

LA VEILLE JURIDIQUE

Centre de Recherche de la Gendarmerie Nationale

N° 128

Janvier 2025

EDITO

Le mois de janvier est marqué par la disruption. Aux États-Unis, tout d'abord, le changement d'administration s'accompagne, dès les premiers jours, de prises de décision pour le moins tranchantes et qui conduisent à des formes de dérégulation. Abandonnées, toutes les mesures prises par Joe Biden relatives à l'encadrement de l'intelligence artificielle (IA), les contraintes de modération pesant sur les réseaux sociaux. La loi de la force prend le pas sur la force de la loi. Désormais c'est la *Big Tech* qui décide ! *Code is Law*, écrivait le professeur américain Lawrence Lessig. Cette déréglementation va s'accompagner d'une explosion des conséquences environnementales de programmes qui ont pour objectif d'empêcher la Chine de dominer. L'IA

(Suite page 2)

Edito

ne peut se développer sans de puissants datacenters, consommateurs d'eau, d'électricité, producteurs de CO². Stargate est annonciateur de bien des renoncements, au moment où la planète est de plus en plus sujette à des catastrophes liées au dérèglement climatique. Une chose est certaine, le duel entre les États-Unis et la Chine ne jouera pas en faveur du développement durable.

Côté chinois, la disruption vient de la sortie d'une IA générative, *DeepJSeek*. Ce *Large Language Model* a des performances qui égalent celles du modèle o1 d'OpenAI avec un coût inférieur de 96 % et sur un nombre de données très inférieur à celui de son principal concurrent, ChatGPT. Il faut sans doute faire preuve de prudence, car la transparence n'est pas l'apanage des Chinois. Il n'empêche qu'après avoir entendu un discours sur l'impossibilité de créer une IA sans un apport de capital très important (en témoignent les levées de fonds), sur la nécessité de disposer de puces très puissantes (les GPU¹ de Nvidia), la Chine nous montre – sous réserve d'inventaire – que l'on peut obtenir des résultats aussi performants à moindre coût, utilisant moins de données, moins consommateurs en énergie et ne nécessitant pas de semi-conducteurs, aujourd'hui dans les mains d'un seul producteur. L'embargo sur les semi-conducteurs ou les restrictions qui pèsent sur certains États doivent être regardées à la lumière de l'actualité. L'histoire nous rattrape ! Marc Andreessen, un des pionniers d'Internet, dit que « *DeepSeek is AI's Sputnik moment* », rappelant le

1. *Graphics Processing Unit*, soit des processeurs graphiques.

Edito

« gap » technologique découvert par les Américains en 1957, lorsque les Soviétiques ont lancé un satellite. Stargate serait-il une réplique de l'Initiative de défense stratégique (IDS) lancée par Donald Reagan dans les années 1980 et qui avait en partie pour objectif d'épuiser l'adversaire dans la course aux technologies ?

Janvier est un mauvais mois pour la régulation, pour la recherche d'une position commune, notamment sur l'IA. Mais février s'ouvre sur de meilleurs auspices avec le Sommet mondial sur l'intelligence artificielle qui a lieu à Paris les 10 et 11 février 2025, au Grand Palais. Cette manifestation fait suite à celles organisées à Bletchley Park (Royaume-Uni en novembre 2023) et Séoul (Corée en mai 2024). Elle vise à « *établir collectivement les fondements scientifiques, les solutions et les standards d'une IA plus durable au service du progrès collectif et de l'intérêt général* ». Cinq thèmes centraux seront au cœur des échanges : l'IA au service de l'intérêt public, l'avenir du travail, l'innovation et la culture, l'IA de confiance, la gouvernance mondiale de l'IA.

Dans ce contexte, l'Europe doit se positionner et considérer comme une opportunité ce qui semble *a priori* contraire à ses intérêts. Se posent aujourd'hui pour elle des questions d'autonomie stratégique. Il lui appartient de choisir entre la position de vassale et celle de puissance qu'elle devrait être si les 27 agissaient de concert. Vaste programme, aurait dit le général de Gaulle !

Bonne lecture de cette Veille du Centre de recherche de la gendarmerie, réalisée par une équipe que je remercie de sa fidélité.

Par le général d'armée (2S) Marc WATIN-AUGOUARD, rédacteur en chef de La Veille juridique

Le Centre de recherche de la gendarmerie nationale (CRGN) est agréé par l'administration fiscale au titre du mécénat d'entreprise pour la recherche, prévu notamment à l'article 238 bis du Code général des impôts. Ainsi, les versements au profit du CRGN ouvrent droit à une déduction d'impôts à hauteur de 60 % des dons effectués. Si vous êtes une entreprise, vous pouvez devenir partenaire du CRGN en nous contactant à l'adresse suivante :

crgn.amgn@gendarmerie.interieur.gouv.fr



SOMMAIRE

Déontologie et sécurité

Révocation d'une brigadière de la police nationale en raison de propos publiés sur son compte personnel Facebook..... [6](#)

Droit de l'espace numérique

L'intelligence artificielle en santé : entre opportunités, défis, éthique et droit..... [16](#)

Les créations par l'intelligence artificielle sont-elles des oeuvres de l'esprit ?..... [43](#)

Actualité pénale

Cour de justice de l'Union européenne et exploitation des données d'un téléphone en enquête : une nécessaire évolution du droit français..... [51](#)

Police administrative

De l'anonymat des policiers et des gendarmes..... [67](#)

Actualité institutionnelle européenne

L'Europe de la sécurité intérieure. Synthèse législative et institutionnelle (été 2024 - hiver 2024)..... [77](#)



Marc-Antoine GRANGER

Révocation d'une brigadière de la police nationale en raison de propos publiés sur son compte personnel Facebook

(Note sous CAA Paris, 9^e ch., 5 juillet 2024, n° 23PA02767)

La liberté d'expression et de communication est protégée aux plus hauts niveaux de la hiérarchie des normes. Au sommet de l'ordre juridique interne¹, soit au sein du bloc de constitutionnalité², elle se présente comme « *un des droits les plus précieux de l'Homme* », selon la formule consignée à l'article 11 de la Déclaration des droits de l'Homme et du citoyen du 26 août 1789. Pour autant, cette liberté n'est pas absolue³. L'article 11 de la Déclaration précise d'ailleurs que si « *tout citoyen peut donc parler, écrire, imprimer librement* », il devra cependant « *répondre de l'abus de cette liberté* »

1. Tous les juges nationaux reconnaissent que la Constitution française (largement entendue) se situe au sommet de l'ordre juridique interne. Voir, en ce sens, Cons. const., décision n° 2004-505 DC du 19 novembre 2004, *Traité établissant une Constitution pour l'Europe*, consid. 10, Cass., Ass. plén., 2 juin 2000, *Mlle Fraisse*, n° 99-60.274, et CE, Ass., 30 octobre 1998, *Sarran et Levacher et autres*, n° 200286.

