# L'INTELLIGENCE ARTIFICIELLE AU SERVICE D'UNE SÉCURITÉ INTÉRIEURE INNOVANTE

SERVICE DE LA TRANSFORMATION
GENDARMERIE NATIONALE

Après des décennies où l'intelligence artificielle a connu une évolution très disparate, elle est arrivée aujourd'hui à un niveau de maturité qui la place comme un vecteur d'innovation sans précédent. Ce n'est pas un hasard si nombre de pays ont consacré une stratégie de développement spécifique à l'IA, elle ouvre en effet des opportunités sans précédent en matière d'innovation dans des domaines des plus divers à la condition d'une exploitation raisonnée dans un cadre éthique et juridique établi. À propos de l'IA, Arvind Krishna, directeur d'IBM Research énonce : "Ce qui était jugé impossible il y a quelques années ne devient pas seulement possible, mais devient très rapidement nécessaire et attendu." L'IA semble être en mesure de résoudre des problèmes jusque-là sans solution et dans un temps record. La vague actuelle des avancées en IA n'aurait pas été possible sans la convergence de facteurs qui se sont combinés pour créer l'équation nécessaire à la croissance de l'IA : l'essor du big data combiné à l'émergence de puissants processeurs graphiques (GPU) pour les calculs complexes, la renaissance de méthodes d'IA, veilles de plusieurs décennies : l'apprentissage profond. À cela s'ajoute pour les années à venir, l'essor de la 5G et l'apparition de la physique quantique dans le monde computationnel. Face à ces nouvelles émergences, le domaine de la sécurité ne peut en retard au risque de laisser se développer une sécurité gouvernée par les GAMAM (Google Amazon, Meta, Apple, Microsoft) et autres BATX (Baidu, Alibaba, Tencent, Xiaomi) comme au risque de ne pouvoir faire face à une criminalité de plus en plus technologique. La Gendarmerie nationale s'est engagée dans la voie de l'IA pour, dès à présent préparer le futur, selon l'ambition de son plan stratégique Gend 20.24.

**PATRICK PERROT**

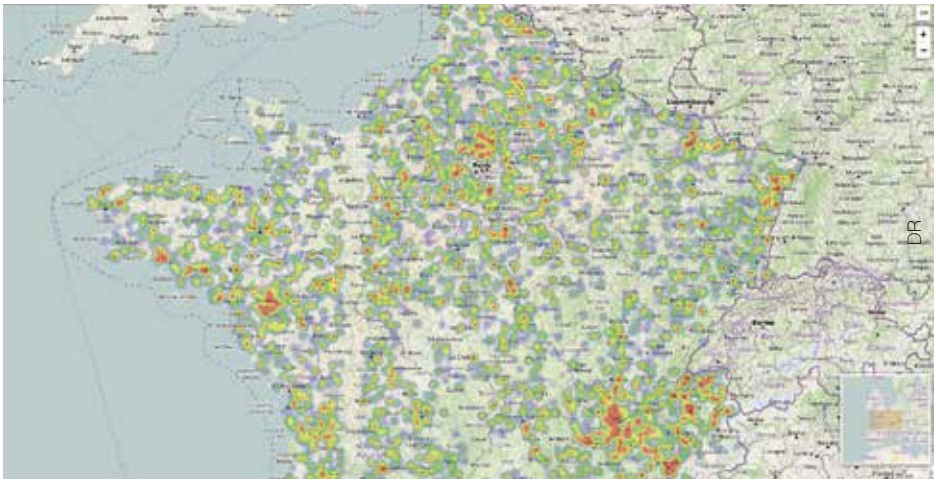
**Général de brigade, coordinateur pour l'Intelligence Artificielle, chargé de la stratégie de la donnée. Service de la Transformation Gendarmerie nationale**

## L'IA, une discipline complexe et souvent mal interprétée

Avant d'en analyser les enjeux et de présenter la stratégie déployée au sein de la Gendarmerie, il peut être utile de comprendre ce qu'est l'intelligence artificielle. Selon la définition communément admise, l'IA est « un ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence humaine ». Mais simuler l'intelligence humaine n'est pas en réalité l'objectif de l'IA qui a déjà largement supplanté les capacités humaines en terme de célérité de calcul, de traitement et d'exécution et de capacité d'anticipation sur des applications très précises. L'IA doit être perçue

comme un amplificateur de l'intelligence humaine développé à partir de méthodes mathématiques auto apprenantes.

Mais les mathématiques à ce jour ne sont pas parvenues à résoudre le problème de la non linéarité en grande dimension.




