sans succès, car le projet de loi de finance avait été rejeté. Quoi qu'il en soit, le ministre avait insisté dans sa réponse sur la possibilité pour le propriétaire du véhicule de refuser la commercialisation de ses données en cochant une case. 35% des propriétaires l'avait fait en 2013. Si, en matière de maintien de l'ordre, il n'est absolument pas question de monétiser des données personnelles mais d'entraîner des algorithmes, l'obstacle juridique semble donc bien mince pour les défenseurs des libertés.

On peut donc légitimement imaginer qu'aucun obstacle sérieux ne se dresse à l'encontre de données anonymisées, fournies à des opérateurs privés triés sur le volet. C'est dans ce sens que l'Union européenne, fer de lance en matière de protection des données personnelles, travaille à une certification de la donnée traitable. Lors de la présentation de sa stratégie pour l'intelligence artificielle en février 2020, la Commission européenne a entendu défendre la voie d'une IA « éthique », plus respectueuse des libertés fondamentales que les applications développées ou en fonctionnement aux États-Unis ou en Chine. L'UE se concentre à l'heure actuelle sur quatre « secteurs critiques » : santé, transports, police et justice. Elle vise particulièrement les utilisations qui impliquent des effets juridiques et celles qui présentent, selon elle, directement ou indirectement des dangers mortels ou des risques de dégâts et de blessures. Une intelligence artificielle du maintien de l'ordre pourrait donc naître dans le cadre de données européennes partagées, labellisées, et respectueuses des libertés individuelles.

Cette certification pourrait, outre garantir le respect des droits aux citoyens européens, avoir des retombées commerciales implicites pour les entreprises. En effet, dans le cadre d'une dualisation de technologies civiles évoquée *supra*, les opérateurs privés ayant travaillé au développement d'IA régaliennes pourraient présenter leur labellisation comme un gage de sérieux, auprès de clients cherchant des solutions éthiques responsables.

Enfin, la mise en commun de données anonymisées permet une massification de la capacité d'entraînement des algorithmes, avec un bénéfice pour l'ensemble des États participants. Sans les priver pour autant du choix des données qu'ils fourniront, si d'aucuns les considèrent sensibles. C'est en ce sens que le préfet Vedel, coordinateur ministériel IA au ministère de l'Intérieur, propose d'ores et déjà de créer une banque nationale de données en recherche et développement afin d'entraîner les algorithmes dans le champ régalien. Il s'agit en premier lieu de valider l'approche, mais aussi de la fiabiliser car les données en sources ouvertes sont d'une moins grandes fiabilité et peuvent biaiser l'apprentissage machine.

§3. Développer et conserver un socle de compétences techniques en interne

Un tel recours à l'externalisation ne doit pas pour autant conduire à priver la puissance publique d'une maîtrise de la technologie en interne. Seulement, face aux difficultés posées par sa faible attractivité, l'État doit trouver et activer les leviers qui lui permettront de capter les ingénieurs issus des formations spécialisées : ingénieur en sciences des données, automaticien, cogniticien, développeur en intelligence artificielle. Cette difficulté de recrutement est en fait double. D'un côté, l'État fait face à une sérieuse concurrence du privé, avec la promesse des fonctions mieux rémunérées pour ce dernier, une plus grande souplesse d'emploi et des perspectives d'évolution quasi-infinies dans un secteur en pleine expansion. À cela s'ajoutent des entreprises qui bataillent dur pour débaucher des spécialistes chez le concurrent, ce qui complexifie l'attrait du public. De l'autre, l'État voit ses propres services se faire concurrence entre eux, ce qui pénalise encore plus le pourvoi des postes. Le recrutement de spécialistes est ainsi devenu, au fil du temps, un enjeu stratégique pour l'État quel que soit le ministère concerné.

En effet, on ne saurait que trop mal comprendre l'indépendance, dont pourrait se vanter l'État vis-à-vis d'acteurs privés, si celui-ci ne disposait pas en interne de personnels hautement qualifiés sur le plan de la technique. L'exigence d'un travail en plateau évoquée plus haut nécessite également pour l'État d'avoir dans ses rangs, non pas seulement des donneurs d'ordres, mais également des experts qui puissent sur un même pied d'égalité technique que les prestataires privés.

D'ailleurs une difficulté en termes de gestion et de pilotage semble s'être ajoutée à la difficulté conjoncturelle du recrutement pour l'État. Pour Henri Verdier, entrepreneur français et ancien directeur interministériel du numérique et du système d'information et de communication de l'État français (DINSIC), les pouvoirs publics manqueraient de souplesse et de transparence dans les décisions qu'ils prennent, du fait des nombreux intermédiaires qui échelonnent la chaîne hiérarchique[60]. Dès lors, les pouvoirs publics éprouveraient une réelle difficulté à diriger des projets en lien avec le numérique, ce qui a pour conséquence d'en compromettre leur réussite. Ce constat général est à nuancer en ce qui concerne l'Intérieur, une des administrations les plus matures, car les directions de la Police nationale et de la Gendarmerie nationale sont à l'initiative dans de nombreux domaines. L'une et l'autre sont en bonne voie pour réussir leur

[60] Henri VERDIER, « La transformation de l'État doit surtout être organisationnelle et managériale », *Les Échos*, 22 juillet 2019

transformation numérique (brigade numérique, dématérialisation des procédures *via* Néopol et Néogend, centre de lutte contre les criminalités numériques…).

Ce nivellement des compétences sera, quoi qu'il en soit, un préalable nécessaire à l'émergence d'une position ministérielle, puis interministérielle, forte. L'objectif final reste l'émergence d'un partenariat et d'une position européenne commune, dans lesquels la France pourrait jouer un rôle de premier plan. Ce genre de partenariat pourrait certainement conduire à mettre en commun les financements et les compétences techniques propres à chaque État, à l'image de la coopération interétatique européenne en matière de spatial. Le volet juridique portant sur les enjeux en termes de libertés publiques inhérent à l'existence d'une telle technologie pourrait également faire l'objet d'un dialogue avec le juge de Strasbourg, tout au long de son développement. Ce dialogue à double niveau, horizontal entre États partenaires et vertical avec la Cour européenne des droits de l'Homme, serait le gage d'un développement sain, « long-termiste » et maîtrisé. Cette maîtrise se retrouverait également dans les coûts de développement et de production, dans la mesure où un produit déjà conforme, tant opérationnellement que juridiquement, garantit les donneurs d'ordre d'un potentiel dérapage supplémentaire des coûts.

Enfin, la nécessité pour l'État de disposer en interne des compétences est primordiale, dans l'hypothèse d'application plus sensible de l'intelligence artificielle ; notamment si le législateur envisageait une intégration des données biométriques aux ressources d'entraînement des algorithmes, en vue de permettre la reconnaissance faciale dans des hypothèses limitées. Ces applications plus régaliennes ne pourrait évidemment pas faire l'objet d'un partage avec des opérateurs privés, qu'ils soient nationaux ou, pire encore pour nos libertés, étrangers. Ces développements techniques ne privent en revanche pas les États partenaires de développer un cadre juridique commun.

Ainsi, fondée sur une solide base industrielle et technologique de sécurité, et disposant en son sein de techniciens hautement qualifiés, la France disposerait de deux atouts de taille pour orienter une coopération européenne.

Chapitre 2 – UN CADRE JURIDIQUE À ADAPTER AUX MODALITÉS DE MISE EN ŒUVRE DE L'INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle peut ainsi être physiquement schématisée comme la somme d'un algorithme auto-apprenant[61], d'une base de données et d'une puissance de calcul. Nous écarterons la problématique de la puissance de calcul de notre recherche juridique, car au-delà de la question du traitement de masse des données, la quantification de cette puissance n'est pas en elle-même sujette à discussion juridique. Il n'en demeure pas moins que cette quantification de la puissance présente des enjeux, notamment éthiques et commerciaux, non négligeables tant pour les États que pour les opérateurs privés[62].

La ministre française des Armées, Mme Florence Parly, a très rapidement donné une orientation quant à l'exploitation des données recueillies par son ministère. *« Nous investirons d'abord dans les carburants de l'IA : c'est-à-dire les données et les capacités de calcul… Ces données ne seront plus perdues ou gaspillées faute d'outils pour les recueillir, les stocker ou les traiter… Nous prendrons le virage du cloud pour disposer des capacités de calcul et de stockage indispensables au développement de l'IA, sans compromettre la sécurité et la souveraineté de nos données. Il nous faudra décloisonner les données, les partager, en faire un actif stratégique de notre ministère »*[63]. Si le cadre dans lequel le ministère des Armées recueille, analyse et conserve les données obtenues sur ses théâtres d'opération extérieures est bien loin des canons dans lesquels l'action du ministère de l'Intérieur s'inscrit, ce dernier n'en démontre pas moins un intérêt aigu en témoignent l'existence d'un coordinateur ministériel IA et la création d'un cycle supérieur d'IA afin de penser ses applications tant gestionnaires qu'opérationnelles.

À l'heure actuelle, la France dispose d'un cadre juridique relativement protecteur en matière de numérique (Section 1). Néanmoins, il est nécessaire de le consolider pour permettre un usage raisonné et raisonnable de l'IA au regard des enjeux en matière de libertés individuelles (Section 2).

---

[61] Un algorithme auto-apprenant est défini par la CNIL comme un *« algorithme conçu de sorte que son comportement évolue dans le temps, en fonction des données qui lui ont été fournies »*. Ils relèvent également *« du domaine de recherche des systèmes experts »* : https://www.cnil.fr/fr/definition/algorithme

[62] Frank AUTRE, Kunal ARYA, Ryan BABBUSH, « Quantum supremacy using a programmable superconducting processor », *Nature*, n°574, 2019, p. 505-510 : l'entreprise américaine Google affirme avoir atteint la suprématie quantique. L'ordinateur quantique développé serait capable de résoudre en un peu plus de trois minutes une opération pour laquelle l'ordinateur le plus puissant actuellement disponible au monde mettrait une dizaine de milliers d'année.

[63] Florence PARLY, Discours « Intelligence artificielle et défense », ministre des Armées, Saclay, 05 avril 2019

Section 1 : Un cadre juridique protecteur des libertés en apparente phase avec l'IA

La protection des données personnelles et le traitement automatisé des données ne sont pas des problématiques nouvelles. Ces enjeux ont progressivement intégré le quotidien des citoyens, d'abord dans leurs usages privés personnels puis dans l'espace public. Le législateur est ainsi intervenu dès 1978 dans la grande loi structurante relative à l'informatique, aux fichiers et aux libertés. Puis les usages des nouvelles technologies ont largement diffusé dans l'espace public, notamment avec la mise en place de réseaux de vidéoprotection dans les lieux particulièrement exposés aux crimes et aux délits. Il faut donc s'intéresser à la régulation des données (§1) telle qu'elle a été classiquement envisagée, et à leur définition commune, avant de traiter l'encadrement normatif du traitement algorithmique, qui pour sa part a fait l'objet d'un renforcement constant (§2).

§1. La régulation des données : une problématique déjà ancienne

Les données personnelles ont fait l'objet d'une régulation dès 1978 en France avec la loi Informatique et Libertés, régulation approfondie par l'intervention des institutions européennes avec le règlement générale sur la protection des données (A). En outre, cette régulation des données est également la conséquence de l'action du code de la sécurité intérieure en matière de conservation des images issues de la vidéoprotection (B).

A. Les données à caractère personnel de la loi « Informatique et Libertés » au RGPD

Lorsque l'on se penche sur les enjeux juridiques qui entourent l'exploitation de l'intelligence artificielle à des fins de préservation de l'ordre public, il faut nécessairement se questionner sur la régulation qui est faite des données personnelles. Dès les années 1970, ces problématiques ont conduit les pouvoirs publics à en réglementer leurs usages, donc dégager des grands principes et définir les notions impliquées. L'article 2 de la loi n°78-17 du 06 janvier 1978 dispose que *« constitue une donnée à caractère personnelle toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »*. Bien que cette définition soit en elle-même déjà très large, la CNIL – qui est compétente pour veiller à la protection du citoyen contre tout usage abusif de données informatiques le concernant – lui donne un sens encore plus extensif. Dès lors, l'autorité administrative

considère que l'on ne peut surveiller un individu sur Internet sans recourir à l'exploitation de ses échanges, ses préférences exposées par des « *likes* » quand bien même ces éléments seraient publics, car ils renvoient irrémédiablement vers cette possibilité d'identification indirecte de l'individu.

L'Union européenne est venue parachever ce mouvement avec le règlement général relatif à la protection des données (RGPD). Dans la continuité de la loi de 1978, le texte européen a précisé à son tour les modalités de protection des informations *« se rapportant à une personne identifiée ou identifiable »* […] *« directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »*[64].

Ce faisant, le droit positif vient assurer une protection étendue des données que l'usager va – pourtant volontairement – diffuser sur un réseau électronique, potentiellement accessible de n'importe quel poste informatique mondial. Cette protection représente bien plus qu'une simple déclaration d'intention car elle est assortie de nombreux droits pour l'usager, qui se traduisent en obligations pour le fournisseur du service en ligne. On citera particulièrement le droit à l'information sur le stockage de ces données, les finalités de leur traitement par des outils algorithmiques ou encore le droit pour l'usager à modifier voire supprimer les données incorrectes conservées par le fournisseur dans ses fichiers.

Du fait de ces obligations, les fournisseurs de service en ligne doivent respecter un principe fondamental : celui de la minimisation. Le principe de minimisation vise à ce que les données à caractère personnel collectées soient *« adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »* (Art. 5, §1, RGPD). Ce faisant, le droit européen reprend à son compte les principes qui animaient déjà la loi française en vue de préserver la vie privée. Cette dernière a toujours prévu des conditions précises de collecte (finalités, proportionnalité, sécurité) et de conservation des données (durées limites) par les opérateurs privés.

Bien que très attentive à une protection stricte des données personnelle, l'Union européenne – comme la France d'ailleurs – a toutefois largement pris conscience du potentiel lié aux mines

[64] Article 4, Règlement (UE) 216-679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

informationnelles qui sont générées quotidiennement. En ce qui concerne les services propres des États membres de l'UE, ils participent eux aussi à la production de ces mines d'informations. La question de l'application du RGPD, et des obligations qui en découlent, aux fichiers de l'État aurait pu se poser. Cependant l'article 2 du RGPD vient explicitement exclure l'application du règlement au traitement de données à caractère personnel effectué *« par les autorités compétentes à des fins de prévention et de détection des infractions pénales »* (…) *« y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces »*. Les activités qui relèvent de la sécurité nationale demeurent donc l'apanage des États membres, et se trouvent en dehors du champ d'application du droit de l'UE. Néanmoins cette dernière ne cache pas sa faveur pour un partage approfondi des données entre autorités compétentes, et à cet égard elle encourage les États membres à faciliter le libre flux des données en vue de l'efficacité des services étatiques de police et de justice[65].

Cet intérêt de l'UE à développer une coopération sans cesse plus étroite, qui se matérialise ici par un fondement textuel, permet donc d'imaginer un échange massif de données entre pays membre en vue du développement d'une intelligence artificielle commune en matière de prévention des troubles à l'ordre public.

Est-ce pourtant à dire qu'aucune garantie démocratique n'entoure la création de fichiers de police par les États membres ? Non, il est ici un relais législatif, ou plutôt une exclusivité souveraine de l'encadrement des traitements en lien avec la sécurité publique. La loi « Informatique et Libertés » n'a donc pas été supplantée par le RGPD, et des mécanismes de contrôle certes indirects permettent au citoyen de s'assurer de la légalité qui entoure la mise à jour et l'exploitation des données nécessaire au traitement par les services de l'État. Nous reviendrons plus particulièrement dans cette étude sur les modes d'action de la CNIL et du juge.

B. Le code de la sécurité intérieure et le régime dual des images recueillies sur la voie publique

Les données ne doivent pas uniquement être considérées comme une production exclusive de l'individu. Ainsi, le code de la sécurité intérieure est venu encadrer les conditions dans lesquelles la puissance publique peut déployer des moyens de vidéoprotection. Il y a bien

[65] Article 4, Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 : *« Il convient de faciliter le libre flux des données à caractère personnel entre les autorités compétentes à des fins de prévention et de détection des infractions pénales »* […] *« y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces au sein de l'Union »* […] *« tout en assurant un niveau élevé de protection des données à caractère personnel. »*

là production de données, dans les images captées en temps réel sur la voie publique. Puisqu'il y a bien moyen d'identifier directement ou indirectement une personne physique à partir d'un ou plusieurs éléments qui lui sont propres, les enregistrements constituent en eux-mêmes des données à caractère personnel. Ainsi au regard des enjeux en matière de vie privée et de libertés, le législateur a pris le soin de placer les enregistrements *« utilisés dans des traitements automatisés ou contenus dans des fichiers structurés »*[66] sous le régime de la loi de 1978. Tous les autres enregistrements visuels de vidéoprotection font quant à eux l'objet d'un régime protecteur particulier. C'est la raison pour laquelle les conditions de mise en œuvre, d'enregistrement et de conservation de ces enregistrements hors traitement automatisé sont très précisément encadrées et leur non-respect sévèrement puni.

