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

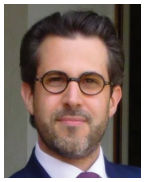
Floran VADILLO

Alors que des algorithmes permettent d'optimiser les processus industriels, de guider la prise de décisions stratégiques, d'identifier une fraude bancaire ou encore de contenir la cybercriminalité, certains envisagent déjà des applications au domaine de l'enquête pour favoriser la résolution d'affaires, voire anticiper un passage à l'acte. En effet, l'intelligence artificielle (IA) investit progressivement de nombreux secteurs d'activité, permettant d'élargir le champ des possibles dans le domaine de la connaissance et de l'aide à la décision grâce notamment à des algorithmes de reconnaissance des formes ou de la voix, à des outils capables d'agréger et d'extraire automatiquement des informations concordantes, etc. De fait, l'IA se nourrit des données de masse, fruit de la numérisation des activités humaines, pour générer des potentialités économiques, cognitives ou stratégiques tout à fait considérables.

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

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

Floran VADILLO



Floran Vadillo, Docteur en science politique est directeur en charge de la sécurité intérieure chez Sopra Steria

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

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

La trop récente massification des données d'enquête

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

La lente construction d'un outillage d'enquête

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

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

– l'accès à différents fichiers (fichiers de police judiciaire, fichiers administratifs, système d'information Schengen, etc.) ;

– les « écoutes téléphoniques », juridiquement nommées « interceptions de sécurité » (IS, régies par la loi du 10 juillet 1991) ;

– et le recueil des données techniques de connexion (*ex post* à partir de la loi du 23 janvier 2006, puis y compris en temps réel à partir de la loi du 18 décembre 2013).

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

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

(2) Pour ce dernier pays, on citera par exemple 5D, Verint, TA9.
(3) L'existence d'un écosystème militaro-industriel propice constitue sans doute l'un des facteurs d'explication les plus pertinents.
(4) Car, en France, la dualité des ordres juridictionnels et les importantes prérogatives de l'État ont conduit à structurer une *summa divisio* entre la police judiciaire (chargée de la répression) et la police administrative (chargée de la prévention). Le Conseil constitutionnel rappelle avec constance cette distinction qui sépare les objectifs et les moyens et, par conséquent, les administrations concernées et les instances de contrôle.

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

l'adoption de la loi précitée de juillet 1991 ;

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

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

– ainsi la filature, la sonorisation, la captation d'images et l'infiltration firent-elles leur entrée dans le CPP grâce à la loi du 9 mars 2004, dite « Perben II » ;

– la captation de données informatiques procéda de la LOPPSI 2[5] de 2011 ;

– puis, à partir de 2013, les ajouts furent plus rapprochés avec, outre la géolocalisation déjà mentionnée, l'enquête numérique sous pseudonyme (loi du 13 novembre 2014) ou le recours aux IMSI *catchers* (loi du 3 juin 2016).

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

La perpétuation du retard de la police judiciaire

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

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

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

(5) La loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure dite « LOPPSI 2 ».
(6) Verdier (H.), 2017, « le vrai sujet : faire advenir l'État d'après la révolution numérique », *Bercy numérique*, 20 décembre.

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

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

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

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

Les techniques désormais autorisées par la loi devraient donc permettre de constituer progressivement des gisements de données. Toutefois, le droit applicable à l'exploitation de ces derniers accuse à la fois une trop grande complexité et un réel retard pour prendre en charge les conséquences des évolutions juridiques précitées.

La balkanisation du droit de l'enquête

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

– le renseignement de souveraineté concourt à la défense et à la promotion des intérêts fondamentaux de la Nation. Il se compose de deux cercles[9] de services, le premier d'entre eux accueillant la direction générale de la Sécurité extérieure (DGSE), la direction générale de la Sécurité intérieure (DGSI), la direction du Renseignement militaire (DRM), la direction du Renseignement et de la Sécurité de la défense (DRSD), la direction nationale du Renseignement et des Enquêtes douanières (DNRED) et Tracfin. L'ensemble de ce dispositif est placé sous le contrôle de la Commission nationale de contrôle des techniques de renseignement (CNCTR). La loi du 24 juillet 2015 constitue son principal cadre juridique ;

– mais, sous ce même régime, œuvrent également des services de police judiciaire de la direction centrale de la Police judiciaire (DCPJ), de la préfecture de Police de Paris (PP) ou de la direction générale de la Gendarmerie nationale qui agissent alors dans une zone d'indistinction communément appelée « pré-judiciaire ». Ils mobilisent donc des prérogatives administratives à des fins de judiciarisation. Si la CNCTR ne publie pas de statistiques par services demandeurs, sa prédécesseure, la Commission nationale de contrôle des interceptions de sécurité (CNCIS) avait eu l'occasion de souligner que près de la moitié des IS étaient mises en œuvre par des services agissant en pré-judiciaire[10] ;