Carte d'analyse prédictive de la délinquance

Elle est donc un agglomérat de méthodes mathématiques qui conviennent plus ou moins à la modélisation du problème posé. La question sous-jacente à l'utilisation de l'IA est donc d'abord mathématique. Il s'agit de savoir comment approximer des données non linéaires dans un espace de grande dimension. Pour accomplir ce « miracle », l'IA fait appel à de nombreuses disciplines : l'analyse harmonique, la morphologie, les statistiques, les probabilités, la théorie de la décision, la géométrie, les systèmes dynamiques… de toutes ces méthodes, la plus pertinente pour éclairer le mystère mathématique qui entoure l'IA est certainement à rechercher du côté de la géométrie par la caractérisation de formes invariantes dans des données communes.

C'est du côté de l'observation et donc de la physique qu'il a fallu s'orienter pour trouver une solution : l'apprentissage automatique et notamment via sa dernière déclinaison l'apprentissage profond.

L'apprentissage profond a connu depuis les années cinquante des phases de rebond et d'hibernation pour s'imposer totalement en 2012 lors du concours de reconnaissance d'images « Image Net ». Avec les réseaux de neurones profonds, le champ des possibles semble vertigineux tant les applications apparaissent performantes notamment lorsque les données sont présentes en grand nombre. Le principe de base de ces réseaux pourrait être le principe d'Euclide : « diviser pour régner ». En effet, du perceptron en 1957 aux

réseaux de neurones profonds, plus d'un demi-siècle s'est écoulé pour, finalement la mise en pratique du principe euclidien énoncé. Pour simplifier, nous pourrions dire que plus un réseau est profond, plus il y a de couches, plus le problème est réduit ou divisé et plus la solution est généralisable. Il faut néanmoins se prévenir de certaines difficultés comme un sur-apprentissage qui nuirait à la généralisation. Un réseau de neurone est en quelque sorte un compromis entre un biais et une variance. Ce compromis consiste à minimiser simultanément deux sources d'erreurs en déterminant un équilibre entre la performance de la prédiction et la capacité à généraliser au-delà de l'échantillon d'apprentissage.

Les réseaux de neurones profonds sont particulièrement adaptés à représenter le monde non linéaire dans lequel nous évoluons et surtout à généraliser un modèle appris sur des données inconnues. Ils sont utilisés pour des tâches des plus variées : classifier, segmenter, simuler, anticiper, identifier… La question demeure de savoir pourquoi les réseaux de neurones profonds sont aussi efficaces pour reconnaître un chat dans une image, pour traduire un langage parlé en texte ou encore pour conduire un véhicule. La réponse aujourd'hui est que les principes mathématiques fondamentaux sous-jacents et les lois physiques régissant ces différentes applications sont les mêmes notamment après la réduction de l'espace des données et la mise en évidence d'invariants. Les réseaux neuronaux profonds permettent d'atteindre les régularités d'une architecture très complexe.

L'IA est donc avant tout une solution empirique pour faire face à un problème théorique. Elle permet à partir de données observées de construire des modèles qui parviendront à déterminer les structures identifiantes des données.

### Quels sont les enjeux d'avenir de l'IA en matière de sécurité ?

Les enjeux en matière d'intelligence artificielle sont pluriels pour les forces de sécurité intérieure. Ils concernent les questions de souveraineté, de présence sur les nouveaux territoires numériques, de protection de la population, de l'égalité du service à l'usager.

Les réseaux, un enjeu fondamental

Alors que l'IA est parfois difficile à définir ou à comprendre, elle est devenue incontestablement un enjeu stratégique pour les nations tant sur les applications militaires que civiles. Les États sont évidemment concernés par ce développement et nombre de nations ont initié des plans stratégiques en IA. Mais le domaine est aujourd'hui largement dominé par les grands acteurs du numérique relevant davantage de la sphère privée. Nous sommes dans une période de transition où

la souveraineté des États est disputée par le pouvoir des multinationales.


Comparaison des faits réels de délinquance et des faits prédits

Dans le domaine de la sécurité en particulier, cette transition peut avoir des conséquences majeures, génératrices d'un transfert d'activités régaliennes des États vers les géants du numérique. C'est ainsi que l'engagement des forces de sécurité en IA est un impératif pour une protection des libertés individuelles comme des données à caractère personnel.

L'émergence des villes et territoires connectés illustre parfaitement l'urgence pour les pouvoirs publics de trouver leur place dans cet écosystème. Comprendre l'IA, en maîtriser son fonctionnement est un enjeu de souveraineté majeur qui doit dès à présent concerner les forces de sécurité intérieure. Il ne s'agit pas pour le service public d'être leader sur le plan technologique face à des opérateurs privés déjà très puissants et hégémoniques mais bien de conserver la gouvernance des applications, et d'en mesurer les conséquences.