Le livre II du code de la sécurité intérieure contient ainsi un titre V exclusivement dédié à la vidéoprotection, dans lequel sont énumérés un nombre important de mesures visant à contrôler le déploiement de tels moyens et les personnes habilitées à les mettre en œuvre, et d'assurer une sanction pénale en cas de non-respect de ces règles (Art. L254-1 et suivants). Le régime général est celui de l'autorisation, et là encore sont prévues des conditions strictes en matière de conservation des enregistrements. Quand bien même une autorisation viendrait à prévoir un délai minimal de conservation des images, *« ce délai ne peut excéder un mois »*. En dehors des cas d'enquête de flagrant délit, d'enquête préliminaire ou d'information judiciaire, le législateur encadre donc fermement l'exercice rétroactif de la surveillance télévisuelle de la voie publique par la puissance publique.

À la lecture de ces articles, on comprend bien que cette dualité de régime de conservation, entre les enregistrements qui feront l'objet d'un traitement automatisé et ceux qui n'en feront pas, s'accompagne d'une exception pour les seconds. La possibilité que ces enregistrements non traités servent une enquête représente donc un intérêt supérieur à l'atteinte possible à la vie privée des gens qui apparaissent sur ces enregistrements conservés. On peut donc tout à fait imaginer que le législateur trouve un pareil intérêt supérieur dans l'exploitation de ces images à des fins d'apprentissage-machine, c'est-à-dire dans le but de créer une intelligence artificielle de prévention des troubles à l'ordre public.

[66] Art. L251-1, Code de la sécurité intérieure

§2. Un encadrement normatif du traitement algorithmique constamment renforcé

À nouveau, le développement d'algorithmes de traitement des données a fait l'objet d'une réflexion tant par les autorités européennes que les autorités nationales. On parle de traitement pour désigner l'ensemble des processus qui permettent de dégager un savoir, une connaissance, à partir de données brutes qu'elles soient à caractère personnel ou non. Le traitement algorithmique intervient dès lors que ces processus intègrent une ou plusieurs opérations automatisées appliquées à ces données.

Dès le début des années 2000, à l'occasion de l'examen de la loi pour la sécurité intérieure, le Conseil constitutionnel avait été saisi par des parlementaires sur le risque d'atteinte à la vie privée inhérent à la création de fichiers informatisés de police portant sur des données nominatives. Dans sa décision 2003-467 DC du 13 mars 2003, le Conseil écarte les arguments des requérants en considérant que de nombreux garde-fous préservent de ces fichiers d'éventuels mésusages par les forces de l'ordre. Par conséquent, il constate que *« la conciliation opérée par le législateur entre le respect de la vie privée et la recherche des auteurs d'infractions n'est pas manifestement déséquilibrée »*. C'est donc dans un mouvement assuré que les juges de la rue Montpensier ont permis aux autorités policières de massifier les fichiers, grâce notamment aux garanties apportées par la CNIL et la surveillance de l'autorité judiciaire. Il s'agissait donc d'un grand pas vers une meilleure connaissance des individus représentant ou ayant représenté une menace à l'ordre public.

À l'occasion de la transposition du RGPD, le Conseil constitutionnel a eu l'occasion pour la première fois de se prononcer sur les algorithmes auto-apprenants – qui voient leur structure évoluer en fonction des données qui leurs sont implémentées dans le temps. Les parlementaires à l'origine de la saisine soutenaient que l'exception prévue par le RGPD que constituait le recours exclusif aux algorithmes pour l'adoption de décisions administratives individuelles conduisait l'administration à renoncer à l'exercice de son pouvoir d'appréciation des situations individuelles. Le Conseil va donc poser trois conditions essentielles[67] pour permettre la mise en œuvre de cette exception à l'interdiction du profilage posée par le RGPD. En premier lieu, le traitement algorithmique et ses évolutions doivent être maîtrisés, et la manière dont le traitement a été mis en œuvre doit pouvoir être expliqué de manière intelligible à la personne concernée. En second lieu, cette décision administrative exclusivement fondée sur l'algorithme doit pouvoir faire l'objet d'un recours. Enfin, le traitement ne doit pas porter sur des données

[67] Cons. 69 à 72, Décision n°2018-765 DC du 12 juin 2018, Loi relative à la protection des données personnelles

qualifiées de sensibles, au rang desquelles on trouve notamment l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, les données génétiques, de santé, etc…

Comme le souligne une étude[68] produite par l'Institut d'aménagement et d'urbanisme sur la police prédictive, le Conseil constitutionnel vient ici renforcer la crainte à l'égard de ces algorithmes qui se proposent de changer les modes de fonctionnement des administrations. Il pointe indirectement la responsabilité des concepteurs dans l'explicabilité de ces décisions, qui sont dans une très large mesure susceptibles d'emporter d'importants effets juridiques à l'égard des administrés. Nous sommes donc bien au début d'une nouvelle ère juridique, où les algorithmes auto-apprenants vont progressivement intégrer de plus en plus de données contenus aujourd'hui dans des fichiers détenus par les administrations de l'État.

Ce croisement impliquera le respect de règles juridiques identiques à celles obligatoires à la création d'un nouveau fichier. Il faudra suivre la lourde et nécessaire procédure qui passe notamment par un avis de la CNIL. Une voie détournée permet néanmoins d'éviter cette lourdeur procédurale, il s'agit d'interroger les fichiers sur la présence ou non d'informations sur un individu sans avoir un accès direct au contenu. Il appartient alors au service réclamant d'adresser une demande de communication des éléments au service responsable du traitement du fichier. Dans l'hypothèse où les développements technologiques conduisent à un impératif de communication en temps réel des informations contenues dans ces fichiers, alors il faudra adapter leurs modes d'interrogation, quitte à faire cette demande de croisement et suivre la procédure classique avec un passage pour avis devant la CNIL

Face à ce travail normatif et jurisprudentiel encore imparfait qui cherche à garantir et préserver les libertés des citoyens, il convient de s'attarder un peu plus sur les points juridiquement controversés liés à l'émergence de systèmes apprenants en matière de prévention des troubles à l'ordre public.

[68] Lien vers l'étude : https://www.iau-idf.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf

Section 2 : La nécessité de consolider ce cadre juridique : se défaire des « angles morts »

Consolider ce cadre juridique n'est pas seulement une question de forme, c'est avant tout une question de fond dans la mesure où la donnée est au cœur de l'action policière[69]. Dès lors, un paradoxe émerge quant à la manière dont ce traitement qui en est fait : manuellement ou automatiquement.

Alors que l'exploitation massive des données est plus que jamais d'actualité, faisant courir le risque d'usages liberticides et attentatoires à la vie privée de ces nouveaux outils, il est indispensable d'évaluer les failles et d'ouvrir des pistes de réflexion. Là où l'essayiste Paul Virilio envisage l'époque actuelle, où la surveillance de masse se fait de plus en plus prégnante, comme un *« monde sans angle mort, constamment sous contrôle »* et où *« les capacités instantanées de soumission et de contrôle sont telles »* (…) *« que le totalitarisme n'était au fond qu'un accident local à côté de celui qui peut survenir »*[70]. L'auteur évoque à cet égard l'émergence d'un *« globalitarisme »*, c'est-à-dire un monde totalitaire dans lequel la surveillance de masse est l'instrument principal du pouvoir. Il convient justement d'explorer les angles morts démocratiques, liés à la mise en œuvre d'une intelligence artificielle de l'ordre public, pour lesquels l'absence de réponse conduirait à des dérives liberticides.

L'étude de ces angles morts vient ouvrir des perspectives nouvelles sur une collecte et une exploitation responsables des données. Le droit de l'Union européenne est venu faciliter la répartition des compétences entre secteurs privé et public (§1), laissant une marge suffisamment large d'appréciation à chaque État. Ce dernier est en effet pressé par les développements technologiques (§2) qui le conduisent à adopter des réponses propres à sa situation. La nature même des données en jeu en matière de prévention des troubles à l'ordre public doit nous conduire à s'interroger sur le degré de délégation du processus de création des algorithmes dans ce domaine (§3).

[69] *Ibid.*
[70] *Op. cit.* note 26, p. 20

§1. Une répartition des compétences entre secteurs privé et public facilitée par le droit de l'UE

Si le principe repose actuellement sur une interdiction du traitement des données sensibles par les opérateurs privés (A), des exceptions limitatives et conditionnées demeurent (B).

A. Le principe : une interdiction du traitement des données « sensibles »

La première des questions est celle du cadre juridique dans lequel des données pourraient être fournies, à des opérateurs privés qui viendraient se positionner en partenaires de la puissance publique. Si la loi Informatique et Libertés et le RGPD viennent encadrer aussi bien la collecte, la conservation et la qualité des données personnelles que leur traitement, ces données proviennent de l'utilisation par l'individu d'un service proposé par un acteur économique privé. Qu'en serait-il de cette protection juridique, pour des données à caractère personnel fournies par l'État à des opérateurs privés, dans le but de développer des algorithmes apprenants ?

Il est en fait tout à fait possible pour les services de l'État de fournir certaines données à caractère personnel, dès lors qu'au préalable le consentement des personnes concernées a été recueilli. Tel est déjà le cas, nous l'avons vu, pour les données d'immatriculation des véhicules transférées à des centres de contrôle technique ou vendues des garagistes et des détaillants en pièces automobiles. Tel est également le cas pour certaines informations relatives à des examens ou concours nationaux comme le peuvent être les résultats du baccalauréat transmis par les rectorats à la presse. Il existe donc déjà de nombreuses hypothèses de transfert de données à caractère personnel par les autorités publiques auprès d'opérateurs privés, à des fins de traitement. Le transfert de ces données conduit dès lors les opérateurs privés à leur appliquer un régime de protection élevé, tel qu'il est prévu par la loi Informatique et Libertés et le RGPD.

Pour autant, les données présentées ici sont assez éloignées de notre sujet sur la prévention des troubles à l'ordre public en manifestation. Et le sujet d'un transfert de données au privé dans ce domaine est d'autant plus sensible que le RGPD consacre une interdiction de principe relative au traitement des données à caractère personnel dites « sensibles ». Il y a donc une catégorie dans la catégorie, qui vise explicitement les données dont le traitement conduirait à révéler *« l'opinion raciale ou ethnique, les opinions politiques, les convictions religieuses ou*

philosophiques ou l'appartenance syndicale » (…) *« des données génétiques, des données biométriques »* ou encore *« des données concernant la santé »* (…) *« la vie sexuelle ou l'orientation sexuelle »* (Art. 9). Tout responsable de traitement établi dans l'UE, ou tout responsable de traitement hors UE qui mettrait en œuvre des traitements visant à fournir des biens ou services à des citoyens européens, ou servant à profiler des citoyens européens, y est donc soumis. Or, la manifestation est le lieu d'expression publique des idées, là où justement le citoyen exprime sa sensibilité qu'elle soit politique, syndicale, voire parfois religieuse. La captation d'images à des fins de traitement lors d'un défilé syndical conduirait ainsi à cataloguer des individus, donc largement atteindre ce principe d'interdiction du traitement des données personnelles sensibles. La puissance publique ne peut donc pas, à première vue, transférer en l'état ce type de données sensibles à des opérateurs privés. Le Conseil d'État l'a d'ailleurs rappelé récemment à l'égard de l'usage de drones par la préfecture de police de Paris[71] pour veiller au respect des mesures de déconfinement post-Covid-19. En l'absence d'arrêté pris après avis de la CNIL, la préfecture de police ne pouvait régulièrement pas déployer ces appareils, sans dispositif technique rendant impossible l'identification des personnes filmées.

Une première alternative s'offre donc à l'État s'il souhaite malgré tout recourir au privé. Cette alternative se présente sous la forme d'un transfert de données anonymisées. Cette hypothèse séduisante permettrait au service de l'État d'opérer un transfert sur des données dont les éléments caractéristiques sensibles seraient effacés. Les modalités d'une telle anonymisation doivent encore être discutées pour en déterminer les contours. Mais d'ores et déjà le floutage des visages, des inscriptions que pourraient porter de manière visible des manifestants qui permettrait d'identifier leurs idées, ou encore l'anonymisation des dates, heures et lieux durant lesquels la manifestation a eu lieu seraient autant de pistes permettant une exploitation de ces données par des opérateurs privés.

En ce sens, les institutions européennes réfléchissent à une certification des données traitables[72] ; ce qui permettrait d'avoir un régime commun aux autorités policières de l'UE quant à la régularité de tel ou tel procédé. Car si l'idée est intéressante, il doit y avoir suffisamment de garanties techniques en vue de prévenir une ré-identification des individus, qui pourrait avoir lieu par recoupement à l'occasion du traitement. Cette première critique

[71] Conseil d'État, ordonnance du 18 mai 2020, *Ligue des droits de l'Homme et autres*
[72] https://www.lesechos.fr/tech-medias/intelligence-artificielle/intelligence-artificielle-bruxelles-promet-un-encadrement-bien-reel-1173157

s'adjoint d'une difficulté qui pourrait émerger, sur ce qui est de déterminer à 27 les données intéressantes à certifier.

B. Des exceptions limitatives et conditionnées

En dehors du consentement exprès de l'individu au traitement de données personnelles le concernant, l'État peut valablement recourir au traitement informatisé de données non anonymisées pour des motifs *« d'intérêt public important »*. L'article 9 du RGPD vient en effet consacrer une exception de taille pour l'exploitation de masse de données personnelles, dès lors que celle-ci est proportionnée à l'objectif poursuivi et que le droit de l'Union ou le droit de l'État membre prévoit des *« mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée »*.

Il existe donc une très large marge d'appréciation pour les États membres quant à ces mesures de protection. L'existence de la CNIL, autorité administrative indépendante, est un des gages du respect des droits et libertés fondamentales ; de même que peut l'être le juge des référés.

Le droit de l'Union européenne vient donner un certain nombre d'éléments entourant les conditions d'un tel traitement informatisé. On trouve ainsi dans le RGPD cinq règles générales qui touchent à la licéité du traitement, sa transparence, l'interdiction sauf exceptions mentionnées *supra* de l'intégration de données sensibles, un droit à l'opposition par l'individu concerné, et le droit de ce dernier à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques ou l'affectant de manière significative. Ces règles générales sont assez largement aménagées par la directive (UE) 2016/680 relative au traitement des données personnels à des fins de prévention et de détection des infractions pénales.

La loi Informatique et Libertés a intégré cette directive dans ses articles 87 et suivants, autorisant désormais les traitements de données personnelles sensibles pour le compte de l'État sous trois conditions cumulatives (Art. 87 et 88) :

- le traitement de telles données ne doit avoir lieu qu'en cas de nécessité absolue ;

- son recours est conditionné à l'existence de dispositions législatives et réglementaires ;

- dans le cas d'une disposition réglementaire, elle doit faire l'objet d'un avis de la CNIL.

Sous le respect de ces conditions, l'État peut donc recourir à un prestataire privé pour l'exercice du traitement automatisé de données personnelles sensibles. L'article 90 dispose à cette fin que le responsable du traitement (ou son sous-traitant), agissant pour le compte de l'État, devra toutefois réaliser une étude d'impact qu'il adressera à la CNIL.

Le droit de l'UE s'inscrit donc dans une approche résolument libérale de la donnée. Il se satisfait des garanties posées par la législation de chacun des États membres, quand lui ne régule pas. La donnée, même sensible, n'est qu'une marchandise comme une autre, autorisée à la libre circulation sous le couvert de ces garanties. Si celles-ci peuvent paraître légères au regard des libertés fondamentales, il faut reconnaître qu'en toute hypothèse les opérateurs privés n'ont pas attendu l'État pour compiler en masse des bases de données en vue de l'apprentissage-machine.

§2. Une temporalité technologique pressant le législateur

Le législateur est confronté à une double exigence qui le presse dans sa régulation. En premier lieu, la massification des données en accès libre le conduit à repenser son action protectrice (A). Il en est de même au regard de la diversification des sources de données (B).

A. La massification des données en accès libre

Chaque seconde à travers le monde, environ 29 000 gigaoctets d'informations sont publiées sur Internet. Dans cette masse de donnée, qui apparaît donc comme un flot intarissable à la disposition du plus grand nombre, le flux photo et vidéo intéresse particulièrement les opérateurs privés. Se poser la question de réguler le cadre dans lequel ces opérateurs évoluent ne doit pas nous conduire à ignorer que ceux-ci travaillent déjà sur des données qui y échapperont. La quantité de données accessibles en sources ouvertes sur Internet permet d'ores et déjà de développer les algorithmes apprenants.