2. Sur la notion de bloc de constitutionnalité, voir, notamment : DENIZEAU-LAHAYE, Charlotte. La genèse du bloc de constitutionnalité. Titre VII, avril 2022, n° 8, et GRANGER, Marc-Antoine. *Fiches de contentieux constitutionnel*. Ellipses, janvier 2023, p. 77-81.

3. Dans la plupart des cas, les droits et libertés sont effectivement susceptibles de faire l'objet de limitations. Il faut cependant réserver l'hypothèse des droits

Déontologie et sécurité

dans les cas déterminés par la loi ».

Aussi n'y a-t-il rien de surprenant à ce que la liberté d'expression des agents publics rencontre des limites, à l'instar de celles qu'imposent les obligations statutaires et déontologiques, à commencer par le devoir ou l'obligation de réserve⁴. Sur les réseaux sociaux, plus encore que sur les autres vecteurs de communication, la prudence est de rigueur en raison « *de la difficulté pour l'utilisateur qui y publie des propos de s'assurer de leur caractère privé ou de leur diffusion restreinte, d'en garantir l'intégrité ou d'en maîtriser la portée, eu égard notamment aux réactions auxquelles ils sont susceptibles de donner lieu, parfois presque instantanément* »⁵. Cette recommandation prudentielle est parfois explicitement énoncée ici ou là⁶, comme c'est le cas dans le dernier rapport d'activité de l'Inspection générale de la police nationale, publié sous la forme originale d'un abécédaire⁷. On peut y lire que « *l'usage qui peut être fait des*

indérogeables ou intangibles. En guise d'illustration, dans le champ conventionnel européen, l'interdiction de la torture et des peines ou traitements inhumains ou dégradants (art. 3 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, ci-après CESDH), ainsi que la prohibition de l'esclavage et de la servitude (art. 4, § 1, de la CESDH) ne tolèrent ni dérogation ni exception, pas même en cas de guerre ou de danger public menaçant la vie de la nation (art. 15, § 1 et 2, de la CESDH).

4. Le devoir (ou l'obligation) de réserve est apparu dans la jurisprudence du Conseil d'État avec l'arrêt *Sieur Bouzanquet* du 11 janvier 1935.

5. CE, 4^e et 1^{ère} ch. réunies, 25 mars 2020, *Syndicat de la juridiction administrative*, n° 421149, § 13.

6. Charte de déontologie de la juridiction administrative, § 47.

7. IGPN. *Rapport annuel d'activité au titre de l'année 2023*.

Déontologie et sécurité

réseaux sociaux par un agent de police nécessite de respecter certaines précautions au regard du risque lié à leur propre sécurité et à celle de leurs proches, ainsi qu'au regard des règles imposées par la déontologie et les règlements. Au-delà d'une obligation générale de vigilance, les instructions rappellent notamment aux agents les préconisations et obligations relatives à la protection de leur anonymat, la connaissance de leurs contacts, la maîtrise des paramètres de confidentialité, la préservation de leur identité professionnelle, le respect du devoir de réserve et de l'image de la police nationale »⁸. Au bénéfice de ces précisions liminaires, l'arrêt commenté, rendu le 5 juillet 2024 par la cour administrative d'appel de Paris⁹, illustre une nouvelle fois¹⁰ que le policier national ne peut pas tout dire sur les réseaux sociaux.

En l'espèce, une brigadière de la police nationale, affectée à la circonscription de sécurité publique du Raincy, a fait l'objet d'un rappel à la loi pour avoir, entre les 23 mars et 7 octobre 2014, affiché sur son compte Facebook des propos relevant de l'apologie du crime et de la provocation publique à la discrimination, à la haine raciale ou à la violence envers des États et un groupe de personnes en raison de son origine ou de son appartenance ou non-appartenance à une

8. *Ibidem*, p. 141.

9. CAA Paris, 9^e ch., 5 juillet 2024, n° 23PA02767.

10. Voir, par exemple, GRANGER, Marc-Antoine. La révocation d'un gardien de la paix en raison de propos tenus au sein d'un groupe de discussion WhatsApp. Note sous CE, 6^e et 5^e ch. réunies, 28 déc. 2023, n° 474289 [en ligne]. *Veille juridique du CREOGN*, avril 2024, n° 122, p. 7-15. Disponible sur : <https://www.calameo.com/read/002719292ff6247d6ce56?page=7>

Déontologie et sécurité

ethnie, nation, race, religion déterminée. Sur le plan disciplinaire, la policière a été révoquée de ses fonctions par un arrêté du ministre de l'Intérieur du 26 octobre 2020, sanction conforme à l'avis rendu par le conseil de discipline réuni le 5 février 2020.

À partir de là, la procédure contentieuse est classique. Le 6 janvier 2021, la brigadière a porté l'affaire devant le tribunal administratif de Montreuil qui, par son jugement du 21 avril 2023¹¹, a rejeté la requête en annulation de l'arrêté pris par le ministre de l'Intérieur. Le 22 juin 2023, la policière sanctionnée a alors interjeté appel de ce jugement devant la cour administrative d'appel de Paris. L'appelante développe plusieurs moyens ; aucun d'eux n'a fait mouche. Sa requête a donc été rejetée en toutes ses conclusions, y compris celles tenant aux frais liés à l'instance¹². Pour l'essentiel, après avoir rappelé le cadre juridique applicable (I), la cour admet le bien-fondé de la sanction de révocation prononcée par le ministre de l'Intérieur (II).

I. Le cadre juridique applicable

Au cas présent, le cadre juridique pertinent est bien balisé et se dédouble.

D'un côté, il repose sur quelques fondements généraux fixés par le législateur en matière de responsabilité disciplinaire du fonctionnaire, l'appelante étant elle-même fonctionnaire d'État en

¹¹. TA Montreuil, 3^e ch., 21 avril 2023, n° 2100105.

¹². CAA Paris, 9^e ch., 5 juillet 2024, préc., § 8.

Déontologie et sécurité

sa qualité de brigadière de la police nationale¹³. À ce titre, la cour énonce le principe de la responsabilité disciplinaire, tel qu'il a été posé par la loi en ces termes : « *Toute faute commise par un fonctionnaire dans l'exercice ou à l'occasion de l'exercice de ses fonctions l'expose à une sanction disciplinaire sans préjudice, le cas échéant, des peines prévues par la loi pénale* »¹⁴. La cour rapporte aussi les dispositions par lesquelles le législateur a déterminé l'échelle des sanctions disciplinaires susceptibles d'être prononcées à l'encontre des fonctionnaires¹⁵. Sont plus particulièrement visées les sanctions du quatrième groupe, c'est-à-dire celles les plus sévères de la mise à la retraite d'office et de la révocation.