Au-delà des territoires connectés se profilent aussi de nouveaux espaces virtuels dont l'impact dans la vie quotidienne sera bien réel. Il n'est pas surprenant de voir aujourd'hui Facebook devenir Meta ou Microsoft proposer des espaces professionnels virtuels même si ces territoires virtuels sont nés au début du siècle. Ces espaces devraient redessiner les relations humaines individuelles comme les interactions sociales. Ils constituent également un terreau particulièrement favorable au développement sans impunité d'une nouvelle forme de criminalité. Ils peuvent, par manque de présence des FSI, devenir des zones interlopes propices au dévelop-

pement d'une criminalité sexuelle, d'opérations de blanchiment d'argent, de trafics de biens ou encore de simulation d'actions délinquantes voire terroristes.

L'IA constitue ainsi un enjeu fondamental en matière de développement de la criminalité qu'elle soit de droit commun ou organisée. La délinquance a connu une mue considérable depuis l'avènement des outils numériques à disposition et l'IA démultiplie les possibles en accroissant les zones d'impact pour une minimisation du risque. Il est aujourd'hui largement accessible aux criminels non seulement de tracer le déplacement d'individus comme de marchandises mais aussi de les anticiper. Il est également possible de diffuser de fausses informations très réalistes à grande échelle ou encore de compromettre la réputation d'un individu et les opportunités criminelles ne manquent pas. L'enjeu réside alors dans l'asymétrie des possibilités offertes aux criminels et la capacité d'anticipation comme de réponse des FSI.

Le service offert à la population constitue lui aussi un enjeu majeur pour la Gendarmerie nationale, très attachée à la notion de redevabilité vis-à-vis du citoyen. La question est de pouvoir distribuer une protection égale en termes de moyens quelle que soit la zone sur le territoire. Il ne peut y avoir de fracture entre les métropoles et les territoires en matière d'offre de protection. L'IA doit contribuer à cette ambition en aidant à mieux comprendre les particularités territoriales, en anticipant les besoins des élus comme des citoyens, en rendant accessible les services à l'usager.

Pour faire face à ces différents enjeux de l'IA, la Gendarmerie développe une stratégie plurielle. Le principe est de considérer l'IA comme un vecteur de transformation de notre organisation et de nos modes d'action pour optimiser la protection des populations. Il s'agit désormais de nous placer en proaction plutôt qu'en seule réaction. C'est une véritable transformation dans l'appréhension de la délinquance : prévenir, agir, réagir. En réalité, nous n'avons plus le choix pour faire face aux enjeux et défis de demain. Mais il s'agit aussi de proposer une exploitation de l'IA raisonnée et progressive. L'ensemble du spectre fonctionnel doit permettre d'accroître la sécurité des citoyens, de prévenir les usages malveillants de l'IA, de faciliter les démarches de l'usager, mais aussi d'améliorer le travail du personnel de la gendarmerie.

## Une stratégie IA résolument orientée vers l'innovation

La Gendarmerie nationale a engagé une stratégie en matière d'intelligence artificielle qui d'emblée considère l'IA, non comme un simple outil informatique mais comme un vecteur d'innovation en mesure de transformer l'organisation comme les processus métiers. L'ambition est d'envisager l'IA dans la plénitude de sa polysémie en appréhendant les aspects de formation, d'éthique et de régulation, de développement, de recherche mais aussi de partenariats pour proposer l'exploitation d'une IA de confiance au profit de tous comme de chacun.

En matière de formation, la Gendarmerie est à l'origine de la création de la première chaire qui lie l'IA et la Sécurité. Elle a été créée en partenariat avec l'Institut Supérieur d'Électronique de Paris (ISEP) et organise des séminaires sur les applications de l'IA en matière de protection des populations comme des travaux de recherche appliquée au champ de la sécurité. La formation, c'est aussi la réalisation d'un MOOC « Objectif IA » par 87 % des gendarmes, c'est encore une revue bimestrielle, « Cultur'IA », qui diffuse une information sur les grands principes et acteurs de l'IA mais aussi sur les applications dans le domaine de la sécurité intérieure. La formation est au cœur de la politique de gestion des compétences de la Gendarmerie et constitue pour l'intégration de l'intelligence artificielle dans les processus métiers un enjeu fondamental. L'ambition est de former le personnel à utiliser, à conduire ou à développer des applications pour prévenir tout effet de « boîte noire » et ainsi :

- comprendre l'interprétation d'un système d'intelligence artificielle c'est-à-dire être capable de comprendre le pourquoi et le comment du résultat du système issu d'un contexte spécifique. En d'autres termes, il s'agit de comprendre la rationalité qui se cache derrière la décision et le comportement du système.