L'une des applications les plus intéressantes de l'IA en maintien de l'ordre est l'analyse comportementale. Bien moins intrusive que peut l'être la reconnaissance faciale, elle a pour objectif d'anticiper les comportements au regard des expressions corporelles, et même faciales. Elle est moins intrusive dans la mesure où l'analyse de l'expression faciale ne nécessite pas de comparaison avec tels ou tels bases de données, fichiers de police, biométriques ou non. En cela elle préserve le citoyen d'un contrôle d'identité permanent, comme celui qu'impliquerait une reconnaissance faciale systématique et en temps réel. Cette analyse comportementale trouve

d'ores et déjà à s'appliquer de manière expérimentale dans le tramway de Nice, sous le contrôle de la CNIL. L'entreprise *Two-i* propose à l'exploitant d'identifier tout changement émotionnel des usagers, afin de prévenir au plus tôt les comportements déviants des passagers. Or avec cet exemple, on comprend que le développement d'un tel outil peut uniquement reposer sur la multitude des données accessibles librement sur Internet. Le secteur privé n'a donc aucune dépendance à l'égard des services de l'État quant au besoin d'accéder à des bases de données. Il n'y a alors aucun contrôle indirect de l'État sur la capacité du secteur privé à développer des algorithmes

La vraie question est donc celle du droit à appliquer pour l'exploitation de données rendues publiques, à des fins d'apprentissage-machine. Car à nouveau deux questions se posent, et la première amène à déterminer si, en l'absence d'un tel cadre juridique, les opérateurs privés pourraient recourir à un traitement automatique de l'ensemble des flux Internet. Ainsi, en l'absence d'exercice du droit de rectification et quand bien même les données concerneraient des citoyens européens, leur consentement serait présumé du fait de la publication de leurs données en ligne. Là où, dans le monde numérique, les capteurs sont omniprésents, la CNIL a souligné de longue date la forte asymétrie entre ceux qui contrôlent les algorithmes et les données qui les alimentent, et les individus qui souhaitent voir leurs droits respectés. À l'inverse, la seconde question conduit à réfléchir à une stratégie de sélection des données, voire à une certification, par des services de l'État compétents et sous le contrôle des autorités classiques en la matière (CNIL, Défenseur des droits), sorte de garantie qui viendrait s'ajouter au consentement individuel pour le traitement automatisé en ligne.

Quoi qu'il en soit, cette massification des données va de pair avec une diversification des sources qui les produisent.

B. La diversification croissante des sources de données

Cette diversification en matière administrative est tout autant le fait d'avancées techniques que d'une rationalisation du renseignement. Sur ce second point, le domaine administratif a connu une nette expansion à la suite des attentats de 2015. Là où, jusqu'en 2015, les services de renseignement ne pouvaient recourir qu'à trois outils légaux, la loi Renseignement a complété ce cadre juridique afin d'en faciliter leur travail. Ainsi à côté de l'accès aux fichiers de police, aux interceptions de sécurité et au recueil de données techniques de connexion (depuis 2018 autorisé en temps réel), les services de renseignement peuvent

désormais recourir à des techniques spéciales d'enquête inspirées de la police judiciaire. On note ainsi le recours autorisé à des *IMSI catchers*, qui simulent une borne téléphonique mobile afin d'en écouter les conversations qui transiteraient par elle ; technique ô combien intrusive pour les tiers qui verraient leurs appels écoutés par la même occasion.

Pour Florian Vadillo, il ne faut pas pour autant considérer que ces nouvelles techniques font l'objet d'une exploitation débridée. À l'instar des mesures décidées dans un cadre judiciaire, elles sont mises en œuvre sous le contrôle du juge, à peine de nullité des procès-verbaux qui seraient dressés pour des faits relevés à l'occasion de ces mises en œuvre. D'autre part, il ne faut pas ignorer que des problématiques financières et technologiques demeurent. Les moyens accordés aux services de renseignements, quand bien même ils ont été fortement revalorisés depuis 2015, ne permettent pas des captations tous azimuts. Il y a toujours un jeu de priorités qui s'installe dans le travail de ces services.

Si l'intelligence artificielle pourrait ainsi jouer un rôle prépondérant en matière de détection de signaux faibles, elle pourrait également se nourrir des données collectées dans ce cadre strictement contrôlé, aux fins d'alerte pour les manifestations sur la voie publique.

La diversification des données touche également aux avancées techniques. Si nous nous sommes jusqu'alors concentrés sur les données textuelles et audiovisuelles, de nombreuses autres sources pourraient venir enrichir la connaissance sur les individus. On peut ainsi citer les données ADN, odontologiques ou encore olfactives, qui intègrent le champ plus large des données biométriques, propres à chaque individu. Le sujet est particulièrement sensible, et suit la même logique que la problématique de la reconnaissance faciale où il s'agit de faire la différence entre la détection faciale et la reconnaissance faciale. La première consiste à détecter le visage puis en déterminer algorithmiquement les expressions afin d'en tirer une conclusion sur le comportement de l'individu. On peut appuyer ou remettre en cause cette hypothèse en ajoutant des critères, comme par exemple un changement de démarche ou des gestes particuliers. La seconde vise à détecter le visage puis d'en comparer les caractéristiques avec les bases de données biométriques. Les outils sont donc les mêmes mais la finalité est différente, et l'impact sur les libertés fondamentales n'est pas le même. Dans le premier cas il s'agit de décoder les expressions et gestuelles communes à tout individu (il demeure ainsi anonyme), dans le second cas on peut y voir un contrôle d'identité qui se prolongerait autant que l'individu demeure dans le champ de la caméra. Il faut donc rapidement préciser les contours de telles

utilisation, afin d'offrir au plus vite au citoyen une sécurité juridique sur un tel usage des réseaux de vidéoprotection.

Quoi qu'il en soit, il est pour l'instant difficile d'envisager le soutien de l'UE en matière de reconnaissance faciale. Lors de la présentation de la stratégie européenne en matière d'IA début 2020, les commissaires se sont montrés particulièrement réticents à l'égard d'une telle technologie. Tout juste ont-ils esquissé l'idée d'un débat sur les circonstances qui pourraient justifier l'utilisation de la reconnaissance faciale dans les secteurs qualifiés de « critiques », au rang desquels on trouve la santé, les transports, la police et la justice.

§3. Vers une délégation totale au privé de la création des algorithmes ?

La question de la répartition des compétences est d'autant plus primordiale que des acteurs privés sont amenés à travailler sur ces données personnelles, et même des données sensibles. Évoquant la détection faciale et l'analyse comportementale, les entreprises qui mettent d'ores et déjà en œuvre des solutions pour les collectivités (tramway de Nice) manipulent quotidiennement des données biométriques. Ces dernières sont définies par la CNIL comme des *« caractéristiques physiques ou biologiques permettant d'identifier une personne »*. Si dans ses attributs, le visage ne fait aucun doute sur cette qualification, comment garantir que les expressions faciales sont un critère personnel et déterminant d'identification de l'individu ? De même pour le comportement et la gestuelle : peut-on considérer que ces éléments sont extérieurs à la personne, et qu'ils peuvent donc faire l'objet d'un traitement automatisé direct par un opérateur privé, sans plus de besoin de les anonymiser ?

Deux solutions s'offrent aux autorités quant à la répartition des compétences. La première, la plus « libérale », consisterait dans le développement d'une plateforme commune à la puissance publique et aux partenaires privés, à l'image du projet Artemis initié par le ministère des Armées. Il s'agit de fédérer les industriels de la défense, les jeunes pousses innovantes et le donneur d'ordre (service en charge de la conception et du suivi, en l'espèce la direction générale de l'armement) pour développer de nouvelles solutions sur un plateforme sécurisée, tout en bénéficiant d'un accès privilégié et sécurisé aux ressources en données du ministère. L'objectif à terme est d'obtenir des solutions opérationnelles recourant à l'IA, au profit des utilisateurs sur le terrain. En cela, les bases de données sont valorisées selon des approches différentes, propres à chaque partenaire, ce qui est favorable à l'innovation. En cela la puissance publique bénéficie

de la variété des expertises et des imaginations dont elle ne dispose pas nécessairement en interne.

La seconde solution, plus restrictive, consiste à tout développer en interne, ce qui est extrêmement gourmand en ressources pour les ministères, pour un résultat pas plus immédiat *a priori*. Mais une hypothèse intermédiaire pourrait trouver sa place, dans une coopération raisonnée, fondée sur la qualité des données. La création d'une telle plateforme pourrait servir à fournir des données strictement anonymisées dans le but de de développer une première mouture de l'algorithme apprenant. Puis, par la suite, de nouvelles données non-anonymisées pourraient y être incrémenté directement par les services de l'État. Cette solution intermédiaire permettrait dès lors de ne pas fournir les données les plus sensibles aux opérateurs privés. Conséquence logique, il sera donc nécessaire de disposer et de conserver un haut niveau d'expertise en interne pour continuer à développer l'algorithme, à partir d'une architecture de base modelable fournie par le privé.

Cette exigence protectrice irrigue la loi du 20 juin 2018 relative à la protection des données personnelles. Ainsi, au regard du traitement par un sous-traitant dans le cadre de la prévention et de la détection des infractions pénales, la loi lui oppose une obligation de moyen quant *« à la mise en œuvre de mesures techniques et organisationnelles appropriées, de manière que le traitement réponde aux exigences du présent chapitre et garantisse la protection des droits de la personne concernée »* (Art. 30). C'est un minimum à exiger du partenaire privé, et une nécessité compte tenu de la difficulté à rendre parfaitement anonymes des données.

En l'état actuel du cadre juridique, le choix est laissé à la discrétion de la puissance publique quant aux modalités de cette répartition des compétences. La loi Informatique et Libertés, modifiée par l'ordonnance n°2018-1125, vient implicitement autoriser le traitement automatisé des données personnelles nécessaires à l'authentification ou au contrôle de l'identité des personnes, mêmes les plus sensibles (génétiques et biométriques), par le secteur privé dès lors qu'il opère *« pour le compte de l'État, agissant dans l'exercice de ses prérogatives de puissance publique »* (Art. 31 et 32 LIL). L'exigence européenne de textes internes encadrant l'action d'opérateurs agissant pour le compte de l'État est donc accomplie. Leur recours dans le cadre des activités qui intéressent la sécurité publique et la prévention des infractions pénales est donc expressément prévu. Ce sera essentiellement la confiance accordée aux opérateurs privés et les garanties que ces derniers apporteront en termes de protection des données confiées que dépendra l'étendue des compétences déléguées par l'État en matière de création algorithmique.

Enfin, cette réflexion ne doit pas nous conduire à ignorer que bien des algorithmes n'utilisent pas de données personnelles. Ainsi, ceux qui ont pour objet la détection d'objets peuvent tout à fait faire l'objet d'une délégation complète au secteur privé. Tel pourra être le cas pour les algorithmes dont l'objectif sera d'identifier les objets et leurs influences et interactions sur les individus.

TITRE II – UN DÉVELOPPEMENT TECHNOLOGIQUE À ENCADRER

Le développement d'une technologie dans le domaine sensible du maintien de l'ordre nécessite d'infinies précautions. Il s'agit d'en maîtriser les implications, et l'exemple des données en témoigne : il y a une opportunité évidente au croisement des fichiers de police, mais un danger pour les libertés s'ils ne sont pas mis à jour régulièrement. Et la mécanique froide et implacable de l'algorithme n'a pas nécessairement le recul sur les données qu'elle traite. Ainsi, c'est un équilibre général qu'il faut trouver entre les fins légitimes poursuivies et les mesures engagées pour ses buts.

Le risque est évidemment de réaliser le rêve du libéral britannique Jeremy Bentham et de son panoptique qui, par la surveillance totale qu'il impose, soumet l'individu à une intériorisation de l'interdit. C'est l'enjeu majeur de l'IA du maintien de l'ordre : ne pas dériver en un panoptique des temps modernes.

Il faut donc, dès la conception, intégrer les prérequis structurants à une intelligence artificielle raisonnée du maintien de l'ordre (Chapitre 1). Puis, il faut s'interroger sur les protections qui entourent les cas possibles de mésusages : c'est toute la réflexion sur les garanties juridictionnelles et non juridictionnelles qui devront accompagner la mise en œuvre de cette IA (Chapitre 2).

Chapitre 1 – LES PRÉREQUIS STRUCTURANTS À UNE INTELLIGENCE ARTIFICIELLE RAISONNÉE DU MAINTIEN DE L'ORDRE

Ces prérequis structurants trouvent leur source dans la recherche d'une efficacité opérationnelle qui ne soit pas dénué d'éthique (Section 1). La confiance qui sera accordée à cette intelligence artificielle du maintien de l'ordre, et donc le succès de sa mise en œuvre opérationnelle, dépendra ensuite de deux éléments fondamentaux : la robustesse du système (Section 2) et l'explicabilité qu'elle devra réaliser (Section 3).

Section 1 – La recherche d'une efficacité opérationnelle dans un cadre éthique

Deux maîtres-mots ont guidé la rédaction du rapport Villani : l'efficacité et le pragmatisme. Tous deux servent en fait à qualifier l'essence même de l'intelligence artificielle, et en cela son développement ne peut en faire fi. L'application de solutions en IA dans les opérations de maintien de l'ordre ne doit donc pas conduire à autre chose qu'à un résultat efficace et pragmatique, sous peine d'en condamner son utilisation. Les difficultés que rencontrent les forces de l'ordre, dans l'exercice de leur mission de maintien de l'ordre au regard de la multiplicité des enjeux en termes de politique, d'opinion et de libertés publiques, ne leurs laissent pas le loisir d'une solution technologique inadaptée ou incomplète.

L'efficacité opérationnelle de l'IA au service des opérations de maintien de l'ordre passera par une catégorisation des hypothèses d'usages facilitant la compréhension situationnelle (§1). Par-delà le cadre légal existant, ces cas d'utilisations doivent d'ores et déjà faire l'objet d'une réflexion éthique (§2) afin de guider leurs mises en œuvre.

§1. Catégoriser les usages pour faciliter la compréhension situationnelle

Quatre cas d'usage permettent de synthétiser les apports opérationnels de l'IA. Chacun d'eux s'inscrit dans cette double exigence d'efficacité et de pragmatisme et se marie avec les objectifs sans cesse rappelés de modernisation de l'action publique. Si souvent, cette modernisation de l'action publique rime avec rationalisation des dépenses publiques, le recours

à l'IA fait ici d'une pierre deux coups. Le recours aux algorithmes, par les autorités politiques et les forces de maintien de l'ordre dans un environnement budgétaire contraint, valide également une approche économique de cette efficacité opérationnelle.

Aussi le premier usage qui puisse être fait de l'IA concerne l'automatisation d'un certain nombre de tâches qui, réalisées par l'homme, sont coûteuses en temps et en personnels. L'analyse en temps réel de l'ensemble du flux audiovisuel capté sur une manifestation à la recherche de tout indice de dérapage est à cet égard fastidieuse et rébarbatif. Sans d'ailleurs plus de réelles garanties d'une meilleure anticipation par les agents situés dans les postes de commandement. Ces techniques d'analyse, tant en reconnaissance d'objet qu'en identification de mouvements de foule et détection comportementale, se présentent donc comme une solution applicable à très court terme. Avec des résultats quasi-immédiats au regard des expérimentations menées dans le tramway de Nice. Cette automatisation pourrait trouver une utilité dès lors que la reconnaissance faciale serait adoptée. Dans la mesure où l'algorithme comparerait les caractéristiques des visages qu'il identifie avec les bases de données biométriques auxquelles il est relié, il pourrait faire émerger d'une part les profils inconnus des bases, de l'autre les profils qui feraient l'objet d'une interdiction judiciaire de manifester, ou d'une assignation à résidence.

Le second type d'application, déjà évoqué dans cette recherche, réside dans la détection d'anomalies. Il faut ici se poser la question du seuil de référence puisqu'il faut bien un élément de comparaison, décrivant une situation « normale » en manifestation. Ainsi il pourrait être envisagé de proposer une détection d'anomalie à deux niveaux. L'une par rapport à la situation en temps réel des comportements de la foule. L'autre par rapport à des manifestations passées, ce qui fait appel au travail d'apprentissage par l'algorithme sur le long terme. Ce deuxième niveau semble donc plus sûr dans une logique d'aide à la décision. À titre d'exemple, l'IA pourrait porter à l'attention des décideurs les éléments d'une foule qui, hors de la portée visuelle des forces à pied, commenceraient à s'armer ou revêtir des effets en vue d'un affrontement direct. Ce travail algorithmique pourrait s'accompagner d'une priorisation des événements, si d'aventure d'autres manifestants commençaient à adopter la même attitude, mais cette fois-ci dans un mouvement de convergence organisé, comme savent en construire certains groupes anarcho-libertaires.

Une troisième application, que l'on peut considérer comme dérivée de la détection d'anomalie, est l'identification de faux. Dans l'hypothèse d'une mise en œuvre de la reconnaissance faciale,

l'IA pourrait faire ressortir les profils d'individu faisant l'objet d'un maquillage, d'un déguisement, notamment à l'égard de ces fauteurs de troubles qui infiltreraient les cortèges ou de personnes inscrite au Fichier des Personnes recherchées (FPR) faisant l'objet d'une interdiction judiciaire de manifester ou d'un mandat de recherche.