(7) Google, Apple, Facebook, Amazon et Microsoft.
(8) Article L. 822-2 du CSI.
(9) En application des articles L. 811-2 et 4 du Code de la sécurité intérieure selon une capacité de recourir pleinement ou non aux techniques de recueil du renseignement. La liste des services composant chacun de ces deux cercles a été publiée par le biais du décret du 28 septembre 2015 et du décret du 11 décembre 2015.
(10) Cf. CNCIS, *21e rapport d'activité 2012-2013*, p. 60 : « *Le taux de clôture des demandes d'interception pour ouverture d'une procédure judiciaire* [...] *témoigne aussi de l'intérêt de ce dispositif de prévention et de police administrative qui permet d'exclure des hypothèses d'enquête et de stopper les mesures d'investigation avant toute phase judiciaire. Il ouvre aussi la possibilité, en cas de confirmation des soupçons quant à des projets d'infractions, de poursuivre par l'ouverture d'une procédure judiciaire avant la commission des faits, ce qui est particulièrement essentiel dans le cadre de la prévention des attentats terroristes* ».

– en outre, le Service national du renseignement pénitentiaire, pourtant service de renseignement du deuxième cercle placé au sein du ministère de la Justice, jouit d'un double régime juridique : à la fois l'article L.855-1 du CSI qui le place sous le contrôle de la CNCTR, et l'article 727-1 du CPP qui confie sa supervision au procureur de la République. Cette entité recourt donc, concomitamment et pour les mêmes objectifs, aux deux types de police ;

– on pourrait, en dernier lieu, citer les prérogatives confiées aux services de police et de gendarmerie à la suite de la transposition dans le droit commun de certaines dispositions de l'état d'urgence, et notamment les mesures individuelles de contrôle administratif et de surveillance ou les visites domiciliaires[11]. Ces prérogatives administratives requièrent néanmoins l'intervention de l'autorité judiciaire.

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

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

– les services qui la composent assument des missions classiques de rassemblement des preuves participant à la manifestation de la vérité au profit de la Justice ; ils œuvrent au sein de la direction centrale de la Police judiciaire (DCPJ), de la préfecture de Police de Paris, mais aussi au sein de la direction centrale de la Sécurité publique (DCSP) ou encore de la sous-direction de la Police judiciaire de la gendarmerie nationale (SDPJ). Leur action est alors régie par le Code de procédure pénale (CPP) ;

– en parallèle, ces mêmes services peuvent déployer des activités pré-judiciaires telles que précitées ;

– en outre, la sous-direction de la Police judiciaire de la DGSI et la Sous-direction antiterroriste (SDAT) de la direction centrale de la Police judiciaire (DCPJ) agissent en matière de lutte contre le terrorisme très en amont de la commission d'une infraction grâce au délit d'association de malfaiteurs en relation avec une entreprise terroriste qui, par sa dimension préventive, permet de mordre clairement sur le champ d'action de la police administrative ;

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

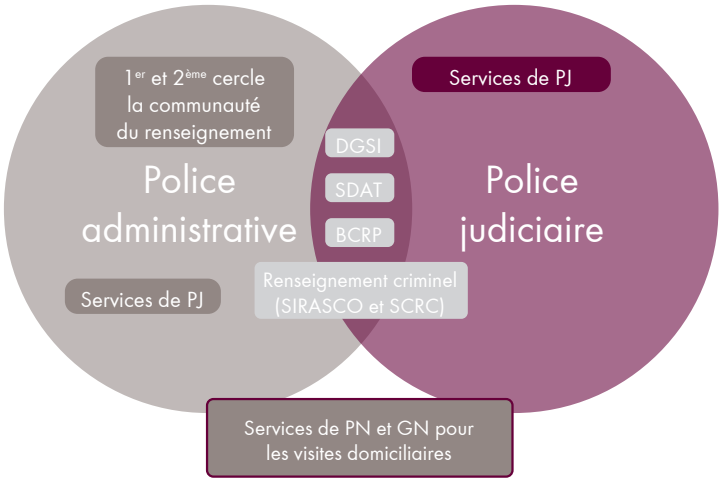
En définitive, un même service peut appartenir à une sphère et agir dans l'autre, voire dans les deux simultanément. À cet égard, la *summa divisio* importe moins dans ses conséquences organisationnelles que dans les cadres juridiques autorisés pour collecter les données nécessaires et les exploiter.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

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

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

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

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



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

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

Ces considérations posées, il apparaît que les services de renseignement peuvent appliquer sans peine un dispositif d'IA sur leur base de données interne. En revanche, l'application sur des éléments mutualisés soulève plus de questions. De même, l'interconnexion de fichiers, même temporaire, demeure très strictement encadrée par la CNIL qui la considère comme un nouveau traitement de données devant être soumis à autorisation. Indéniablement, les dispositions législatives limitent les facultés de déploiement de l'IA dans le légitime souci du respect des droits fondamentaux. Le sujet se situait à ce titre en bonne place dans le discours du président de la République aux préfets, le 5 septembre 2018 : « *Pour améliorer l'exploitation des informations sept décrets relatifs aux fichiers de renseignement viennent d'être également publiés au début du mois d'août. J'ai également demandé au SGDSN*[12] *d'engager une réflexion sur la modernisation et les possibilités de croisement de certains de ces fichiers* ».