D'un autre côté, le cadre juridique s'articule autour des règles déontologiques et statutaires des policiers nationaux. D'abord, en dérivation des dispositions législatives précitées, l'article R. 434-27 du Code de la sécurité intérieure (CSI) dispose que « *tout manquement du policier ou du gendarme aux règles et principes*

13. Rappelons que les deux premiers grades de gardien de la paix et de brigadier ont été fusionnés, de sorte que ce dernier grade a disparu : voir le décret n° 2023-676 du 28 juillet 2023 modifiant le statut particulier du corps d'encadrement et d'application de la police nationale.

14. Les dispositions alors en vigueur étaient celles du premier alinéa de l'article 29 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, dite loi Le Pors. Elles sont désormais codifiées au premier alinéa de l'article L. 530-1 du Code général de la fonction publique (CGFP).

15. Les dispositions alors en vigueur étaient celles de l'article 66 de la loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'État. Elles sont désormais codifiées à l'article L. 533-1 du CGFP.

Déontologie et sécurité

définis par le (...) code de déontologie [de la police nationale et de la gendarmerie nationale] l'expose à une sanction disciplinaire en application des règles propres à son statut, indépendamment des sanctions pénales encourues le cas échéant ». Ensuite, la cour rappelle certaines des obligations du policier national, consacrées par le pouvoir réglementaire principalement, mais non exclusivement, dans le CSI. En ce sens, la cour mobilise l'article 29 du décret du 9 mai 1995¹⁶ qui impose, en tout temps, au fonctionnaire actif des services de la police nationale de « *s'abstenir en public de tout acte ou propos de nature à porter la déconsidération sur le corps auquel il appartient ou à troubler l'ordre public* ». Surtout, quatre articles du CSI sont cités par la cour, à savoir les articles R. 434-11, R. 434-12, R. 434-14 et R. 434-29 qui consacrent les « *devoirs de réserve, d'exemplarité, de dignité, de neutralité et d'obéissance* »¹⁷ ou, plus précisément, de loyauté à l'égard des institutions de la République. Deux de ces articles méritent d'être reproduits dans le cadre de ces lignes parce qu'ils concernent le devoir de réserve du policier national, y compris lorsqu'il s'exprime sur les réseaux sociaux. D'une part, en vertu de l'article R. 434-29 du CSI, « *le policier est tenu à l'obligation de neutralité. / Il s'abstient, dans l'exercice de ses fonctions, de toute expression ou manifestation de ses convictions religieuses, politiques ou philosophiques. / Lorsqu'il n'est pas en service, il s'exprime*

16. Décret n° 95-654 du 9 mai 1995 fixant les dispositions communes applicables aux fonctionnaires actifs des services de la police nationale.

17. CAA Paris, 9^e ch., 5 juillet 2024, préc., § 7.

Déontologie et sécurité

librement dans les limites imposées par le devoir de réserve et par la loyauté à l'égard des institutions de la République »¹⁸. D'autre part, selon l'article R. 434-12 du CSI, « le policier ou le gendarme ne se départ de sa dignité en aucune circonstance. / En tout temps, dans ou en dehors du service, y compris lorsqu'il s'exprime à travers les réseaux de communication électronique sociaux, il s'abstient de tout acte, propos ou comportement de nature à nuire à la considération portée à la police nationale et à la gendarmerie nationale. Il veille à ne porter, par la nature de ses relations, aucune atteinte à leur crédit ou à leur réputation ».

II. Le bien-fondé de la sanction de révocation

Dans le cadre de l'effet dévolutif de l'appel, la cour n'a pas vérifié l'exactitude matérielle des faits¹⁹, car ceux-ci sont établis et non contestés²⁰. En effet, l'appelante reconnaît avoir, « *entre les mois de mars et octobre 2014, posté sur son compte personnel Facebook en accès public sans paramétrage restrictif et alors qu'elle avait révélé sa profession de policier, des commentaires ouvertement haineux et vindicatifs à caractère discriminatoire, revendiquant avec véhémence*

18. Le dernier alinéa de l'article R. 434-29 du CSI, non cité par la cour, prévoit que, « *dans les mêmes limites, les représentants du personnel bénéficient, dans le cadre de leur mandat, d'une plus grande liberté d'expression* ».

19. Rappelons que ce contrôle de l'exactitude matérielle des faits ou de l'erreur de fait est susceptible d'être exercé depuis la célèbre jurisprudence Camino : CE, 14 janvier 1916, Camino. Pour un commentaire de cette décision, voir : *Les grands arrêts de la jurisprudence administrative*. Dalloz, 2023, 24^e éd., p. 175-179.

20. CAA Paris, 9^e ch., 5 juillet 2024, préc., § 7.

Déontologie et sécurité

ses convictions religieuses islamiques, ainsi que son hostilité à la politique gouvernementale française et à celle d'autres pays partenaires comme Israël et les États-Unis, ainsi qu'à leurs ressortissants, en usant d'une sémantique communautariste, religieuse et radicale et en tenant des propos subversifs et outranciers »²¹. Elle admet aussi « avoir fait l'éloge de l'organisation armée du Hamas dans sa lutte au côté du peuple palestinien présenté comme victime d'un "génocide" sioniste et partagé des publications appelant à participer à une manifestation en faveur de la Palestine organisée le 26 juillet 2014, officiellement interdite par la Préfecture de police »²².

Sur le terrain de la qualification juridique²³, la cour a considéré, du reste comme les premiers juges, que la brigadière a franchi la ligne rouge dans l'exercice de sa liberté d'expression. À l'aune du cadre juridique susvisé, cette solution n'est guère discutable. L'appelante a bien « porté une atteinte grave à l'image du service public de la police nationale » et manqué « à ses obligations statutaires et déontologiques, en particulier aux devoirs de réserve, d'exemplarité, de dignité, de neutralité et d'obéissance »²⁴ ou, plus

²¹. *Ibid.*

²². *Ibid.*

²³. C'est dans son arrêt *Gomel* que, pour la première fois, le juge de l'excès de pouvoir du Conseil d'État a exercé un tel contrôle de la qualification juridique : CE, 4 avril 1914, *Gomel*. Pour un commentaire de cette décision, voir : *Les grands arrêts de la jurisprudence administrative*, *op. cit.* note 19, p. 165-174.

²⁴. CAA Paris, 9^e ch., 5 juillet 2024, préc., § 7.

Déontologie et sécurité

exactement, de loyauté à l'égard des institutions de la République. Au demeurant, en raison de l'autonomie de la répression disciplinaire vis-à-vis de la répression pénale, la circonstance que les faits n'aient donné lieu qu'à un rappel à la loi n'était pas « *susceptible de remettre en cause l'incompatibilité [des] manquements avec les fonctions exercées* »²⁵.