Enfin et surtout, par cette capacité d'agrégation massive des données et de traitement des signaux faibles dans la foule, l'IA pourrait dresser un panorama des corrélations et des liens relationnels entre les individus qui la constituent. Sur la durée d'une manifestation, l'IA pourrait relever les points géographiques d'intérêt du cortège qui nécessitent une attention particulière du décideur, ou encore les interactions entre individus qui sortent de l'ordinaire d'une manifestation (échange d'objets en vue d'affrontements, proximité et échanges répétés entre individus connus pour des faits de violence, migration de ces individus vers des points sensibles du cortège).

Par conséquent, à côté du gain de temps dégagé par l'automatisation de certaines tâches, et donc d'une réorganisation des effectifs sur d'autres qui s'y prêtent moins, l'IA représentera un moyen incontournable d'aide au commandement. La gestion d'une opération de maintien de l'ordre, quelle qu'elle soit, nécessite une décomposition en actions intermédiaires et une priorisation de celles-ci, qui seront largement facilitées par ces quatre approches. Indéniablement l'intelligence artificielle deviendra la pierre angulaire de l'appréciation et de la gestion de ces priorités. En cela, elle apporte au décideur des clefs de compréhension froides et rationnelles, qui lui permettent une mise à distance. Le décideur dispose donc d'une marge de manœuvre supplémentaire, autorisée par une prise en compte complète des intérêts en jeu.

Au demeurant, comme tout outil d'aide au commandement, la mise en œuvre de l'intelligence artificielle nécessite de s'inscrire un cadre éthique structuré. Cette exigence d'éthique dans l'action policière est d'ailleurs l'un des axes majeurs de l'exécutif en place.

§2. Une réflexion éthique à intégrer

Cette réflexion éthique devra se fonder sur des structures multilatérales, favorables au consensus (A). La question fondamentale qui se posera est celle des moyens de programmer l'éthique par conception (B).

A. Pour un développement des structures de réflexion

Les accusations de violences par certains membres des forces de l'ordre à l'encontre de manifestants ont fait l'objet d'une actualité brûlante dans les toutes premières semaines de 2020, ce qui a conduit le ministre de l'Intérieur à rappeler ses troupes au devoir d'exemplarité et à l'éthique. Le Président de la République Emmanuel Macron est lui-même intervenu sur ce dossier à l'occasion d'une question posée lors d'un de ses déplacements[73]. Attendant des policiers et des gendarmes *« la plus grande déontologie »* [74], le chef de l'État a invoqué *« la crédibilité et la dignité »* des forces de sécurité intérieure qui étaient en jeu.

Par-delà le respect du cadre légal, c'est donc toute la légitimité des modes d'action qui est visée par cette exigence d'éthique. Aux fins d'intégrer pleinement l'intelligence artificielle dans les processus de planification et de conduire des opérations de maintien de l'ordre, il faut donc au plus tôt créer les instances de réflexion sur les conditions et modalités de son emploi. La nécessité d'organiser cette réflexion est d'autant plus pressante qu'elle est un prérequis à un développement industriel satisfaisant. Les expérimentations qui sont actuellement conduite tant par les collectivités locales que par de grandes entreprises ne doivent pas à elles seules servir de référence aux développements futurs, mais simplement de démonstrateurs de capacités. Il convient de réunir toutes les parties prenantes (puissance publique, collectivités, opérationnels des forces de l'ordre, magistrats, membres des AAI, entreprises, citoyens) afin d'obtenir le plus large aperçu des enjeux démocratiques. Car sinon l'on s'expose à une vision capacitaire de la technologie, où seule la technique compte, sans préjudice d'atteintes quasi-inévitables en

[73] http://www.leparisien.fr/video/video-macron-j-attends-de-nos-policiers-la-plus-grande-deontologie-14-01-2020-8235834.php

[74] Policiers et gendarmes sont soumis à un ensemble de dispositions réglementaires, tantôt communes tantôt particulières en raison des différences statutaires, en matière de déontologie. Le code de la sécurité intérieure y consacre à cette fin un chapitre complet (Art. R434-1 et suivants), qui comprend notamment une série de principes généraux encadrant l'action policière. La déontologie vise donc l'intégration de principes éthiques et de valeurs morales dans le droit, afin de les opposer juridiquement aux agents peu scrupuleux.

matière de libertés publiques. Là où se désengage – ou s'abstient – l'État, les opérateurs privés d'autorégulent à leur avantage au risque d'ignorer les conséquences de leurs activités.

Il faut donc agréger la réflexion, qui existe d'ores et déjà dans les ministères à l'image du cycle supérieur d'intelligence artificielle du ministère de l'Intérieur[75] proposé par le Centre des Hautes Études du ministère de l'Intérieur (CHEMI) ou de la production doctrinale du centre de recherche de l'École des officiers de la Gendarmerie nationale (CREOGN)[76], puis la décliner en fonction des objectifs de chacune des branches-métiers.

De telles structures devront également être les lieux d'échanges autour des retours d'expérience qui accompagneront le développement opérationnel de cette technologie. Les études d'impact qui guideront l'évaluation pourraient également prendre naissance dans ces comités de réflexion.

Il est donc question de donner du sens aux capacités techniques qui pourraient être proposées par les entreprises, d'en vérifier et ajuster la compatibilité avec le cadre légal existant et surtout d'en proposer d'éventuelles modifications s'il en était nécessaire.

B. Programmer l'éthique ?

L'intégration matérielle de l'éthique est aussi une question fondamentale, dans la mesure où la solution apportée par l'IA en opération de maintien de l'ordre doit être conforme à l'esprit dans lequel le commandant de la force publique la dirige. Ainsi il est intéressant de s'attarder sur la méthode de raisonnement tactique (MRT), développée et appliquée par les officiers de Gendarmerie. La MRT est un outil universel qui permet de cadrer la réflexion et d'inscrire l'action dans des schémas tactiques connus et répétés lors des entraînements, et ce quel que soit le domaine. Elle vise une réponse coordonnée et disciplinée des forces. Appliquée au maintien de l'ordre, elle est déclinée en amont de la mission, de manière aussi précise que l'urgence dans laquelle une opération de maintien de l'ordre est montée le permet (manifestation spontanée, contre-manifestation).

Le chef opérationnel utilise à cette fin un moyen mnémotechnique qui balaye l'ensemble des éléments essentiels à une analyse rapide de la situation qui se présente à lui. L'acronyme TUMAC permet de couvrir : la nature du **T**errain (urbain, rural, semi-urbain, clos, couvert),

[75] https://www.interieur.gouv.fr/Archives/Archives-des-actualites/2018-Actualites/Naissance-du-CSIA
[76] https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN

l'**U**rgence (détresse vitale, exactions, crimes ou délits en cours), les **M**oyens dont il dispose (humains, matériels, renforts, délais d'arrivée de ces renforts), la connaissance de l'**A**dversaire (position, nature, attitude, volume), et enfin le **C**adre légal de l'action au début de la mission et ses évolutions possibles.

L'intégration des éléments d'analyse de cette MRT pourrait servir de fondement à l'élaboration pas à pas de l'IA, et à son apprentissage progressif. Là où l'apprentissage profond se révèlerait être d'une grande aide, c'est dans sa capacité à analyser les résultats d'une opération de maintien de l'ordre au regard des éléments décisionnels initiaux qui ont servi au décideur pour mener les actions. Par une analyse des opérations passées, il serait d'un grand intérêt de déterminer les critères prépondérants et décisifs de réussite d'une opération de maintien de l'ordre, afin – à terme et par la simulation – de pouvoir renseigner le décideur sur les implications de tel ou tel ordre.

Cependant, envisager un tel niveau de prévisibilité n'est en rien une annonce de ce qui sera la réalité des opérations de maintien de l'ordre de demain. Comme le souligne le professeur Dominique Lambert à propos de la capacité d'analyse des système informatiques par rapport aux modèles et aux exemples qui lui sont soumis : *« Pour juger, il faut voir quelles sont les lois qui s'appliquent et comment les adapter dans des situations contingentes, particulières, où cela n'est nullement automatique »*, et de poursuivre *« une machine autonome ne peut juger, car, pour juger, il faut interpréter et aussi s'abstenir d'appliquer les règles ou même les transgresser pour sauver l'esprit des règles et les valeurs que l'on défend »*[77].

Programmer l'éthique s'annonce donc déjà comme une tâche quasi-insoluble pour le technicien. Face au dilemme que pose une situation entre morale et imprécision légale, seules l'imagination et la créativité permettent à l'être humain de sortir du carcan de règles universelles et formelles posées à la machine par le technicien. C'est ici la question du discernement, dont font preuve au quotidien les forces de l'ordre, qui ne peut se coder. En cela il ne peut y avoir de concurrence entre l'être humain et la machine, tout l'enjeu réside dans la capacité de cette dernière à fournir les solutions les plus pragmatiques. Car à potentiel d'analyse égal, la machine peut prendre l'avantage sur l'humain en ce qu'elle est dépassionnée. Pour autant, si l'on veut que ses propositions aient une plus-value opérationnelle, encore faut-il qu'elle fasse l'objet d'une construction robuste.

[77] Dominique LAMBERT, « Éthique et autonomie : la place irréductible de l'humain », *RDN*, n°820, 2019

Section 2 – La nécessité d'une intelligence artificielle robuste, tant structurellement que matériellement

L'intelligence artificielle ne sera réellement au service des opérations de maintien de l'ordre que si elle est robuste. Dans les sciences de l'ingénieur sont qualifiés de « robustes » les systèmes qui offrent une stabilité de leurs performances dans le temps. Ces performances doivent être appréciées au regard d'indicateurs, qui dans notre cas tiennent pour beaucoup à la protection des droits et libertés fondamentales. Il importe donc de mesurer la performance quant aux garanties apportées par la protection externe (ou structurelle) et par la protection interne (ou matérielle).

Si l'IA devait avoir un jour accès aux fichiers de police en temps réel, il faudrait s'assurer qu'elle ne soit pas le vecteur de logiciels malveillants, qui se seraient glissés dans le système lors de sa conception, tant auprès des structures de développement publiques que chez les opérateurs privés. La première conséquence dommageable pour la puissance publique pourrait être la destruction pure et simple des contenus numériques, voire même la destruction physique des matériels informatiques qui en sont les supports.

De manière plus subreptice, l'IA ainsi détournée de son objectif initial pourrait servir à divulguer massivement les données personnels présentes dans les fichiers de police, ou pire encore falsifier les données, rendant impossible le travail des services de police et de justice. L'IA ne serait donc pas en tant que telle exploitée, mais serait le vecteur de tels logiciels informatiques malveillants. La réussite du développement d'une solution informatique comme l'est l'intelligence artificielle du maintien de l'ordre doit prendre en compte ces problématiques de cybersécurité. Les opérateurs privés désireux de se positionner en partenaire de la puissance publique devront donc présenter un maximum de garanties, et les services de l'État (l'Agence nationale de la sécurité des systèmes d'information en tête) – utilisateur final du produit – devront en assumer les risques politiques si une défaillance a lieu.

À nouveau, l'exemple de la plateforme ARTEMIS – mise en œuvre par la Direction générale de l'Armement pour le compte du ministère de la Défense – est une solution d'intérêt pour les opérateurs privés et qui pourrait être transposée par le ministère de l'Intérieur. Car elle permet à ces opérateurs privés de développer leurs solutions d'intelligence artificielle sur un espace numérique sécurisé, à partir des données collectées et anonymisées par le ministère.

À cet égard, il existe une protection de la structure même dans laquelle évolue l'opérateur privé, que l'on peut analyser sous un double prisme. D'une part, ces acteurs privés du numérique sont

bien souvent de petites voire très petites entreprises qui n'ont pas nécessairement les moyens financiers de développer de telles infrastructures sécurisée de stockage et de partage de données. D'autre part, en sus des risques de piratage ou d'intrusion numérique à des fins destructives, il s'agit d'une garantie supplémentaire de lutte contre l'espionnage industriel auquel ces entreprises de petite taille sont particulièrement exposées[78].

Enfin, la création d'une telle plateforme numérique présente une garantie supplémentaire pour le ministère de l'Intérieur, dans la mesure où les données qu'il « prête » à l'exploitation sont moins exposées à une divulgation dans l'espace numérique.

Au plan matériel, la robustesse de l'IA s'apprécie au regard des biais cognitifs. Conséquence logique car dépendante de la quantité et de la nature des données qui ont servis à la développer, l'intelligence artificielle en tant qu'outil prédictif est particulièrement sujette à cette problématique. Le développement initial de l'outil est à cet égard la phase la plus sensible, car l'introduction d'un biais à ce moment particulier de la chaîne risque de compromettre l'ensemble de l'apprentissage ; et ce d'autant plus s'il s'agit d'une IA faible, portée par des logiques statistique et probabiliste.

C'est ce constat qui conduit les développeurs à penser la protection par conception, en sélectionnant rigoureusement les données qui seront proposées à l'apprentissage. Les réseaux de neurones sont ainsi extrêmement instables face à des attaques de type « exemples contradictoires », et subissent de plein fouet les perturbations qu'elles accolent à des données d'entraînement, ce qui conduit à biaiser le résultat donc l'interprétation[79]. Cette problématique est d'autant plus importante qu'il est fait appel aux données en sources ouvertes. Si celles-ci présentent des intérêts multiples en termes économiques et juridiques, l'exemple du logiciel *Tay* (outil de dialogue automatique recourant à l'apprentissage par renforcement, c'est-à-dire par mimétisme avec l'environnement dans lequel il est déployé), illustre bien les dérives d'une intelligence artificielle soumise à la pression de données malveillantes. L'agent conversationnel, développé par Microsoft et déployé sur Twitter, a l'objet d'assauts coordonnés par certains utilisateurs en vue de le détourner de son usage. Malgré deux tentatives et des corrections appliquées par Microsoft, le logiciel a fini par publier des messages à caractère raciste et misogynes. La CNIL s'en était également inquiétée[80] dans son rapport de décembre

[78] https://toulouse.latribune.fr/entreprises/business/2015-02-02/espionnage-industriel-et-secret-des-affaires-les-pme-francaises-sont-elles-en-danger.html
[79] Voir Annexe V
[80] CNIL, « Commet permettre à l'homme de garder la main ? », 2017, p.31 : *« La propension des algorithmes et de l'intelligence artificielle à générer des biais pouvant conduire à leur tour à créer ou à renforcer des*

2017 sur les enjeux éthiques, notamment sur les risques d'accentuation des discriminations et des exclusions, l'IA n'agissant en fait que comme une loupe sur des problématiques ancrées dans la société où sont puisées les données.

La perspective d'un tel fiasco, en matière de données à caractère personnels utilisées à des fins de sécurité publique et de prévention des troubles à l'ordre public, n'est pas envisageable. C'est la raison pour laquelle les autorités publiques pourraient exiger de ne recourir qu'à des prestataires utilisant des données certifiées à cette fin, et donc fruit d'une collecte réalisée exclusivement pour cet objectif d'apprentissage-machine. Il semble tout à fait possible juridiquement de procéder à des extensions de durée, sur la conservation des images enregistrées à l'occasion d'opérations de maintien de l'ordre. Tout comme il appert logique que ces données fassent l'objet d'un contrôle par une autorité administrative indépendante, office que pourrait remplir la CNIL.

C'est donc sur un savant dosage entre qualité, quantité et pertinence des données d'entraînement que reposera la réussite du développement de toute intelligence artificielle. Au regard des implications liée à la surveillance de masse qui se dessine en manifestation, il conviendra d'étudier attentivement les critères qui devront entourer la fourniture de telles ou telles données aux développeurs. Ces critères devront être aussi objectifs que possible, car de cette « pertinence » des données dépend la construction d'un outil qui se veut égalitaire dans les traitements qu'il met en œuvre. Là pourrait intervenir un comité formé d'experts, de magistrats et de citoyens qui les détermineraient ; ce qui favoriserait une démarche encore plus consensuelle et démocratique que le recours à une AAI.

C'est aussi en vue de cet objectif que le préfet Vedel, coordinateur IA au ministère de l'Intérieur, proposait cette fameuse banque de donnée dans le champ régalien pour l'entraînement des algorithmes.

Après avoir brossé les différentes facettes de la robustesse, condition *sine qua non* d'une intelligence artificielle résiliente, il faut désormais s'appesantir sur son explicabilité.

---

discriminations » (…) *« La constat mérite d'autant plus d'être souligné que ces systèmes techniques peuvent également parfois nourrir une croyance en leur objectivité. Une objectivité d'autant plus précieuse qu'elle ferait souvent défaut aux humains. »*

Section 3 – L'explicabilité : enjeu majeur de l'acceptabilité d'une telle technologie

Il faut le dire d'emblée, l'intelligence artificielle fonctionnant sur la base de réseaux neuronaux présente une difficulté de taille pour une technologie qui se veut être une solution d'analyse rationnelle reposant sur des critères objectifs : elle fonctionne comme une boîte noire, ce qui conduit à considérer les résultats qu'elle produit comme « magiques ».