- comprendre la justification à la fois du processus d'implémentation et du résultat c'est-à-dire le bien-fondé de l'application. Cela nécessite notamment de vérifier l'aspect non discriminatoire et la loyauté du système. Cet aspect est très lié aux données utilisées.

En matière d'éthique, la Gendarmerie est également pionnière par la réalisation d'une charte Éthique applicable à l'ensemble de ses applications déployées comme en cours de développement. L'objectif est de placer la confiance au cœur des enjeux en s'appuyant sur les notions de responsabilité, de transparence, de connaissance, de loyauté et de respect. Exploiter le potentiel de l'intelligence artificielle dans le domaine de la sécurité est un atout considérable à la condition de s'appuyer sur un cadre éthique assuré pour un meilleur service au citoyen. L'intelligence artificielle doit permettre, là encore, d'« humaniser » la mission de sécurité et de secours en apportant plus de temps aux acteurs opérationnels pour gérer les questions qui relèvent de l'intelligence humaine. Celle-ci demeure fondamentale pour superviser, contextualiser, valider ou rectifier les analyses produites en vue d'une prise de décision.

En matière de recherche et de développement, la Gendarmerie est aussi la première institution à avoir développé en interne et déployé une application d'analyse prédictive de la délinquance avec pour objectif d'adopter une posture proactive en complémentaire de sa réactivité face aux évènements générateurs de crise ou aux actes de délinquance. Avoir un temps d'avance est un concept militaire qui fournit un avantage sur l'adversaire, aujourd'hui c'est même devenu un impératif pour la Gendarmerie nationale. Elle s'est également engagée dans des développements originaux d'authentification des hyper-trucages mieux connus dans leur traduction anglaise de « deepfakes » en exploitant les

réseaux génératifs adverses. L'exploitation de ces méthodes se révèlent particulièrement performantes dans la détection des deepfakes mais aussi pour lutter contre le caractère potentiellement discriminatoire des algorithmes, encore un travail précurseur de l'Institution. Ces méthodes originales font l'objet d'évaluation comme de publications afin de développer des outils validés scientifiquement et contrôlés en continu. Dans le domaine de la recherche, il est essentiel de confronter les travaux comme d'échanger sur les méthodes novatrices. C'est la raison pour laquelle la Gendarmerie entretient de nombreux liens avec les centres de recherche en IA que ce soit avec les Instituts interdisciplinaires en IA, ANITI à Toulouse ou 3IA Côte d'Azur mais aussi avec le Centre de Recherche des Radicalisations et de leurs Traitements de l'université de Paris sans compter les travaux menés avec l'ISEP ou encore la participation à la Chaire « Smart City et Philosophie » de l'Institut Méditerranéen du Risque de l'Environnement et du Développement Durable.

Parce que l'IA nécessite de la transparence, la Gendarmerie a développé une politique partenariale dynamique en travaillant en proximité avec le Hub France IA dans le domaine de l'IA appliquée aux ressources humaines, avec l'Institut EuropIA pour rendre accessible l'IA au plus grand nombre, avec l'Institut Sapiens dans le domaine de l'éthique mais aussi au niveau international en coprésidence du groupe relatif au développement de la stratégie en IA comme aux travaux en matière d'anticipation et d'éthique à l'échelle européenne. L'objet de ces partenariats est d'échanger sur les bonnes pratiques applicatives, de s'enrichir mutuellement et de révéler aussi les enjeux comme les difficultés rencontrées autour des méthodes utilisées.

Ainsi, l'intelligence artificielle constitue une opportunité considérable d'innovation pour une meilleure protection des populations en développant une capacité proactive complémentaire à la réactivité nécessaire des forces de sécurité intérieure. Elle offre la possibilité de gagner à la fois en connaissance des besoins de l'usager comme du personnel et en célérité comme en objectivité dans la prise de décision. Il est pourtant nécessaire pour atteindre cet objectif d'appréhender l'intelligence artificielle dans la diversité de ses composantes et d'envisager des applications raisonnées et progressives dans un cadre éthique et juridique défini. Comprendre l'intelligence artificielle est la condition nécessaire et suffisante à son développement au sein de l'administration publique mais aussi à la sauvegarde d'activités régaliennes pour lesquelles l'État est aujourd'hui de plus en plus concurrencé par les géants du numérique dans l'offre de services publics. Les forces de sécurité n'ont d'autres choix que d'investir dans l'intelligence artificielle afin de préserver les libertés individuelles et collectives et maintenir un haut niveau de protection des populations. La Gendarmerie a intégré dans sa démarche d'innovation la nécessaire anticipation préalablement à la préparation de la mission, l'IA est un formidable vecteur pour participer à cette ambition.