Quant à la proportionnalité de la sanction²⁶, l'arrêt de la cour administrative d'appel s'inscrit, là encore, dans le sillage du jugement rendu par le tribunal administratif de Montreuil puisqu'il est décidé que « *le ministre de l'Intérieur n'a pas entaché l'arrêté attaqué d'une erreur d'appréciation en (...) infligeant la sanction disciplinaire de révocation* »²⁷. Pour forger sa conviction, le juge d'appel s'est fondé sur « *la gravité des manquements commis* » par l'appelante du fait de « *l'expression d'idéologies diffusées sans restriction sur les réseaux sociaux pendant plusieurs mois et par nature incompatibles avec la qualité de fonctionnaire de police* »²⁸. En outre, la cour précise – en réponse sans doute à l'argumentation produite devant elle – que le comportement global de la brigadière (notamment ses états de service) n'est pas de nature à atténuer sa responsabilité disciplinaire. Finalement, le verdict se comprend d'autant que le contrôle normal exercé ici ne doit pas « *priver*

²⁵. *Ibid.*

²⁶. En vertu de la jurisprudence *Dahan* de 2013, le juge de l'excès de pouvoir exerce un contrôle normal afin de vérifier si la sanction retenue est proportionnée à la gravité des fautes : CE, Ass., 13 novembre 2013, *Dahan*, n° 347704.

²⁷. CAA Paris, 9^e ch., 5 juillet 2024, préc., § 7.

²⁸. *Ibid.*

Déontologie et sécurité

l'administration de toute marge d'appréciation sur le choix de la sanction », le juge devant « vérifier que la sanction se situe dans les bornes de la légalité »²⁹.

En définitive, comme l'a déjà relevé la Cour européenne des droits de l'Homme, Internet constitue assurément « *un outil sans précédent d'exercice de la liberté d'expression* »³⁰. Toutefois, cette affaire commentée est l'occasion de rappeler combien il importe au policier ou au gendarme connecté de faire preuve d'une particulière retenue lorsqu'il s'exprime dans le cyberspace.

29. LABRUNE, Nicolas, concl. sur CE, 7^e ch., 5 juin 2024, n° 490987.

30. CEDH, Gr. ch., 16 juin 2015, *Delfi AS c. Estonie*, aff. n° 64569/09, § 110.

Droit de l'espace numérique

Sandrine Richard

L'intelligence artificielle en santé : entre opportunités, défis, éthique et droit

« *Science sans conscience n'est que ruine de l'âme* »,
écrivait Rabelais.

Cette phrase prend tout son sens à l'heure où plus une journée ne s'écoule sans que l'intelligence artificielle (IA) focalise l'attention des pouvoirs publics¹, des médias, des citoyens et des professionnels affectés par cette percée de l'utilisation des robots et des machines.

Face à cette frénésie et cette crainte d'une place grandissante de l'IA, le droit s'est naturellement préoccupé des questions juridiques soulevées par le recours aux machines et aux robots, notamment avec l'entrée en vigueur de l'*IA Act*².

1. Voir, par exemple, l'étude réalisée à la demande du Premier ministre sur l'IA dans les services publics : CONSEIL D'ÉTAT. *IA et action publique : construire la confiance, servir la performance*, 30 août 2022.

Voir également : MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES, Secrétariat d'Etat à l'Enseignement Supérieur et à la Recherche, Secrétariat d'Etat à l'Industrie, au Numérique et à l'Innovation. *France Intelligence Artificielle*. Rapport de synthèse, mars 2017, 36 p., et les 13 propositions du Rapport Touraine (*Rapport d'information fait au nom de la mission d'information sur la révision de la loi relative à la bioéthique*, n° 1572, janvier 2019, propositions 41 à 53).

2. BOURCIER, Danièle, HASSET, Patricia, ROQUILLY, Christophe. *Droit et intelligence artificielle*, Romillat, Coll. Droit et Technologies, 1994, 304 p. Voir également le règlement européen sur l'*IA Act*, entré progressivement en vigueur depuis le 1^{er} août 2024.

Droit de l'espace numérique

S'agissant du droit de la santé, chacun s'accorde à reconnaître qu'il est difficile de le cerner précisément, principalement en raison du fait que le législateur lui-même ne s'aventure pas à tenter une définition. En effet, « *le droit de la santé définit peu les termes qu'il utilise* »³. À cette difficulté, s'ajoute le fait que les frontières de ce droit de la santé sont extrêmement vagues et larges, dès lors qu'elles sont conditionnées au concept même de santé, lui-même largement insaisissable, à l'instar de la formule portée par l'Organisation mondiale de la santé pour qui « *la santé n'est pas seulement une absence de maladie ou d'infirmité, mais un état de complet bien-être physique, mental et social* ».

I) Les opportunités et les défis de l'utilisation de l'IA en santé

Les technologies développées autour de l'IA concernent de nombreux domaines d'application (médecine, transports, cybersécurité, commerce, industrie, etc.) et leur irruption dans nos usages quotidiens s'accélère à un rythme soutenu. Ce contexte encourage de nombreux États et institutions à considérer les enjeux éthiques qui accompagnent cette transformation.

Le secteur de la santé et de la médecine apparaît particulièrement concerné par le développement de systèmes d'IA. Leur application au champ médical induit une transformation de la relation entre

3. TRUCHET, Didier, APOLLIS, Benoît. *Droit de la santé publique*. Dalloz, 2020, p. 20.

Droit de l'espace numérique

médecins et patients et pose de nombreuses questions sur l'avenir des systèmes de santé.

Le Comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE) et le Comité national d'éthique du numérique (CNPEN)⁴ ont rendu un avis et identifié plusieurs axes de tensions éthiques. Ils ont rappelé que les équipes soignantes et les patients ne doivent pas se priver des avantages apportés par ces outils d'IA, tout en se donnant constamment les moyens de prendre de la distance avec le résultat fourni. Tout système d'intelligence artificielle d'aide au diagnostic médical (SIADM) doit être soumis à un contrôle humain. Ses résultats doivent être explicables. Le contrôle de conformité du SIADM, qui assure qu'il n'est pas dangereux et ainsi autorise sa mise sur le marché, doit être amélioré et surtout doit à l'avenir être accompagné d'une évaluation de son efficacité clinique, montrant non seulement son absence de nocivité mais aussi qu'il contribue efficacement au principe de bienfaisance.

Il en ressort que les systèmes d'intelligence artificielle appliqués au diagnostic médical doivent donc toujours être utilisés en priorité dans une optique d'amélioration du soin, avant les intérêts organisationnels, économiques ou managériaux.