Là où un système expert nécessite d'avoir des règles écrites dans son programme pour être opérant au regard des données injectées ; les réseaux neuronaux traitent d'importantes quantités de données, en les répartissant sur l'ensemble de leurs branches, selon des méthodes d'optimisation afin d'en dégager des règles[81]. Le modèle qui en résulte est donc celui d'un programme complexe issu d'une interdépendance entre plusieurs algorithmes qui le composent, donnant naissance à plusieurs couches de paramètres. Le traitement d'une donnée en entrée, dans le but d'en obtenir une analyse, est donc le fruit d'une interaction complexe de cette donnée avec ces couches successives de paramètres. On est donc bien loin d'une simple suite de causalités.

Dans le paragraphe précédent, nous avons saisi l'importance de la qualité des données qui avaient permis l'entraînement de l'IA. Aussi l'unicité de ces données d'entraînement doit nous interroger sur la reproduction du résultat. Qu'en serait-il de l'identité de résultat si les données d'entraînement n'avaient pas été les mêmes ?

De la même manière, les algorithmes développés dans le domaine de l'intelligence artificielle le sont à des fins bien précises. Dans un article paru à la Revue de Défense Nationale en 2019 cosigné par le général Olivier Kempf et la polytechnicienne Éloïse Berthier, tous deux soulignent l'architecture unique de ces algorithmes particuliers, qui tient à leur entraînement. Dès lors, il n'est pas possible de les employer à d'autres fins. À nouveau l'on comprend la nécessité qu'il y a à fournir des données issues de fichiers certifiés et régulièrement mis à jour par les services de l'État pour une IA du maintien de l'ordre la moins biaisée possible. Il en va du droit des individus à un traitement impartial et équitable.

Même si les auteurs évoquent deux remèdes à ce défaut d'explicabilité, dont l'un d'eux a donné des résultats concrets[82] dans la capacité de l'IA à fournir à l'utilisateur, par conception, les

[81] Voir Annexe II

[82] L'agence militaire américaine DARPA a développé dès 2016 un programme afin d'encourager la recherche en matière d'explicabilité des algorithmes d'apprentissage statistique (programme *Explainable Artificial Intelligence*). Deux types de modèles en ont émergé. D'une part, les outils qui servent à expliquer les méthodes

étapes du « raisonnement » qui l'ont amené à identifier le contenu d'une photographie grâce à des éléments caractéristiques de celle-ci. C'est fondamentalement une question de confiance qui devra émerger entre les utilisateurs et ce système complexe. Et comme la confiance ne se fonde pas uniquement sur une simple promesse, ce seront les résultats et les performances de l'IA qui seront les déclencheurs de cette confiance.

Si l'explicabilité n'est pas encore le fondement sur lequel les parties prenantes (utilisateurs, citoyens) peuvent baser leur acceptation de la technologie, la confiance doit être de mise et reposer sur des éléments concrets (§1). La transparence des modalités de mise en œuvre de l'IA en est un, est en son absence pèsent un certain nombre de conséquences (§2).

§1. Les clefs du socle indispensable de la confiance

Cette confiance doit être recherchée tant auprès des professionnels du maintien de l'ordre que des citoyens qui en seront les destinataires.

Pour les premiers, il s'agit d'organiser « l'acceptabilité interne »[83] d'une IA du maintien de l'ordre, essentiellement par la formation. En effet, seul l'entraînement des personnels qui auront à y recourir pourra créer les conditions de cette confiance. Pour le décideur politique représentant de l'État dans les territoires ainsi que pour le chef opérationnel, il s'agit d'en saisir les potentialités et les limites dans l'aide à la décision. Pour les policiers et gendarmes déployés sur le terrain, il s'agit d'en comprendre les bénéfices et de faire remonter les cas où l'utilisation n'a pas *a priori* porté de fruit.

Comme l'expliquait le général Bertrand Cavallier, qui a longtemps commandé le Centre national d'entraînement des forces de gendarmerie (CNEFG) où sont formés les escadrons de gendarmerie mobile, devant la commission d'enquête Popelin : « *Trois notions structurent l'entraînement à Saint-Astier : premièrement, le rappel du sens* » (…) « *deuxièmement, le renforcement des capacités individuelles* » (…) « *troisièmement, le réalisme des entraînements, qui permet de placer les gendarmes dans des situations les plus proches possibles de la réalité, afin de favoriser une certaine maturité psychologique dans la gestion du stress* ».

d'apprentissage pour des systèmes déjà en fonction. D'autre part, les IA disposant par conception d'une capacité explicative de leur raisonnement.

[83] Par opposition à l'acceptabilité externe, expression développée par le colonel de gendarmerie et polytechnicien Rémy Nollet, qui représente l'adhésion des populations à cette technologie.

C'est donc par l'utilisation de l'IA lors des entraînements que les forces mobiles pourront par la suite en tirer tous le potentiel. Il faut démystifier l'outil, et en imprégner au plus vite les futurs cadres des forces de maintien de l'ordre dès lors que les conditions de mise en œuvre d'une telle technologie seront validées.

C'est également pour cette raison de confiance qu'il faudra continuer à recruter des spécialistes de haut-niveau, car la confiance n'exclut pas le contrôle et il faut sans cesse adapter l'outil aux conditions opérationnelles. En ce sens, les diverses expérimentations menées en matière de police prédictive dans les territoires sont à examiner de près. Les personnes auditionnées à l'occasion de l'étude menée par l'Institut d'aménagement et d'urbanisme en 2019 porte à cet égard un regard assez critique sur les outils développés actuellement en matière de prévention de la délinquance et de la criminalité, et sur leur appréhension par les opérationnels[84]. La question qui sous-tend ces critiques est celle du niveau de performance de l'algorithme attendu, au regard de l'expérience humaine acquise tout au long d'une carrière.

S'agissant de l'acceptabilité externe, l'enjeu est encore plus important dans la mesure où il s'agit de la confiance des administrés au regard de leurs situations personnelles. Les questions tournent autour de possibles atteintes à la vie privée, à l'impartialité et au respect des règles traditionnelles du service public (notamment les principes d'égalité et de neutralité). Car oui, une opération de maintien de l'ordre répond à la définition classique du service public, c'est-à-dire une activité assurée ou assumée par la personne publique, en vue de la satisfaction des besoins d'intérêt général (ici l'ordre public).

L'intelligence artificielle du maintien de l'ordre s'inscrit donc à cet égard dans un mouvement plus large de *policing by consent*, principe dégagé par le britannique Robert Peel au XIX^{ème} siècle. Ce principe vient à considérer la reconnaissance des pouvoirs détenus par la police en vue d'accomplir ses missions est fonction de l'adhésion de la population, donc de la capacité de la police à obtenir et conserver le respect qui lui est accordé. Dans ce cas, une consultation large des citoyens[85] sur les conditions de déploiement d'une telle technologie en manifestation serait seule à même de garantir cette visée démocratique.

---

[84] « La police prédictive », IAU, 2019, p. 22 : *« Pour un gendarme au niveau local qui connaît normalement bien sa délinquance, la plateforme présente peu de plus-value. »* (…) *« Le problème de cet outil, c'est que ce n'est pas un outil algorithme »* (…) *« il ne prend pas assez de variables, c'est seulement un outil statistique. »*

[85] https://www.lemonde.fr/economie/article/2019/10/14/cedric-o-experimenter-la-reconnaissance-faciale-est-necessaire-pour-que-nos-industriels-progressent_6015395_3234.html

§2. Les conséquences d'un manque de transparence dans la mise en œuvre de l'IA

Outre le possible manque d'adhésion des citoyens à cette technologie, plusieurs éléments viennent corroborer un possible échec du déploiement de l'IA en manifestation.

Le premier de ces éléments est le risque (ou la peur ?) d'une confiscation du pouvoir. Si certains voient dans les algorithmes auto-apprenants et leur autonomie complète une nouvelle dictature, un nouvel asservissement[86], d'autres considèrent cette autonomie comme un but à atteindre en se fondant sur l'objectivité pure dont ferait preuve l'IA. Ce serait méconnaître la possibilité que l'IA puisse être biaisé, comme nous l'avons expliqué plus haut. Ce serait également ignorer la difficulté pour un algorithme de faire la différence entre un lien de causalité et un simple lien de corrélation, ce que reprochent certains spécialistes en IA[87].

Ces derniers constats sont également vrais pour le risque d'abandon du pouvoir décisionnel par l'humain au profit d'une machine, qu'il considère comme supérieur à lui, en raison de ses capacités supérieures de traitement des données. Rien ne garantit une meilleure capacité décisionnelle à la machine, c'est la raison pour laquelle l'IA devra rester cantonnée à une activité d'aide à la décision. La CNIL se montre d'ailleurs très critique envers ces technologies et leurs énormes capacités de soutien à l'humain. Elle attire l'attention des utilisateurs futurs sur le risque d'une *« érosion des vigilances individuelles »*[88].

Enfin, face à des analyses qui pourraient s'avérer décevantes, le dernier écueil sera d'abandonner le tournant que représente l'IA. Le potentiel est bien là, et si les résultats ne sont pas au rendez-vous, ce n'est pas l'ensemble de la technologie qu'il faut remettre en cause, mais plutôt ses modalités de mise en œuvre.

Au regard de l'ensemble de ces prérequis qui structurent la technologie et des implications en matière de libertés publiques, il convient de ne pas abandonner le développement de cet outil aux lois du marché. S'il ne faut évidemment pas laisser de côté les innovations développées par le secteur privé, il convient de les encadrer autant que possible (juridiquement, éthiquement, procéduralement) sous peine de voir ce secteur privé s'autoréguler au détriment possible des droits et libertés.

---

[86] Cathy O'NEILL, *Weapons of math destruction : how big data increases inequality and threatens democracy*, Broadway Books, 2017

[87] Judea PEARL et Dana MACKENZIE, *The book of why : the new science of cause and effect*, Basic Books, 2018

[88] *Op. cit.* note 80, p. 80

Concevoir une IA respectueuse des libertés publiques, c'est concevoir une IA autant que possible « objectivisée » : ce qui pose la question de la qualité, de la quantité et de la pertinence des données qui lui seront injectées tant son développement initial que dans son aguerrissement continu. La réussite de cet entraînement constitue à cet égard un enjeu primordial en termes d'efficacité opérationnelle et de prévention des biais. Là réside le cœur de la problématique, car les biais seront la principale cause de contestation juridique des décisions prises sur la base, où plutôt sur le conseil, d'un algorithme.

Une question fondamentale s'immisce lentement mais sûrement dans le débat. Avec le mouvement de judiciarisation des opérations de maintien de l'ordre, qui vient déjà bousculer la frontière entre police administrative et police judiciaire, le recours à l'IA dans l'analyse comportementale et la sélection des choix tactiques ne conduit-il pas subtilement à créer des présomptions de culpabilité ?

Face aux dérives qui pourraient poindre et à une bascule possible du système d'une logique préventive à une logique de présomption, des garanties juridiques doivent être avancées. Le rôle du juge, notamment du juge judiciaire gardien de la liberté individuelle, trouve toute sa place dans ce processus qui doit accompagner le développement d'une intelligence artificielle raisonnée du maintien de l'ordre.

Chapitre 2 – PROTÉGER DES MÉSUSAGES : LES GARANTIES JURIDICTIONNELLES ET NON JURIDICTIONNELLES

Une fois pris en compte les prérequis indispensables, développer la technologie dans le domaine si sensible de la préservation de l'ordre public requiert des protections particulières contre les mésusages. Il faut se pencher sur les garanties juridictionnelles et non-juridictionnelles, en commençant par interroger le rôle que peut jouer le juge dans ce développement technologique et son suivi (Section 1). Puis il faut penser la place déterminante que jouent d'ores et déjà les autorités administratives indépendantes (Section 2). Enfin, il est nécessaire de s'attarder sur la responsabilisation des utilisateurs, et leur militarité en l'espèce, premiers garants d'un usage raisonné de l'IA en manifestation (Section 3).

Section 1 – Quelle protection du juge dans le développement et l'accompagnement de la technologie ?

La place du juge est fondamentale dans l'État de droit. Face à une technologie dont la mise en œuvre pourrait conduire à de graves atteintes aux droits et libertés fondamentales garanties par la Constitution, son action protectrice doit être mise en lumière et pas seulement dans les cours et tribunaux où il a l'habitude de siéger. Si l'on attend évidemment de lui qu'il remplisse son office, il doit pouvoir être consulté pour son expertise dès les phases de développement.

Le juge n'est pas seulement la « bouche de la loi », il en est également le gardien de son esprit. À cet égard, il mérite d'être associé à la réflexion éthique qui accompagne la conception et la mise en œuvre de l'intelligence artificielle. Il ne s'agit pas à terme de le voir entrer dans une opposition de principe avec le législateur, mais de s'assurer qu'il dispose d'une réelle connaissance de l'état des possibilités techniques au regard de ce qui pourrait être valablement mis en œuvre.

§1. Une présence au long cours du juge constitutionnel

Le Conseil constitutionnel est au premier chef concerné dans la mesure où depuis la révision constitutionnelle du 23 juillet 2008 introduisant la question prioritaire de constitutionnalité, il peut connaître *a posteriori* des atteintes aux droits et libertés fondamentales du fait d'une disposition législative déjà promulguée. Cet office, qui lui a été attribué en plus du contrôle des lois qui lui sont déférées avant promulgation, le place donc en situation de connaître les situations particulières dans lesquels les droits des citoyens sont atteints.

Si beaucoup considèrent que ce conseil est couvert d'un vernis politique, faisant parfois même dire à certains que *« le juge constitutionnel est l'institutionnalisation de l'indétermination du droit »*[89], force est de reconnaître qu'il dispose de nombreux outils pour contrôler et infléchir sur les modalités d'exécution des lois. Par-delà la censure qu'il pourrait opposer au texte de loi, il s'est notamment approprié depuis quelques années une technique de contrôle qui jusque-là n'appartenait qu'au juge administratif[90] : le contrôle de proportionnalité. Le Conseil constitutionnel a ainsi eu l'occasion de le mettre en œuvre en matière de sécurité intérieure, notamment à l'occasion de l'examen de la loi pour la sécurité intérieure. Il faut noter qu'à cette époque, la fouille des véhicules dans le cadre de la police administrative avait été considérée conforme aux exigences constitutionnelles par les sages de la rue Montpensier, dans la mesure où elle était conditionnée à l'existence d'une menace à l'ordre public, qui serait contrôlée par la suite par le juge ordinaire s'il était saisi.

Le parallèle peut donc largement être dressé à l'égard de la mise en œuvre de techniques particulières d'aide à la décision en matière de manifestation. Reste à savoir le degré de contrainte qui serait appliqué à cette condition : simple menace de trouble à l'ordre public, ou raisons réelles et objectives de penser qu'une atteinte va avoir lieu ? Là encore, la frontière entre police administrative et police judiciaire est ténue.

Pour Pierre Mazeaud, l'appréciation qu'a portée le Conseil constitutionnel sur le caractère suffisant de cette condition en matière de fouille de véhicule tient selon lui du principe de précaution[91]. Cette balance entre risques pour l'ordre public et préservation des libertés

[89] Dominique ROUSSEAU, Pierre-Yves GAHDOUN, Julien BONNET, *Droit du contentieux constitutionnel*, Montchrestien, 11è éd., 2016

[90] Dans un célèbre arrêt du Conseil d'État, dit « Ville nouvelle Est », rendu en assemblée le 28 mai 1971, le juge administratif procède au bilan entre les coûts et les avantages tirés d'un projet de construction immobilier. Cette jurisprudence du bilan coût/avantage lui a servi de motif afin de considérer que cette opération ne pouvait être légalement déclarée d'utilité publique. Le contrôle de proportionnalité était ainsi clairement matérialisé.

[91] Pierre MAZEAUD, *Libertés et ordre public*, site Internet du Conseil constitutionnel, 2003, p. 4

individuelles est donc la manifestation éclatante d'un contrôle de proportionnalité en matière de police administrative par le Conseil constitutionnel. Cette technique particulière de contrôle pourra s'adjoindre de déclaration de conformité sous réserve. Ces réserves ont également une valeur constitutionnelle, dans la mesure où, en vertu de l'article 62 de la Constitution[92], il existe une autorité juridique liée au dispositif des décisions qu'il rend et aux motifs qui en constituent le soutien nécessaire.

Dans le cadre de sa fonction juridictionnelle, le Conseil constitutionnel aura donc une place prépondérante dans la mise en mouvement de solutions technologiques au soutien des opérations de maintien de l'ordre. Car il faudra bien créer ou mettre en lien par voie législative les fichiers dans lesquels cette IA du maintien de l'ordre puisera ses données. Par la présence de ses membres dans les comités d'éthique, et par les lois et affaires qui lui seront déférées, le juge constitutionnel accompagnera par conséquent l'ensemble du mûrissement de l'IA du maintien de l'ordre.