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

En réponse à ces limites, cinq optiques paraissent envisageables :

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

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

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

– à défaut, pourquoi ne pas imaginer, sur la base de cet article, la création d'un fichier de souveraineté thématique, déclaré à la CNIL, afin d'exploiter les données collectées ? [Évolution n° 2]. Certes, la jurisprudence du Conseil constitutionnel se montre peu clémente à l'égard des traitements généraux de données. Mais on peut légitimement estimer qu'un fichier de souveraineté thématique (lutte contre le terrorisme ou contre-espionnage) ne rencontrerait pas d'objection ;

– la troisième option consisterait à promouvoir le principe d'une interface « hit/no hit » appliquée aux fichiers des services de renseignement (sur le modèle du Fichier national des objectifs en matière de stupéfiants, FNOS) : les recoupements pertinents induiraient un « hit » qui donnerait lieu à une levée d'anonymat, selon les modalités prévues à l'article L. 851-3 relatif à la surveillance algorithmique (demande à la CNCTR qui statue). Toutes les potentialités des fichiers ne seraient pas exploitées, mais il s'agirait d'une avancée très notable [Évolution n° 3] ;

– la quatrième supposerait l'interconnexion de fichiers aux données pseudononymisées qui, en cas de recoupement pertinent, entraînerait une levée de pseudonyme selon le mécanisme décrit ci-avant [Évolution n° 4]. Afin de pleinement respecter la logique de la loi de 1978, sans doute faudrait-il anonymiser certaines données et en pseudonymiser d'autres dans l'objectif de limiter le risque concernant la vie privée des personnes concernées ;

– enfin, et prenant en compte la doctrine de la CNIL en matière d'interconnexion, cette dernière pourrait devenir une technique de recueil du renseignement à part entière : soumise à autorisation du Premier ministre après avis de la CNCTR, elle serait mise en œuvre de manière temporaire concernant un individu. Les renseignements sans lien avec la demande seraient détruits dans les plus brefs délais et ne seraient conservés que ceux en lien direct avec la demande formulée pendant 30 jours. La CNCTR exercerait un contrôle *a priori* et *ex post* [Évolution n° 5]. Cette perspective a le mérite de s'insérer dans un cadre légal précis, lequel met en œuvre les principes de proportionnalité (voire de subsidiarité) en même temps qu'il offre des mécanismes de contrôle et des voies de recours, y compris juridictionnel. Les garanties apportées justifieraient pleinement la mise en œuvre de cette mesure.

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

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

Le renseignement judiciaire borné par la jurisprudence du Conseil constitutionnel

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

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

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

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

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

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

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

– le principe d'une interface « hit/no hit » aiderait les enquêteurs à recouper différentes bases dont ils disposent [Évolution n° 6] ;

– de même, l'interconnexion de fichiers aux données pseudononymisées qui, en cas de recoupement pertinent, donnerait lieu à une levée de pseudonyme sur réquisition judiciaire paraîtrait utile [Évolution n° 7] ;

– enfin, l'interconnexion pourrait gagner le statut de technique d'enquête spéciale sur réquisition judiciaire individualisée et temporaire. Le contrôle de ces opérations et notamment de l'effacement à échéance de l'enquête serait confié à un magistrat ainsi qu'à la CNIL [Évolution n° 8].

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

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

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

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

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

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

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

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

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

– des données administratives, en particulier celles protégées au titre du secret de la défense nationale puisque, par nature, elles n'ont pas vocation à être versées en procédure sauf lorsqu'il en est décidé autrement ;

– de l'opportunité d'apprécier le recours à l'article 40 du CPP lorsqu'un enquêteur souhaite mener à bien des enquêtes plus approfondies ;

– des bénéfices d'un travail d'anticipation qui, par définition, ne répond pas aux mêmes exigences de preuve qu'une enquête judiciaire et gagne ainsi en souplesse ;

– de la conduite d'un fragment de politique publique en matière de sécurité publique puisqu'elle confierait cette mission à l'autorité judiciaire, en contradiction avec notre système actuel.

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

Conclusion

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

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

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

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