4. CCNE, CNPEN. Avis n° 141 et n° 4. *Diagnostic Médical et Intelligence Artificielle : Enjeux Éthiques* [en ligne]. Disponible sur : <https://www.ccne-ethique.fr/fr/publications/avis-ndeg141-du-ccne-et-ndeg4-du-cnpn-diagnostic-medical-et-intelligence-artificielle>

Droit de l'espace numérique

1. Définition de l'intelligence artificielle

Force est de constater qu'à l'heure actuelle, il n'existe pas de consensus sur une définition universelle de ce que compose l'IA selon les domaines. L'*IA Act* définit l'IA comme un « *un système basé sur une machine qui est conçu pour fonctionner avec différents niveaux d'autonomie et qui peut faire preuve d'adaptabilité après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer des environnements physiques ou virtuels* »⁵. La Commission européenne conçoit par conséquent le système d'intelligence artificielle comme un logiciel développé à partir de plusieurs techniques et approches d'IA fondées sur des systèmes auto-apprenants, des systèmes logiques et des systèmes statistiques. C'est pourquoi, l'*IA Act* contient une méthodologie axée sur les risques qui permet de définir quand un système d'IA génère un risque inacceptable, élevé ou faible. Appliquée au domaine de la santé, elle conduit à considérer que les systèmes d'IA relèvent pour l'essentiel d'un système à haut risque au sens de l'article 6-1 soumis à un régime de conformité et de mise en conformité précisé par le règlement. Qu'ils soient intégrés à des dispositifs médicaux de diagnostic *in vitro*⁶ ou qu'ils facilitent l'accès

5. Article 3 : définitions [en ligne]. In : *EU Artificial Intelligence Act*, chapitre 1. Disponible sur : <https://artificialintelligenceact.eu/fr/article/3/>

6. Annexe II, Section A, 11 et 12, *IA Act*.

Droit de l'espace numérique

aux services privés essentiels et aux services publics notamment d'urgence médicale⁷, les systèmes d'intelligence artificielle en santé doivent donc satisfaire à certaines exigences déterminées par l'IA Act.

De nos jours, le champ d'application de l'IA dans le domaine de la santé est immense. Comme l'indique le Conseil d'État dans son rapport, « *de tous les champs de l'action publique dans lesquels il est possible de recourir à l'IA, celui de la santé est peut-être celui qui suscite le plus d'espoirs* »⁸. La quasi-totalité des champs de l'IA, reconnaissance d'image, de vidéos, traitement du langage naturel, apprentissage automatique, robotique, etc., sont susceptibles de générer des applications concrètes en matière de santé. Sur le plan de la prise en charge et de la relation patient-médecin, il n'est pas un domaine qui puisse échapper à l'IA, laquelle est en mesure de s'immiscer dans le diagnostic, les recommandations de prise en charge, les actes de traitement, la chirurgie, le suivi personnalisé, etc.⁹ L'IA peut également s'étendre au domaine médico-social et à la réadaptation, à l'image des robots de soins qui sont déjà développés au Japon et qui offrent prévention, assistance, surveillance, stimulation et accompagnement aux personnes âgées, aux personnes handicapées et aux personnes atteintes de démence, de

7. Annexe III, 5, IA Act.

8. CONSEIL D'ÉTAT, *op. cit.* note 1.

9. V. Cartographie des cas d'usage des systèmes d'IA dans l'action publique en matière de santé, Annexe 9, fiche 8, p. 336 et s. In : *op. cit.* note 1.

Droit de l'espace numérique

troubles cognitifs ou de pertes de mémoire. Dès lors que le domaine visé est la santé, l'IA peut devenir un auxiliaire au service de la prévention, de la recherche clinique, voire devenir un meilleur vecteur de suivi, par les autorités publiques, des risques sanitaires, que ce soit en matière de pharmacovigilance pour détecter de manière anticipée d'éventuels effets secondaires de médicaments ou d'un suivi épidémiologique afin d'anticiper et de gérer les épidémies comme celle du Covid, afin d'ajuster la politique de santé publique au plus vite¹⁰. Parmi un des exemples célèbres et pionniers de cette nouvelle médecine, il faut citer le logiciel Watson du groupe industriel IBM qui fut introduit dès 2005 sur le marché de la santé. Watson a été utilisé notamment au *Memorial Sloan-Kettering Cancer Center*, un institut américain spécialisé en recherche médicale et en traitement du cancer, pour l'aide au diagnostic et à la proposition thérapeutique¹¹. Il s'agit d'un logiciel d'aide à la décision médicale qui synthétise une masse d'informations provenant de millions de rapports médicaux, de dossiers de patients, de tests cliniques et de connaissances issues de la recherche médicale. À ce

10. Récemment, par exemple, dans le cadre de l'épidémie de Covid, le recours à l'IA a permis l'identification d'une signature génique spécifique aux formes graves. Voir : MAUBANT, Thierry. ADAM9, un gène potentiellement impliqué dans les formes graves de Covid-19 identifié par l'intelligence artificielle [en ligne]. *Actu Ia*, 25 novembre 2021. Disponible sur : <https://www.actuia.com/actualite/adam9-le-gene-implique-dans-les-formes-graves-de-covid-19-identifie-par-lintelligence-artificielle/>

11. FRANCE STRATÉGIE. *Intelligence artificielle et travail*. Rapport à la ministre du Travail et au secrétaire d'État auprès du Premier ministre, chargé du Numérique, mars 2018, p. 54.

Droit de l'espace numérique

jour, les logiciels d'aide à la décision sont capables d'égaliser, voire de surpasser le praticien dans la détection des tumeurs cutanées¹² et du sein, où la fiabilité de taux de détection atteint le taux de réussite impressionnant de 92 %, presque équivalent à celui des spécialistes (95 %) ; ils permettent aussi une chute des récives du cancer du poumon¹³.

Cependant, l'intégration de IA dans le domaine de la santé soulève des défis éthiques et juridiques complexes. Voici quelques-uns des principaux défis à relever.

2. Responsabilité et attribution des erreurs

- **Détermination de la responsabilité** : En cas d'erreurs de diagnostic ou de traitement assisté par IA, il est difficile de déterminer qui est responsable : le développeur de l'algorithme, le médecin qui utilise l'IA, ou l'établissement de santé ? Clarifier les responsabilités est crucial pour garantir que les patients puissent

¹². En entraînant un algorithme avec une banque de 100 000 images, une équipe américaine l'a rendu aussi performant qu'un dermatologue expérimenté pour reconnaître des maladies de peau et en particulier distinguer tumeurs bénignes et cancer. Voir : LEACHMAN, Sancy A., MERLINO, Glenn. « The final frontier in cancer diagnosis » [en ligne]. *Nature*, 25 janvier 2017. Disponible sur : <https://www.nature.com/articles/nature21492>

¹³. À propos du logiciel Moovcare voir le site de la classification paramédicale VIDAL, voir : <https://www.vidal.fr/parapharmacie/moovcare-poumon-disp-medical-detection-recidive-cancer-du-poumon-243506.html>

Droit de l'espace numérique

obtenir des recours.