§2. Un juge européen à préparer

Dans la mesure où le développement d'une IA en matière de maintien de l'ordre pourrait concerner un certain nombre de pays membres du Conseil de l'Europe, il paraît important d'associer dès maintenant le juge de Strasbourg aux réflexions. Et ce d'autant plus qu'il n'apparaît pas inintéressant de développer une solution technologique commune dans le cadre d'une coopération interétatique.

Il y a tout lieu de penser que la Cour européenne des droits de l'Homme soit tôt ou tard saisie d'une requête ayant trait à l'usage de l'intelligence artificielle par un État membre. À cet égard, il convient d'entendre les positions de ces juges sur une application de l'IA en matière de d'ordre public, à l'heure où le Conseil de l'Europe prend le dossier de l'intelligence à bras le corps[93]. Il s'agit de prévenir d'éventuelles condamnations, quitte à faire prévaloir en amont de celles-ci une doctrine fondée sur la marge nationale d'appréciation.

---

[92] Art. 62, alinéa 3 de la Constitution : *« Les décisions du Conseil constitutionnel ne sont susceptibles d'aucun recours. Elles s'imposent aux pouvoirs publics et à toutes les autorités administratives et juridictionnelles »*

[93] Une charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires a d'ores et déjà été adoptée en décembre 2018 par la commission européenne pour l'efficacité de la justice du Conseil de l'Europe

§3. L'intervention duale du juge judiciaire

Le juge judiciaire pourrait voir son office renforcé dans le domaine des opérations de maintien de l'ordre. Classiquement, son rôle de gardien de la liberté individuelle confié par l'article 66 de la Constitution lui permet de connaître de toute privation arbitraire de liberté constitutive d'une atteinte au droit à la sûreté. En application de la théorie jurisprudentielle de la voie de fait et par exception au principe de séparation des autorités administratives et judiciaires, il connaît également des décisions des autorités administratives qui conduisent à atteindre la liberté individuelle des citoyens[94]. Ainsi, les forces de maintien de l'ordre qui, en l'absence de troubles à l'ordre public, viendraient interpeler des manifestants sur la base d'une présomption algorithmique de commission d'infraction verraient leur action entrer dans le champ de compétence du juge judiciaire.

De même, on peut s'interroger sur la compétence du juge judiciaire à l'égard du droit constitutionnel au respect de sa vie privée, dans la mesure où des capteurs auditifs viendraient à surprendre une conversation qui, quand bien même elle aurait lieu sur la voie publique et dont les éléments indiqueraient de potentielles actions de troubles à l'ordre public, serait prononcée à titre privé entre deux individus. Une telle captation qui conduirait directement et pour ce seul motif à une interpellation amènerait très probablement le juge judiciaire à se voir saisir pour privation arbitraire de liberté. Même si l'intimité de la vie privée ne fait pas l'objet d'une définition légale, la Cour de cassation a considéré que constituait une atteinte à son endroit la captation, l'enregistrement ou la transmission de paroles prononcées à titre privé ou confidentiel, sans le consentement de la personne, si les entretiens présentent un tel caractère[95]. Il est clair que les frontières sont floues entre l'intention et la présence d'actes préparatoires.

Il y a donc toute une place pour la réflexion des juges judiciaires sur la légalité et la légitimité du déploiement de tels outils en vue d'un traitement algorithmique. La question de savoir s'il existe une vie privée sur la voie publique est une problématique de longue date. Et les évolutions en termes de reconnaissance faciale et d'analyse comportementale sur cette même voie publique

---

[94] Depuis une décision du Tribunal des conflits du 17 juin 2013 (M. Bergoend c/ Société ERDF Annecy Léman) : *« Il n'y a de voie de fait de la part de l'administration justifiant, par exception au principe de séparation des autorités administratives et judiciaires, la compétence des juridictions de l'ordre judiciaire, pour en ordonner la cessation ou la réparation, que dans la mesure où l'administration, soit a procédé à l'exécution forcée dans des conditions irrégulières d'une décision même régulière portant atteinte à la liberté individuelle ou aboutissant à l'extinction du droit de propriété, soit a pris une décision qui a les mêmes effets d'atteinte à la liberté individuelle ou d'extinction d'un droit de propriété et qui est manifestement insusceptible d'être rattaché à un pouvoir appartenant à l'autorité administrative »*

[95] Cass., 1ère civ., 06 octobre 2011, pourvois n°10-21822 et 10-21823

nous amènent à réfléchir sur le point de savoir si finalement le visage n'est pas le dernier lieu de la vie privée.

§4. Vers un bloc de compétence pour le juge administratif ?

Le juge administratif dispose de la compétence de principe en matière de prévention des atteintes à l'ordre public. Il n'a cessé de voir étendre son domaine de compétence, particulièrement en matière de protection des droits et libertés des administrés, du fait d'actions attentatoires de la part de la puissance publique. Par la célèbre loi du 30 juin 2000 créant le référé-liberté, il lui est attribué le pouvoir de prendre toute mesure nécessaire à la sauvegarde d'une liberté fondamentale en situation d'urgence. A ainsi été établi, de manière prétorienne, que la liberté individuelle était une des libertés fondamentales invocable en matière de référé-liberté (CE, 15 octobre 2001, Ministère de l'Intérieur contre Hamani).

Pour autant, il n'est pas opportun de vouloir créer un bloc de compétence administratif, qui aurait pour champ d'application l'ensemble des éléments qui touchent de près ou de loin aux opérations de maintien de l'ordre. En effet, la méthode de répartition actuelle semble de loin la plus efficace, et ne nécessiterait aucun adaptation fondamentale pour l'intégration de solution d'IA. Cette méthode d'attribution repose sur la finalité de l'action policière, qui peut passer sur une même manifestation d'une visée préventive à une visée judiciaire (constat d'un crime ou d'un délit flagrant).

En revanche, le juge administratif pourrait voir son activité de contrôle des fichiers de police démultipliée. C'est auprès de lui que les citoyens pourront faire valoir leur droit à rectification ou effacement des données. La question sensible auquel il devra faire face, et elle n'est pas résolue, est celle de ce droit à rectification alors que le traitement algorithmique a déjà eu lieu ; c'est-à-dire comment revenir sur la construction d'un algorithme alors que la donnée d'entraînement a pu être incomplète ou fausse ? Le citoyen pourra-t-il se satisfaire de la simple suppression des données le concernant ? Y aura-t-il des conséquences sur les analyses à venir ? Ses conséquences seront-elles seulement infimes, sur la masse des données d'entraînement qui auront servi au développement ?

C'est pour cette raison que l'anonymisation des données, quelle qu'en soit sa forme (floutage, absence de données biométriques), est en elle-même une garantie du fonctionnement légitime de l'IA.

Rien ne permet donc de penser que le travail des juges du fond soit bouleversé. L'intégration d'une IA du maintien de l'ordre ne devrait pas changer la capacité d'appréciation juridique des situations de fait qui leur seront présentées.

Section 2 – La place de choix des autorités administratives indépendantes

Là encore, les membres spécialisés de ces AAI ont une place de choix dans les développements d'une IA en manifestation. La CNIL assure ainsi une présence continue en évaluant et garantissant le cadre juridique lors des phases d'expérimentation. Elle accompagne également la mise en œuvre technologique à travers des opérations de contrôle sur pièce et sur place, mais aussi en ligne pour les données librement accessibles ou rendues accessibles *« y compris par imprudence, par négligence ou par le fait d'un tiers »*[96].

La constitution d'une commission en son sein, pour la validation des données qui serviront à l'entraînement algorithmique par exemple, présentera un intérêt pour la vérification du respect des obligations légales tant en amont (anonymat des données, respect des procédures par les services de l'État et les éventuels opérateurs privés) qu'en aval (conditions de conservation de ces données, application du droit de rectification, destruction).

Pour le justiciable, la CNIL représente un interlocuteur de confiance pour s'assurer du respect de ses droits par les services de l'État. Pour ces derniers, la CNIL leur permet d'empêcher les magistrats de remettre systématiquement en cause l'existence et le fonctionnement de la machine à l'occasion d'un litige. De ce fait, la CNIL agirait comme un inhibiteur des passions qui entourent la mise en œuvre de cette technologie, encore faut-il que cette technologie passe le contrôle de conformité du Conseil constitutionnel.

La CNIL est d'ailleurs très attentive à ce que la loyauté et la vigilance entourent le développement de toute intelligence artificielle. Elle considère également trois principes fondamentaux d'ingénierie, dont le respect pourrait être un élément de contrôle par le juge constitutionnel pour les lois d'autorisation de ces technologies : l'intelligibilité, la responsabilité et l'intervention humaine.

Ainsi, la CNIL veut s'affirmer comme un acteur incontournable dans ce domaine, et renforcer sa position en publiant régulièrement sur le sujet. Elle encourage également l'expérimentation,

[96] Art. 19 modifié, Loi n°78-17 du 06 janvier 1978

ce qui essentiel à la compréhension pratique des enjeux pour le citoyen. Mais elle n'est pas la seule AAI à présenter un fort intérêt démocratique en la matière.

Une autre AAI pourrait également voir son activité valorisée : la Commission national de contrôle des techniques de renseignements (CNCTR). Chargée de veiller sur la légalité de la mise en œuvre de techniques spéciales de renseignement sur le territoire national, elle rend des avis sur toute demande de mise en œuvre par les services de police compétents avant accord du Premier ministre et en contrôle l'exécution *a posteriori*.

Son action pourrait viser à déterminer les cas de manifestations qui permettent de recourir à l'intelligence artificielle. Car rien n'interdit au législateur de n'autoriser cette technologie que dans des hypothèses limitatives, portant sur des circonstances de temps et de lieu bien précises. On peut ainsi conditionner l'usage de l'IA de maintien de l'ordre à des périodes d'état d'urgence, ou des risques manifestement élevés de troubles à l'ordre public.

La CNCTR vérifierait alors l'adéquation de la demande des autorités de police administrative avec ce recours à l'IA, la sincérité et la proportionnalité de celui-ci au regard des atteintes aux libertés publiques et à la vie privée, et enfin le respect de conditions légales particulières évoquées précédemment que le législateur aurait assorties.

Section 3 – La militarité des forces de maintien de l'ordre au service de la responsabilisation

La responsabilisation est sans aucun doute le point crucial de la mise en œuvre réussie d'une IA du maintien de l'ordre. S'il est techniquement envisageable d'automatiser complètement la chaîne de commandement, et par conséquent de confier le processus décisionnel à la machine, les avancées de l'intelligence artificielle ne pourront ni ne devront remplacer la responsabilité du décideur. Que celui-ci soit politique, opérationnel ou industriel, le décideur devra continuer d'assumer sa part de responsabilité dans la mise en œuvre des actions qu'il commande.

La première raison est que l'IA n'a pas pour vocation (et ne devra jamais avoir) à remplacer l'humain, mais le suppléer dans la réalisation de tâches complexes. C'est donc un outil d'optimisation qui contracte les coûts temporels, humains et matériels de l'analyse en vue d'une prise de décision accélérée. En cela, l'humain trouve sa place « dans » la boucle décisionnelle, ou « sur » celle-ci : il confronte son analyse et son expérience à celle de la machine afin

d'argumenter la décision qu'il prendra. On entre, au plus, dans une automatisation de l'analyse qui ne doit en rien déposséder le chef de sa responsabilité opérationnelle.

La seconde raison est qu'il est difficilement envisageable que l'IA mette en œuvre elle-même les actions qu'elle préconise. Si cette hypothèse, qui correspond à l'image de l'humain « hors » de la boucle décisionnelle, est tout à fait envisageable pour des systèmes d'arme dans le domaine militaire qui déciderait d'elles-mêmes de la légitimité de faire feu, et de la légitimité ou non de la cible ; ou pour des robots-chirurgiens qui décideraient seuls des parties du corps à opérer et selon quelles modalités. Pour ce qui est des opérations de maintien de l'ordre, il est une réalité pratique qui est celle des personnels de la gendarmerie et de la police nationale, qu'aucune machine ne peut encore remplacer. Maintenir l'ordre en manifestation est une activité qui nécessite une exécution humaine, et qui place chacun des membres des forces de l'ordre dans une réflexion sur le sens de son action, sa légalité et sa légitimité. Il y a par conséquent un obstacle matériel à autonomisation totale de l'IA en manifestation.

Corollaire de cette raison, il n'est pas question de donner une personnalité juridique « robot ». Cette proposition, avancée notamment par l'avocat Alain Bensoussan[97], vise à doter l'algorithme d'une personnalité donc d'une responsabilité juridique. En substance, ne sachant pas où la rechercher (auprès du constructeur ? de l'inventeur ? de l'ingénieur ? du vendeur ?), les actes dommageables que commettrait un robot lui seraient imputés. Par-delà les doutes sur la catharsis que représente la justiciabilité de l'être humain pour les victimes, c'est surtout à la déresponsabilisation de ceux qui commanderait une action que conduirait un tel subterfuge juridique.

Oui, la responsabilisation doit être au cœur de la réflexion éthique et du développement de toute intelligence artificielle. Et cette responsabilisation devra concerner chacun à son niveau (représentant de l'État sur le territoire local, autorité habilitée par celui-ci, commandant de la force publique, gendarme mobile et CRS déployés).

Cette nécessité de ne pas déléguer complètement la chaîne décisionnelle à l'IA trouve aussi une explication technique. Dès lors que l'intelligence artificielle est probabiliste et donc potentiellement soumise aux biais, il est nécessaire d'avoir un « coupe-circuit » humain qui connaît l'algorithme et ses limites, et qui va engager sa responsabilité professionnelle sur les décisions que lui va prendre.

[97] Voir notamment Alain BENSOUSSAN, Jérémy Bensoussan, *IA, robots et droit*, Larcier, 2019

Il est par conséquent nécessaire d'apprendre à se servir de ces outils, mais aussi d'apprendre à ne pas s'en servir car il faut en maîtriser sa dépendance. Le risque, humain, est d'accorder une confiance sans cesse plus grande et aveugle à des systèmes que l'on considère bien moins infaillibles que l'être humain. Aucun processus formel ne garantit que les données et algorithmes ainsi développés soient les bons pour l'objectif assigné. D'un point de vue logique, on ne peut considérer qu'un programme est correctement produit du seul fait des bonnes réponses qu'il apporte : ce serait ignorer qu'il puisse par la suite commettre des erreurs d'appréciation des situations. Et en l'état actuel des choses, rien ne permet de tester la validité des modèles d'IA.

Il s'agit donc de placer l'individu au cœur de la technologie : un individu éclairé, entraîné et responsable. À cet égard, la militarité des forces de maintien de l'ordre est un atout de taille dans la responsabilisation des individus.

En effet, cette militarité – qui tient notamment de sa structure pyramidale – donne une clarté certaine à la chaîne décisionnelle et de commandement. Chaque personnel a une place propre, qui procède d'un supérieur, et dispose de moyens humains et matériels sur lesquels il peut compter pour la réalisation de sa mission particulière. Toute opération est décomposée en une succession de missions intermédiaires qui responsabilisent l'ensemble des personnels pour la part qu'ils doivent accomplir. Cette responsabilité individuelle est un devoir, assumée en vertu de l'obéissance, mais elle ne doit pas être aveugle. Aussi, la théorie des baïonnettes intelligentes est un leitmotiv qui doit interroger tout membre des forces de l'ordre sur son obligation de refuser l'ordre manifestement illégal. Si consécutivement à un biais technique, l'intelligence artificielle en arrivait à proposer un tel ordre, le conditionnement moral et légal des personnels de la gendarmerie et de la police nationale devrait facilement s'imposer.

Cette responsabilisation individuelle a également sa réciproque. Dans toute chaîne de commandement, la défaillance d'un maillon est bien souvent portée par l'ensemble. Le résultat d'une application irréfléchie de l'IA qui conduirait à un dommage, matériel ou physique, mettrait donc en cause directement la responsabilité de l'ensemble de la chaîne de commandement, et à son sommet, l'autorité politique. L'intégration d'une intelligence artificielle du maintien de l'ordre est donc une question bien plus large qu'une seule problématique de mise en œuvre opérationnelle.

CONCLUSION GÉNÉRALE

L'intelligence artificielle se révèle donc comme un potentiel et formidable démultiplicateur de l'action des forces de l'ordre en matière de maintien de l'ordre. Elle se propose de valoriser l'immensité des données et l'expérience acquises par les forces de l'ordre afin d'améliorer la gestion de ces opérations complexes. Si le cadre juridique semble à l'heure actuelle encore insuffisamment solide au regard des enjeux en matière de libertés publiques, il offre néanmoins la possibilité pour les entrepreneurs en intelligence artificielle de mener des expérimentations sous le contrôle de la CNIL.

La réflexion éthique sur les caractéristiques du produit final doit se poursuivre et inclure l'ensemble des intéressés (développeurs, utilisateurs, autorités de contrôle, magistrats, citoyens) dans des structures communes. Cette réflexion se doit également d'être opérationnelle, en vue d'articuler la relation entre la machine et le décideur dans le processus de construction des ordres.

On aurait tort de vouloir tout déléguer à l'intelligence artificielle, même si les promesses sont grandes. Le système peut être faillible et les répercussions en termes de libertés sont trop importantes pour passer outre. Il y a fort à parier que tôt ou tard il y a aura un recours massif aux solutions d'intelligence artificielle dans les opérations de maintien de l'ordre. Il faut donc que les pouvoirs publics se saisissent rapidement de cette question, afin de dessiner les contours de ce qu'il est légitime ou non de développer.

Si dans d'autres domaines régaliens, beaucoup d'initiés appellent à ne pas *« céder aux sirènes des industriels »*[98], c'est que la technique permet de repousser sans cesse les limites du possible. Mais là où sont en jeu la liberté et la sécurité, il faut questionner les attentes réelles de la société, et l'inclinaison de celle-ci à un côté plus qu'à un autre de la balance. Le législateur doit par conséquent rapidement s'intéresser aux applications de l'IA en manifestation, que cela soit pour encadrer ou pour interdire.

Cette implication des pouvoirs publics est d'autant plus pressante que les développements vont bon train ; et qu'en l'absence de régulation, le premier à proposer dirige les comportements de

[98] La Quadrature du net alerte l'opinion publique sur la nécessité de réglementer l'usage de certaines applications, comme la reconnaissance faciale, à des interfaces numériques du service public (telles qu'Alicem). Elle donne l'exemple de villes situées dans des pays démocratiques étrangers qui ont refusé de mettre en œuvre ces solutions pour leurs services publics.
https://www.marianne.net/societe/lancement-de-la-reconnaissance-faciale-en-france-mais-qu-allons-nous-faire-dans-cette-galere

ceux qui suivent. Il existe donc un impératif démocratique à l'émergence d'une position nationale claire. Trois enjeux sont à surveiller particulièrement :

- le maintien d'une souveraineté, au moins européenne fondée sur des valeurs communes ;
- la puissance du privé, propriétaire en quantité de ressources essentielles à l'IA que sont les données ;
- le couplage des technologies et des capacités entre elles, qui conduit à une surveillance de masse dépassant largement le simple cadre du maintien de l'ordre en manifestation.

Tout le monde a donc intérêt à discuter des conditions dans lesquelles déployer cette solution d'aide à la décision opérationnelle, car il faut bien qu'elle en reste là. Le défi qui s'annonce majeur est celui de la synthèse entre les volontés politiques et les capacités techniques, celui de parvenir à coder l'éthique par conception.

Pour l'avocat Alain Bensoussan, l'intégration des nouvelles technologies dans le quotidien des citoyens est une formidable opportunité pour la matière juridique. Le droit doit ainsi être considéré comme un élément d'expression de l'innovation, plutôt qu'un élément de son étranglement. Il faudra pourtant s'assurer que cette innovation ne se fasse pas au détriment des libertés individuelles et collectives.

Le vrai problème est celui de l'acceptabilité de la technologie, quand bien même l'humain reste dans la boucle. Il faut du temps pour gagner la confiance des citoyens. Mais c'est à ce prix, celui du consensus, celui de l'État de droit, que l'on respecte la démocratie. Cette acceptabilité par les citoyens passera en outre par l'efficacité des expérimentations qui sont et seront menées. Là se tient peut-être un des leviers d'avenir pour le rapprochement des forces de police avec la population.

TABLE DES ANNEXES

ANNEXE I : Dessin de presse

ANNEXE II : Schéma de distinction entre système expert et apprentissage automatique

ANNEXE III : Carte des possibilités d'apprentissage machine

ANNEXE IV : Le principe de gradation dans l'emploi de la force

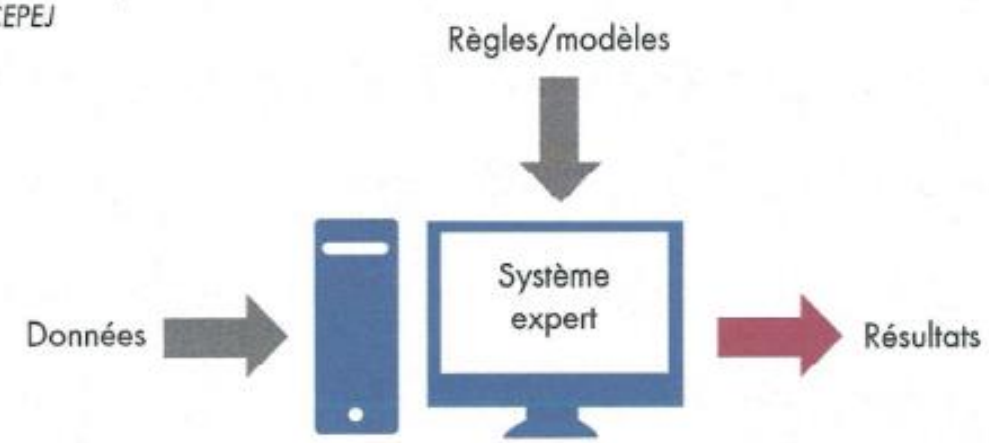
ANNEXE V : Illustration du biais en apprentissage-machine

ANNEXE I

Source : Auteur anonyme

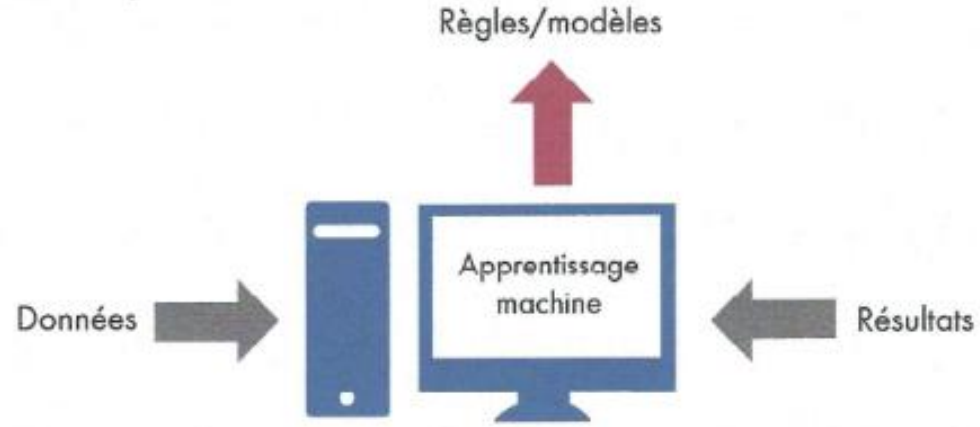
ANNEXE II

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.

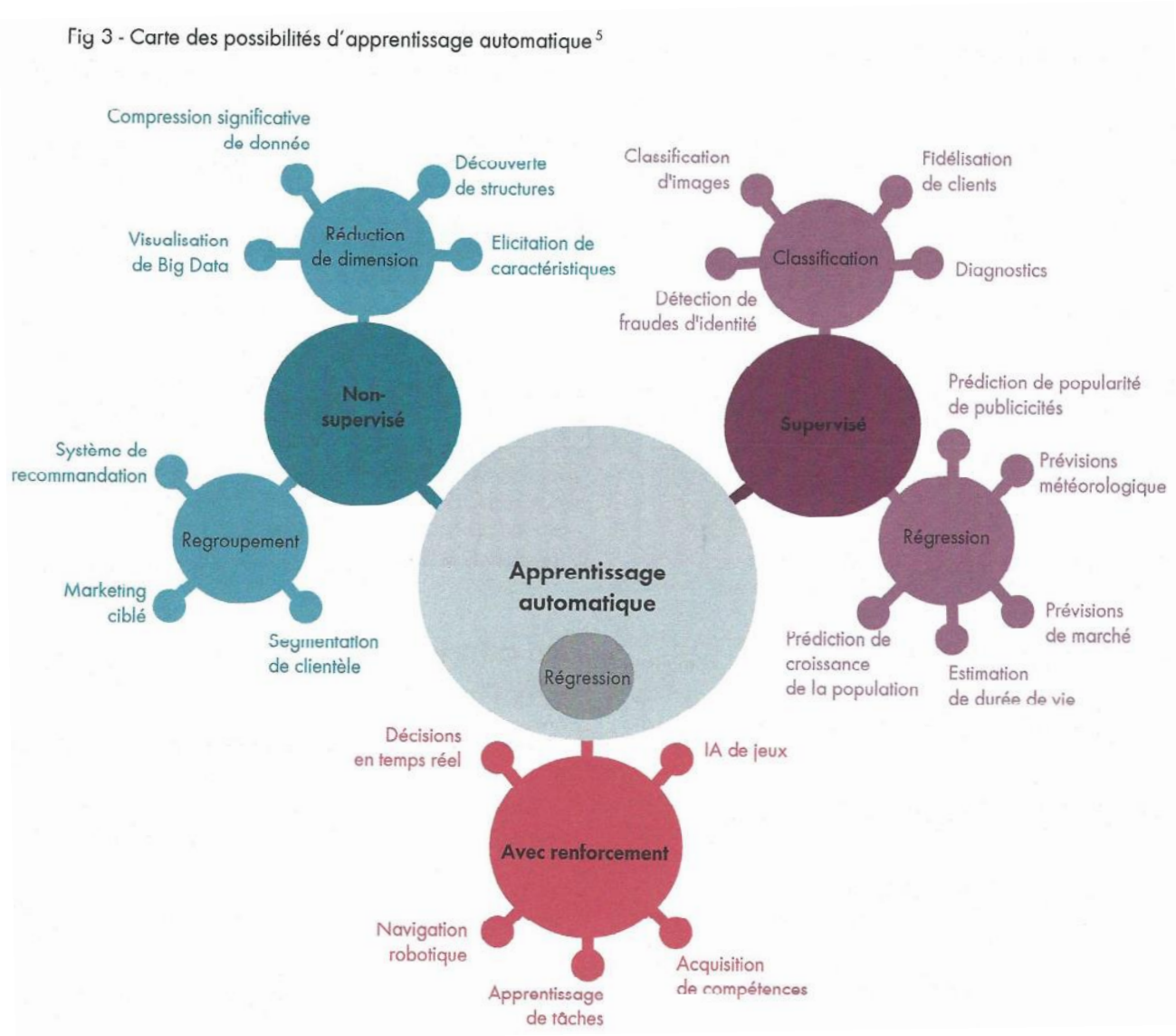
Fig 2 - Aprentissage automatique
Figure CEPEJ



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.

Source : Patrick TOURON, « L'impact de l'intelligence artificielle dans la conduite de l'enquête judiciaire », *Cahiers de la sécurité et de la justice*, mars 2020, n°47, p. 64

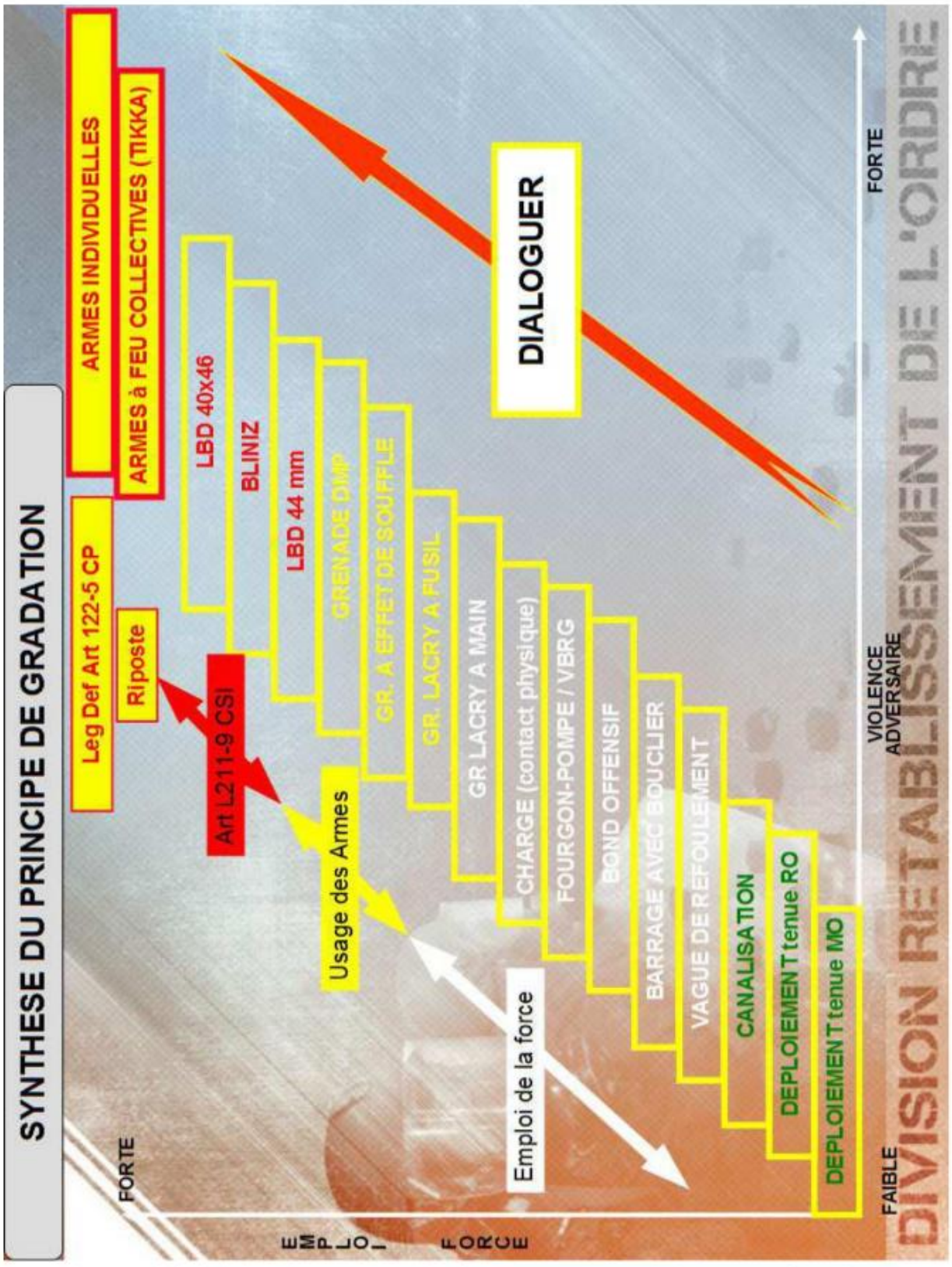
ANNEXE III



Source : Patrick TOURON, « L'impact de l'intelligence artificielle dans la conduite de l'enquête judiciaire », *Cahiers de la sécurité et de la justice*, mars 2020, n°47, p. 65

ANNEXE IV

LE PRINCIPE DE GRADATION DANS L'EMPLOI DE LA FORCE



Source : direction générale de la gendarmerie nationale ; réponse au questionnaire de la commission d'enquête.

ANNEXE V

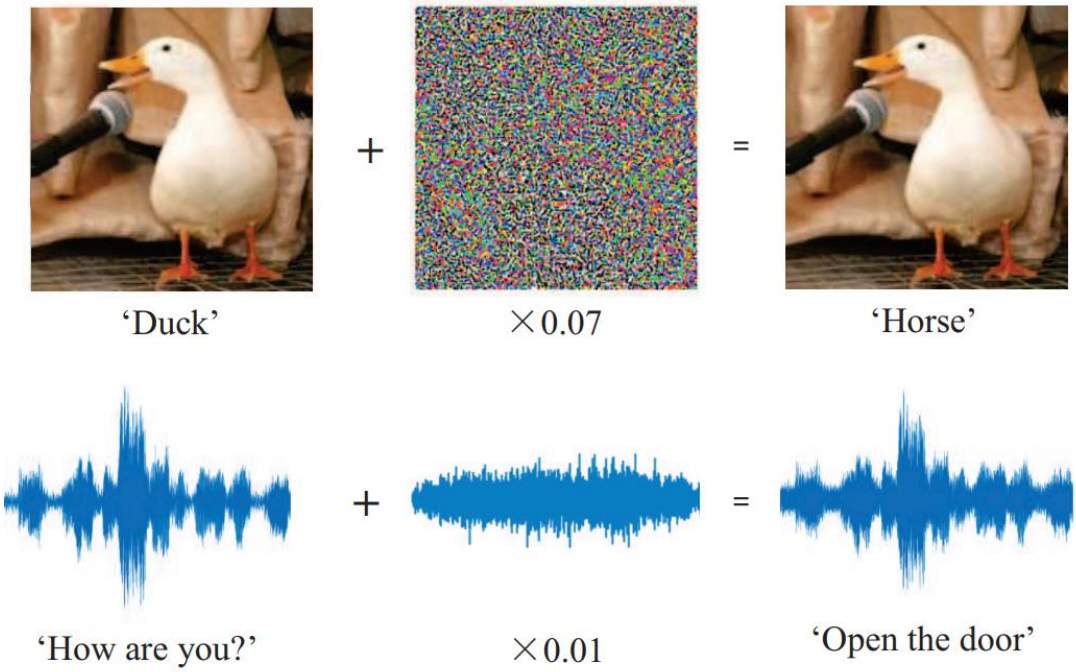


Illustration du procédé « exemples contradictoires » en apprentissage-machine. Les études montrent qu'en ajoutant une perturbation imperceptible, mais soigneusement préparée, une attaque peut mener avec succès le modèle d'apprentissage-machine à faire une mauvaise prédiction. De telles attaques ont été réalisées sur de l'analyse d'image par ordinateur, et sur de la reconnaissance vocale.