L'arsenal juridique relatif à la mise en œuvre de l'IA en médecine s'articule principalement autour des principes généraux du droit de la responsabilité civile et pénale. Mais lorsqu'il existe une implication directe de l'IA dans ce type de contentieux, en tant qu'élément causatif d'un acte défectueux, comme la prescription d'un traitement inapproprié ou d'un acte chirurgical non sécurisé, la question devient difficile à résoudre. Pour illustrer cette difficulté de caractériser la responsabilité, prenons le cas d'un robot chirurgical provoquant une lésion grave au patient pendant l'opération au cours de laquelle il est utilisé. Le médecin qui a supervisé l'opération doit-il être qualifié de responsable alors qu'il ne contrôle pas directement l'appareil robotisé dans son fonctionnement ? Dans de telles situations où la responsabilité du dommage n'est pas globalement raisonnablement appréciable, une clarification législative est nécessaire afin qu'un régime de responsabilité particulier à l'égard des systèmes d'IA médicaux puisse exister.

En cas d'erreur médicale liée à l'IA, déterminer qui est responsable peut être complexe. L'erreur peut être due à un défaut de conception de l'IA, à une utilisation inappropriée par un professionnel de santé, ou à un manque d'entretien de la part de l'hôpital (article 1382 du Code civil).

Afin de protéger les victimes des systèmes d'IA en matière de santé et de les indemniser en attendant d'y voir plus clair, il suffit de revenir aux fondements de la responsabilité médicale posée par

Droit de l'espace numérique

l'article L. 1142-1 du Code de la santé publique¹⁴ et de la consolider si nécessaire. Ce texte, en évoquant la faute, la défektivité des produits de santé et l'accident médical, peut donc fort bien être appliqué en l'état.

14. Article L. 1142-1, version en vigueur depuis le 14 mai 2009 : « I- Hors le cas où leur responsabilité est encourue en raison d'un défaut d'un produit de santé, les professionnels de santé mentionnés à la quatrième partie du présent code, ainsi que tout établissement, service ou organisme dans lesquels sont réalisés des actes individuels de prévention, de diagnostic ou de soins ne sont responsables des conséquences dommageables d'actes de prévention, de diagnostic ou de soins qu'en cas de faute.

Les établissements, services et organismes susmentionnés sont responsables des dommages résultant d'infections nosocomiales, sauf s'ils rapportent la preuve d'une cause étrangère.

II. - Lorsque la responsabilité d'un professionnel, d'un établissement, service ou organisme mentionné au I ou d'un producteur de produits n'est pas engagée, un accident médical, une affection iatrogène ou une infection nosocomiale ouvre droit à la réparation des préjudices du patient, et, en cas de décès, de ses ayants droit au titre de la solidarité nationale, lorsqu'ils sont directement imputables à des actes de prévention, de diagnostic ou de soins et qu'ils ont eu pour le patient des conséquences anormales au regard de son état de santé comme de l'évolution prévisible de celui-ci et présentent un caractère de gravité, fixé par décret, apprécié au regard de la perte de capacités fonctionnelles et des conséquences sur la vie privée et professionnelle mesurées en tenant notamment compte du taux d'atteinte permanente à l'intégrité physique ou psychique, de la durée de l'arrêt temporaire des activités professionnelles ou de celle du déficit fonctionnel temporaire.

Ouvre droit à réparation des préjudices au titre de la solidarité nationale un taux d'atteinte permanente à l'intégrité physique ou psychique supérieur à un pourcentage d'un barème spécifique fixé par décret ; ce pourcentage, au plus égal à 25 %, est déterminé par ledit décret. »

Droit de l'espace numérique

- **Problème de l'« effet boîte noire »** : Les algorithmes d'IA, en particulier ceux basés sur l'apprentissage profond, peuvent être difficiles à interpréter. Cela soulève des questions sur la capacité des professionnels de santé à comprendre et à justifier les décisions prises par l'IA.

3. Biais et équité

- **Biais algorithmique** : Les systèmes d'IA peuvent reproduire ou même amplifier des biais présents dans les données à partir desquelles ils ont été formés. Cela peut entraîner des inégalités dans le diagnostic et le traitement des patients, notamment en fonction de leur sexe, de leur race ou de leur statut socio-économique. (cf. *infra*, p. 40)

- **Équité d'accès** : L'accès aux technologies d'IA peut varier en fonction des ressources des établissements de santé. Les régions ou les populations moins desservies risquent d'être laissées pour compte dans l'accès à des soins améliorés par l'IA. (cf. *infra*, p. 40)

4. Protection des données et confidentialité : le Règlement général sur la protection des données (RGPD) comme instrument juridique protecteur

Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état

Droit de l'espace numérique

de santé de cette personne.

Cette définition, selon la CNIL¹⁵, comprend donc, par exemple :

- les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ;
- les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques ;
- les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée (indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic *in vitro*).

Cette définition permet d'englober certaines données de mesures à partir desquelles il est possible de déduire une information sur l'état de santé de la personne.

Les obligations légales en matière de protection des données de santé sont principalement définies par la CNIL et par le RGPD.

¹⁵. La Commission nationale de l'informatique et des libertés (CNIL) a été créée par la loi relative à l'informatique, aux fichiers et aux libertés, dite « Informatique et Libertés » du 6 janvier 1978.

Droit de l'espace numérique

À ces obligations s'ajoute la certification HDS (Hébergement de Données de Santé), exigée pour « *tous les organismes publics ou privés qui hébergent, exploitent le système d'information de santé ou réalisent des sauvegardes pour le compte d'un établissement de santé ou d'un tiers de santé* » (article L.1111-8 du Code de la santé publique). Cette certification, spécifique à la France, vise à renforcer la sécurité des données de santé en s'appuyant sur la norme ISO/IEC 27001, et en intégrant des exigences supplémentaires adaptées au secteur, présentes dans le référentiel de certification.

Ainsi, le RGPD et la certification HDS offrent un cadre propice à la création d'un environnement de confiance autour de l'hébergement et du traitement des données de santé, l'objectif étant la protection des droits des patients et la conformité aux réglementations en vigueur.

Donc, si l'on se réfère au Règlement (UE) 2016/679 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 (RGPD) , la donnée « *concernant la santé* » se définit comme suit :

« *Les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* » (art. 4 point 15 du RGPD)¹⁶.

¹⁶. Article 4 RGPD. Définitions [en ligne]. Disponible sur: <https://gdpr-text.com/fr/read/article-4/>

Droit de l'espace numérique

- **Collecte et stockage des données** : L'utilisation de l'IA repose souvent sur l'analyse de grandes quantités de données personnelles et sensibles. Garantir la sécurité et la confidentialité de ces données est primordial pour respecter les droits des patients. En outre, le RGPD impose des règles strictes concernant la minimisation des données, leur sécurité et la limitation de la durée de conservation. La CNIL a publié un référentiel « *durées de conservation* » pour les traitements les plus fréquents dans les secteurs social et médico-social et une fiche pratique proposant une méthodologie aux professionnels concernés¹⁷.