Source : Yuan GONG et Christian POELLABAUER, « An overview of vulnerabilities of voice controlled systems », *First international workshop on security and privacy for the Internet-of-Things*, 2018

BIBLIOGRAPHIE

Textes juridiques

Constitution, 1958

Convention européenne de sauvegarde des droits et l'Homme et des libertés fondamentales, 1950

Traité sur l'Union européenne, 1992

Code pénal

Code de la sécurité intérieure

Règlement (UE) 216-679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016

Décret-loi *(abrogé)* du 23 octobre 1935 portant réglementation des mesures relatives au renforcement du maintien de l'ordre public

Loi n°78-17 du 06 janvier 1978

Loi n°95-73 du 21 janvier 1995 *(modifiée)* d'orientation et de programmation relative à la sécurité

Décret n°2013-728 du 12 août 2013 portant organisation de l'administration centrale du ministère de l'intérieur et du ministère des outre-mer

Jurisprudence

Conseil constitutionnel, décision n°80-127 DC du 20 janvier 1981, *Loi renforçant la sécurité et protégeant la liberté des personnes*, cons. 56

Conseil constitutionnel, décision n°82-141 DC du 27 juillet 1982, *Loi sur la communication audiovisuelle*

Conseil constitutionnel, décision n°85-187 DC du 25 janvier 1985, *Loi relative à l'état d'urgence en Nouvelle-Calédonie et dépendances*

Conseil constitutionnel, décision n°94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*

Conseil constitutionnel, décision n°2010-613 DC du 07 octobre 2010, *Loi interdisant la dissimulation du visage dans l'espace public*

Conseil constitutionnel, décision n°2018-765 DC du 12 juin 2018, *Loi relative à la protection des données personnelles*

Conseil constitutionnel, décision n°2019-780 DC du 04 avril 2019, *Loi visant à renforcer et garantir le maintien de l'ordre public lors des manifestations*

Conseil d'État, 28 mai 1971, *Ville nouvelle Est*

Conseil d'État, ass., 27 octobre 1995, *Commune de Morsang-sur-Orge*, 136727

Conseil d'État, ord., 18 mai 2020, *Ligue des droits de l'Homme et autres*

Cass., 1ère civ., 06 octobre 2011, pourvois n°10-21822 et 10-21823

Cour de cassation, chambre criminelle, 09 février 2016, 14-82.234, bull.

Tribunal des conflits, 17 juin 2013, M. Bergoend c/ Société ERDF Annecy Léman

Rapports d'autorités publiques et projets de lois

M. Pascal POPELIN, « Rapport d'enquête sur les missions et modalités du maintien de l'ordre républicain dans un contexte de respect des libertés publiques et du droit de manifestation », XIVème législature, 21 mai 2015, n°2794

Cédric Villani, *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*, 2018

Rapport législatif du Sénat, Proposition de loi visant à interdire l'usage des lanceurs de balles de défense dans le cadre du maintien de l'ordre et à engager une réflexion sur les stratégies de désescalade et les alternative pacifiques possible à l'emploie de la force publique dans ce cadre, 20 février 2019

Rapport du Défenseur des droits, « Le maintien de l'ordre au regard des règles de déontologie », déc. 2017

Stratégie nationale de recherche en intelligence artificielle, 2018

Livre blanc sur l'intelligence artificielle : une approche européenne sur l'excellence et la confiance

Rapport de la CNIL, *Commet permettre à l'homme de garder la main ?*, 2017

Ouvrages généraux

Jacques BAUD, *La guerre asymétrique ou la défaite du vainqueur*, Éditions du Rocher, 2003, p. 110-114

Alain BENSOUSSAN, Jérémy Bensoussan, *IA, robots et droit*, Larcier, 2019

Fabien CARDONI, *La garde républicaine d'une République à l'autre (1848-1871)*, PUR, 2008

Dominique ROUSSEAU, Pierre-Yves GAHDOUN, Julien BONNET, *Droit du contentieux constitutionnel*, Montchrestien, 11è éd., 2016

Eric SADIN, *L'intelligence artificielle ou l'enjeu du siècle, anatomie d'un antihumanisme radical*, L'échappée, 2018

Max WEBER, *Le Savant et le Politique*, 1919

Périodiques et revues spécialisées

Cédric ABRIAT, « L'intelligence artificielle, nouvel indicateur de puissance ? », *Défense et sécurité internationale*, juillet-août 2019

Frank AUTRE, Kunal ARYA, Ryan BABBUSH, « Quantum supremacy using a programmable superconducting processor », *Nature*, n°574, 2019Étienne PICARD, *JCP G*, 1995, I. 155

Egon BITTNER, « Florence Nightingale à la poursuite de Willie Sutton. Regards théoriques sur la police, *Déviance et Société*, vol. 25, n°3, 2001

Jean-Paul BRODEUR, « Le travail d'Egon Bittner, une introduction à la sociologie de la force institutionnalisée », *Déviance et Société*, vol. 25, n°3, 2001

Marc de FRITSCH, Ariane BITOUN, « Commander avec l'IA, une aide à la conception et à l'évaluation des modes d'action », *RDN*, n°820, 2019

Rémy HÉMEZ, « Tactique : le devoir d'imagination », *RDN*, n°704, 2008

Tony JEFFERSON, *The case against paramilitary policing*, Open university press, 1990

Fabien JOBARD, « La militarisation du maintien de l'ordre, entre sociologie et histoire », *Déviance et Société*, vol. 32, n°1, 2008

Dominique LAMBERT, « Éthique et autonomie : la place irréductible de l'humain », *RDN*, n°820, 2019

Jacques de MAILLARD, « Relations police-population », *DéfiS*, n°9, décembre 2018

Philippe MASSONI, « Défense des libertés et ordre public à Paris », *Administration*, 1996, n°173

Nicolas MAZZUCCHI, « Intelligence artificielle et industrie de défense, le grand défi », *R.D.N.*, n°820, 2019

Cathy O'NEILL, *Weapons of math destruction : how big data increases inequality and threatens democracy*, Broadway Books, 2017

Judea PEARL et Dana MACKENZIE, *The book of why : the new science of cause and effect*, Basic Books, 2018

Peter WADDINGTON, « Toward paramilitarism ? Dilemnas in the policing public order », *British Journal of Criminology*, 1987

Actes de colloques, enseignements et travaux universitaires

Olivier LE BOT, « La liberté de manifestation en France : un droit fondamental sur la sellette ? », *La liberté de manifester et ses limites : perspective de droit comparé*, Actes du colloque des 18 et 19 mars 2016

Florian POULET, *Cours de politiques de sécurité publique*, Master 2 Sécurité et défense, 2019-2020

Colloque Sécurité et Justice, *Le défi de l'intelligence artificielle*, INHESJ, 07/11/2019

Articles de presse et communications officielles

Florence PARLY, Discours « Intelligence artificielle et défense », ministre des Armées, Saclay, 05 avril 2019

Cédric O, « Expérimenter la reconnaissance faciale est nécessaire pour que nos industriels progressent », *Le* Monde, 14/10/2019

Henri VERDIER, « La transformation de l'État doit surtout être organisationnelle et managériale », *Les Échos*, 22/07/2019

Général Marc WATIN-AUGOUARD, « Sauvegardons la militarité de la gendarmerie », *Le Journal du Dimanche*, 08 juin 2019

« La somme exorbitante des dégradations causées par les Gilets jaunes », *Capital*, 19/03/2019

« L'État vend aussi vos données », *Le* Parisien, 19/05/2015 (http://www.leparisien.fr/week-end/l-etat-aussi-vend-vos-donnees-19-05-2015-4784563.php)

https://www.elysee.fr/emmanuel-macron/2018/03/29/discours-du-president-de-la-republique-sur-lintelligence-artificielle

https://www.sciencesetavenir.fr/high-tech/intelligence-artificielle/emmanuel-macron-annonce-le-budget-alloue-pour-le-plan-intelligence-artificielle-de-la-france_122578

https://www.usinenouvelle.com/editorial/emmanuel-macron-annonce-la-creation-de-deux-centres-d-expertise-en-ia-a-paris-et-montreal.N899464

https://www.lefigaro.fr/flash-eco/tracking-le-gouvernement-veut-garder-la-maitrise-du-developpement-face-a-google-et-apple-20200415

https://www.lesechos.fr/tech-medias/intelligence-artificielle/macron-appelle-a-une-strategie europeenne-de-lintelligence-artificielle-1144356

https://www.lesechos.fr/industrie-services/air-defense/big-data-faute-de-solution-francaise-les-services-secrets-signe-a-nouveau-avec-palantir-1151255

https://www.lesechos.fr/tech-medias/intelligence-artificielle/intelligence-artificielle-bruxelles-promet-un-encadrement-bien-reel-1173157

https://www.marianne.net/societe/lancement-de-la-reconnaissance-faciale-en-france-mais-qu-allons-nous-faire-dans-cette-galere

http://www.leparisien.fr/video/video-macron-j-attends-de-nos-policiers-la-plus-grande-deontologie-14-01-2020-8235834.php

http://www.leparisien.fr/faits-divers/des-robots-testes-a-la-place-des-juges-dans-les-cours-d-appel-de-rennes-et-douai-30-10-2017-7362198.php

https://toulouse.latribune.fr/entreprises/business/2015-02-02/espionnage-industriel-et-secret-des-affaires-les-pme-francaises-sont-elles-en-danger.html

https://www.ledauphine.com/france-monde/2017/10/08/notre-capacite-d-attention-plus-faible-que-celle-du-poisson-rouge

https://www.futura-sciences.com/tech/questions-reponses/intelligence-artificielle-intelligence-artificielle-six-usages-quotidien-11341/

https://www.leslivresblancs.fr/dossier/ia-lintelligence-artificielle-ou-en-sommes-nous

https://www.bpifrance.fr/A-la-une/Dossiers/L-intelligence-artificielle-est-synonyme-de-rentabilite-accrue-pour-les-entreprises

https://interstices.info/marvin-minsky-un-pere-visionnaire-de-lintelligence-artificielle/

https://www.zdnet.fr/actualites/l-europe-devoile-sa-grande-strategie-en-matiere-d-intelligence-artificielle-39899357.htm

https://lessor.org/a-la-une/lintelligence-artificielle-au-secours-du-maintien-de-lordre/

Sources diverses, sites institutionnels

Joseph HENROTIN, « Les promesses de l'intelligence artificielle », *Le Collimateur*, IRSEM, 09/04/2019

Pierre MAZEAUD, *Libertés et ordre public*, site Internet du Conseil constitutionnel, 2003

La République des lettres, republique-des-lettres.fr/190-paul-virilio.php

Publications du Centre de recherche de l'EOGN

https://erewerra2.files.wordpress.com/2018/07/plan-stratc3a9gique-de-la-recherche-et-de-linnovation-1.pdf

https://thispersondoesnotexist.com/

https://www.interieur.gouv.fr/Archives/Archives-des-actualites/2018-Actualites/Naissance-du-CSIA

https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN

TABLE DES MATIÈRES

RÉSUMÉ / *ABSTRACT*……5

TABLE DES ABRÉVIATIONS……..6

SOMMAIRE……..7

INTRODUCTION GÉNÉRALE……..……8

Section 1 – L'intelligence artificielle : un moteur de développement global……..…8

Section 2 – Des notions contingentes et évolutives……10

§1. L'intelligence artificielle : une technologie encore en construction…….10

§2. L'instabilité notionnelle du maintien de l'ordre……...11

A. Une construction historique de l'ordre public aujourd'hui inachevée……..12

B. De la sauvegarde de l'ordre public au maintien de l'ordre public……13

Section 3 – Enjeux partagés et complémentaires par l'IA et le maintien de l'ordre public……15

TITRE I – UNE TECHNOLOGIE À FORT POTENTIEL OPÉRATIONNEL……18

Chapitre 1 – UN OUTIL STRATÉGIQUE VALORISANT L'ACTION DES FORCES DE MAINTIEN DE L'ORDRE……..……20

Section 1 – Un outil stratégique en matière de préservation et d'expression des libertés publiques……...……...…20

§1. L'intelligence artificielle au service de la liberté de manifester……..…….20

A. Une liberté constitutionnellement garantie……...20

B. Une approche renouvelée pour le décideur…….…..21

§2. Une garantie supplémentaire à la préservation de l'ordre public…….…23

A. Le régime actuel de déclaration : préalable à un exercice apaisé de la liberté de manifester……..23

B. L'intelligence artificielle : un atout dans l'anticipation stratégique et la préparation opérationnelle……25

Section 2 – L'outil du renouveau du maintien de l'ordre achevant sa « déthéâtralisation » ?.....29

§1. D'une consolidation du cadre actuel……30

A. Un usage de l'IA par les forces spécialisées, garantie d'une efficacité de son emploi…..…30

B. D'un encadrement de la foule à son accompagnement : dissuader autrement……32

1. Adapter la gestion du maintien de l'ordre à l'environnement : l'IA des objets…….33

2. D'une logique de stock à une logique de flux : une nouvelle appréhension des opérations de maintien de l'ordre facilitée par l'intelligence artificielle…….35

C. Un outil favorable, par conception, à un usage proportionné et gradué de la force ……39

§2. … à un renouveau de la doctrine du maintien de l'ordre à la française……40

A. L'apprentissage de la codécision……..41

B. Prendre le contrôle de la « profondeur stratégique » ? ……42

C. Vers une gestion individualisée des foules, affirmation d'une judiciarisation du maintien de l'ordre ? …….……43

Section 3 – Une stratégie nationale industrielle et de ressources humaines à développer..46

§1. La nécessité de s'appuyer sur une base industrielle et technologique forte et « souveraine »……. ……..46

§2. L'exigence d'un travail en plateau, protection et ouverture à une interopérabilité européenne……49

§3. Développer et conserver un socle de compétences techniques en interne……..53

Chapitre 2 – UN CADRE JURIDIQUE À ADAPTER AUX MODALITÉS……...…56

Section 1 : Un cadre juridique protecteur des libertés en apparente phase avec l'IA…….57

§1. La régulation des données : une problématique déjà ancienne……57

A. Les données à caractère personnel de la loi « Informatique et Libertés » au RGPD……57

B. Le code de la sécurité intérieure et le régime dual des images recueillies sur la voie publique…….59

§2. Un encadrement normatif du traitement algorithmique constamment renforcé……61

Section 2 : La nécessité de consolider ce cadre juridique : se défaire des « angles morts »……..63

§1. Une répartition des compétences entre secteurs privé et public facilitée par le droit de l'UE……...…64

A. Le principe : une interdiction du traitement des données « sensibles » ……..64

B. Des exceptions limitatives et conditionnées…….…66

§2. Une temporalité technologique pressant le législateur……67

A. La massification des données en accès libre…….67

B. La diversification croissante des sources de données……68

§3. Vers une délégation totale au privé de la création des algorithmes ? …….70

TITRE II – UN DÉVELOPPEMENT TECHNOLOGIQUE À ENCADRER……73

Chapitre 1 – LES PRÉREQUIS STRUCTURANTS À UNE INTELLIGENCE ARTIFICIELLE RAISONNÉE DU MAINTIEN DE L'ORDRE……...75

Section 1 – La recherche d'une efficacité opérationnelle dans un cadre éthique……75

§1. Catégoriser les usages pour faciliter la compréhension situationnelle……75

§2. Une réflexion éthique à intégrer……..78

A. Pour un développement des structures de réflexion…….78

B. Programmer l'éthique ? ……79

Section 2 – La nécessité d'une intelligence artificielle robuste, tant structurellement que matériellement……..……...81

Section 3 – L'explicabilité : enjeu majeur de l'acceptabilité d'une telle technologie……83

§1. Les clefs du socle indispensable de la confiance…….85

§2. Les conséquences d'un manque de transparence dans la mise en œuvre de l'IA……87

Chapitre 2 – PROTÉGER DES MÉSUSAGES : LES GARANTIES JURIDICTIONNELLES ET NON JURIDICTIONNELLES……89

Section 1 – Quelle protection du juge dans le développement et l'accompagnement de la technologie ? ……89

§1. Une présence au long cours du juge constitutionnel……...90

§2. Un juge européen à préparer……91

§3. L'intervention duale du juge judiciaire……92

§4. Vers un bloc de compétence pour le juge administratif ? ……93

Section 2 – La place de choix des autorités administratives indépendantes……....94

Section 3 – La militarité des forces de maintien de l'ordre au service de la responsabilisation……....95

CONCLUSION GÉNÉRALE……98

TABLE DES ANNEXES……...100

BIBLIOGRAPHIE……106

TABLE DES MATIÈRES……111