- **Consentement éclairé** : Obtenir un consentement éclairé pour l'utilisation des données peut s'avérer complexe, en particulier lorsque les patients ne comprennent pas toujours comment leurs données seront utilisées par les systèmes d'IA. L'un des piliers de cette réglementation est la notion de consentement éclairé : l'individu doit être informé de manière claire et complète sur la nature des données collectées, l'objectif de leur collecte et les modalités de traitement. Ce consentement doit être spécifique et explicite, notamment lorsque les données sont utilisées à des fins autres que les soins directs, comme la recherche médicale. En l'absence de ce consentement, la collecte est considérée comme illégale, à moins qu'elle ne réponde à des exceptions prévues par la

¹⁷. CNIL. *Traitements de données dans le domaine de la santé : les référentiels pour simplifier vos démarches* [en ligne], 27 décembre 2023. Disponible sur : <https://www.cnil.fr/fr/traitements-de-donnees-dans-le-domaine-de-la-sante-les-referentiels-pour-simplifier-vos-demarches>

Droit de l'espace numérique

réglementation (sauvegarde des intérêts vitaux, motifs d'intérêt public dans le domaine de la santé publique, etc.). (cf. *infra*, p. 39)

5. Transparence et explicabilité

- **Nécessité de l'explicabilité** : Les professionnels de santé doivent être en mesure de comprendre comment un système d'IA arrive à ses conclusions pour pouvoir l'utiliser de manière appropriée. Le manque de transparence dans les algorithmes d'IA peut nuire à cette compréhension. (cf. *infra*, p. 37 et p. 41)

- **Confiance des patients** : La transparence est essentielle pour renforcer la confiance des patients envers les systèmes d'IA. Si les patients ne comprennent pas comment les décisions médicales sont prises, ils peuvent être réticents à faire confiance à ces technologies. (cf. *infra*, p. 33 et 41)

6. Cadre réglementaire et normatif

- **Évolution rapide de la technologie** : La réglementation doit constamment évoluer pour suivre le rythme des avancées technologiques. Cela nécessite une collaboration étroite entre les développeurs, les professionnels de la santé et les régulateurs.

- **Harmonisation des réglementations** : Au niveau international, des différences dans la réglementation de l'IA en santé peuvent compliquer la mise en œuvre de solutions à l'échelle mondiale et créer des disparités dans la protection des patients.

Droit de l'espace numérique

7. Impact sur la pratique médicale

- **Redéfinition du rôle des professionnels de santé :** L'intégration de l'IA dans la pratique médicale pourrait modifier la relation entre les médecins et les patients, ainsi que le rôle des médecins eux-mêmes. Cela soulève des questions sur la déontologie et la responsabilité professionnelle.
- **Formation et compétences :** Les professionnels de santé doivent être formés non seulement à l'utilisation des technologies d'IA, mais aussi à la compréhension de leurs implications éthiques et juridiques.

8. Dilemmes éthiques

- **Utilisation de l'IA pour des décisions de fin de vie :** L'utilisation de l'IA pour des décisions critiques, comme les soins palliatifs ou les décisions relatives à la fin de vie, soulève des dilemmes éthiques profonds qui doivent être abordés avec soin.
- **Manipulation des données :** Les technologies d'IA peuvent être utilisées pour manipuler des données ou influencer les décisions des patients, ce qui pose des questions éthiques sur l'intégrité des soins de santé.

Les défis éthiques et juridiques associés à l'utilisation de l'IA dans le droit de la santé nécessitent une réflexion approfondie et une collaboration multi-sectorielle. La mise en place de cadres

Droit de l'espace numérique

réglementaires robustes, d'une formation adéquate pour les professionnels de santé et d'approches centrées sur le patient est essentielle pour garantir que les bénéfices de l'IA en santé soient réalisés tout en respectant les droits et les valeurs des individus. Un dialogue continu entre les parties prenantes est crucial pour relever ces défis et naviguer dans le paysage complexe de l'IA et de l'éthique en santé.

II) Le renforcement des droits du patient

L'intégration de l'IA dans le domaine de la santé présente des opportunités uniques pour renforcer la relation entre médecins et patients. Bien que l'IA puisse automatiser certaines tâches et fournir des analyses avancées, son utilisation doit être orientée vers l'amélioration de l'interaction humaine et de la qualité des soins. Voici plusieurs façons dont l'IA peut renforcer cette relation.

1. Soutien à la prise de décision

- **Assistance au diagnostic** : Les systèmes d'IA peuvent fournir aux médecins des recommandations basées sur l'analyse de données cliniques et d'études de cas. Cela peut leur permettre de poser des diagnostics plus précis et de proposer des traitements adaptés, renforçant ainsi la confiance des patients dans leurs soins.
- **Accès à l'information** : L'IA peut aider les médecins à accéder rapidement à des informations médicales pertinentes, réduisant le temps passé à rechercher des données et leur permettant de se

Droit de l'espace numérique

concentrer sur l'interaction avec le patient.

2. Personnalisation des soins

- **Traitements adaptés** : L'IA peut analyser les données individuelles des patients, y compris leur historique médical, leurs facteurs de risque et leurs préférences, pour proposer des traitements personnalisés. Cela montre aux patients que leurs besoins spécifiques sont pris en compte, renforçant leur engagement et leur satisfaction.

- **Suivi des patients** : Grâce à des outils de monitoring basés sur l'IA, les médecins peuvent suivre l'évolution de la santé de leurs patients en temps réel. Cela permet d'intervenir plus rapidement en cas de besoin et d'ajuster les traitements, ce qui renforce la perception de soins attentifs et proactifs.

3. Amélioration de la communication

- **Chatbots et assistants virtuels** : Ces outils peuvent répondre aux questions fréquentes des patients, fournir des informations sur les traitements et aider à la gestion des rendez-vous. Cela libère du temps pour les médecins, leur permettant de se concentrer sur des interactions plus significatives avec leurs patients.

- **Éducation des patients** : L'IA peut aider à créer des ressources éducatives personnalisées, permettant aux patients de

Droit de l'espace numérique

mieux comprendre leur état de santé et les options de traitement. Une meilleure compréhension favorise des discussions plus ouvertes et éclairées entre médecins et patients.

4. Renforcement de la confiance

- **Transparence dans l'utilisation des technologies** : En expliquant comment l'IA est utilisée dans le processus de diagnostic et de traitement, les médecins peuvent renforcer la confiance des patients dans ces outils. Lorsque les patients comprennent que l'IA est un soutien et non un remplacement, ils sont plus susceptibles de s'engager dans leur parcours de soins.

- **Partage des données** : Les outils d'IA peuvent permettre un partage transparent des données de santé avec les patients, leur donnant un meilleur contrôle et une meilleure compréhension de leur propre santé.

5. Facilitation de l'intervention préventive

- **Analyse prédictive** : L'IA peut identifier des tendances et des facteurs de risque, permettant aux médecins d'adopter une approche préventive. Cela non seulement améliore la santé des patients, mais renforce également leur relation avec leur médecin, qui se positionne en tant que partenaire dans la gestion de leur santé.

- **Programmes de bien-être** : Les recommandations générées

Droit de l'espace numérique

par l'IA sur les modes de vie peuvent encourager les patients à s'impliquer activement dans leur santé, instaurant ainsi une dynamique collaborative.

6. Amélioration de l'expérience patient

- **Réduction des temps d'attente** : En optimisant la planification et la gestion des ressources, l'IA peut contribuer à réduire les temps d'attente pour les consultations, améliorant ainsi l'expérience des patients.

- **Feedback en temps réel** : Des outils d'IA peuvent permettre aux patients de fournir un retour d'expérience immédiat sur leurs soins, permettant aux médecins d'ajuster leur approche et de mieux répondre aux attentes des patients.

L'IA représente un puissant outil pour renforcer la relation entre médecins et patients. En permettant une meilleure prise de décision, une personnalisation des soins, une communication améliorée et une approche préventive, l'IA peut contribuer à établir une dynamique collaborative et de confiance. Cependant, il est essentiel que l'implémentation de ces technologies soit accompagnée d'une attention particulière aux valeurs humaines, à l'éthique et à la protection des données, afin de garantir que la relation médecin-patient reste au cœur des soins de santé.

Droit de l'espace numérique

III) L'éthique, la pierre angulaire dans la protection de l'usage des systèmes d'intelligence artificielle

L'éthique de l'intelligence artificielle en santé contribue à la reconnaissance **de trois principes fondamentaux protecteurs** lors de son utilisation. Elle peut tout particulièrement s'exprimer à travers la mise en place d'un nouveau cadre de réflexion et, si possible, par un futur observatoire européen des développements et des usages de l'IA. Est aussi préconisée la promotion de certifications spécifiques des algorithmes dans le domaine de la santé qui ne pourraient être envisageables qu'au niveau des réglementations européennes, sauf à promouvoir un volontariat au niveau national. *In fine*, le rapport Touraine¹⁸ émet treize recommandations spécifiques dans le domaine du numérique, ce qui témoigne de toute l'importance de ce champ lors de la prochaine révision des lois de bioéthique.

Les trois principes fondamentaux du recours à l'IA en santé permettent d'offrir des garanties aux patients. Ces dernières peuvent s'exprimer à travers trois principes fondamentaux : **le principe de garantie humaine du numérique en santé, le principe de l'explicabilité de l'algorithme et le principe de l'effectivité du consentement de la personne.**

¹⁸. *Rapport d'information fait au nom de la mission d'information sur la révision de la loi relative à la bioéthique*, n° 1572, janvier 2019, dit Rapport Touraine, propositions 41 à 53.

Droit de l'espace numérique

a) Le principe de garantie humaine du numérique en santé

Le Comité consultatif national d'éthique (CCNE) a initié un principe visant à garantir une supervision humaine dans l'utilisation du numérique en santé, repris dans l'IA Act. Ce principe a pour objectif de « *garantir une supervision humaine de toute utilisation du numérique en santé, et l'obligation d'instaurer, pour toute personne le souhaitant et à tout moment, la possibilité d'un contact humain susceptible de lui transmettre l'ensemble des informations la concernant dans le cadre de son parcours de soins* »¹⁹. Ce principe assure que toute personne peut, à tout moment, contacter un professionnel de santé pour obtenir des informations sur son parcours de soins, préservant ainsi la maîtrise finale du praticien dans la prise de décisions.

Selon Monsieur David Gruson, Président d'Ethik-IA, cette supervision s'exprime à travers la « *nécessité de préserver la maîtrise finale du professionnel de santé, en interaction avec le patient, pour prendre des décisions appropriées en fonction de chaque situation spécifique* ». Il propose l'élaboration de recommandations de bonnes pratiques par la Haute autorité de santé. Deux actions concrètes sont suggérées :

¹⁹. Avis 129 du CCNE du 8 septembre 2019. Voir également : la reconnaissance du principe de Garantie Humaine dans la révision de la loi Bioéthique du 2 août 2021. L'article 17 de la loi est retranscrit dans le Code de la santé publique (CSP) à l'article L.4001-3.

Droit de l'espace numérique

- **Vérification des algorithmes** : Instituer des procédures de vérifications régulières des options de prise en charge par un « *collège de garantie humaine* » qui consultera des dossiers médicaux pour assurer la pertinence des diagnostics algorithmiques ;
- **Acte de télémédecine de garantie humaine** : Établir un nouvel acte permettant aux patients ou médecins d'obtenir un second avis médical en cas de doute sur les solutions thérapeutiques proposées par un algorithme.

À défaut, en cas de recours à un système d'IA pour établir un diagnostic sans supervision humaine, pourraient être invoqués l'article L.4161-1 du Code de la santé publique concernant l'exercice illégal de la médecine et l'article 10 de la loi « Informatique et Libertés » du 6 janvier 1978 prévoyant qu'aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé des données.

b) Le principe d'explicabilité de l'algorithme

Afin de permettre un meilleur jugement critique des médecins à l'égard des résultats algorithmiques en termes de diagnostics suggérés par la machine, gage de leur autonomie décisionnelle leur permettant de décider en connaissance de cause s'il convient ou pas d'en tenir compte lors des soins, le rapport préconise une exigence d'explicabilité permettant de comprendre le pourquoi et le comment de la proposition émise par l'algorithme.

Droit de l'espace numérique

La CNIL et le Conseil d'État soulignent la nécessité d'informations claires sur la « *logique de fonctionnement* » des algorithmes et les critères utilisés pour classer les données. Cédric Villani met l'accent sur l'importance des « *critères déterminants* » qui influencent les résultats des algorithmes, y compris ceux qui apprennent de nouvelles données. Raja Chatila²⁰ propose que l'exigence d'explicabilité soit adaptée aux différents publics (spécialistes ou non), en se concentrant particulièrement sur les médecins, afin de renforcer la relation médicale et d'assurer des garanties éthiques. Cette approche est reprise dans un rapport qui préconise d'instaurer une exigence légale d'explicabilité des algorithmes, précisant leur fonctionnement et les critères d'évaluation des informations. L'explicabilité est essentielle pour permettre aux professionnels de santé d'améliorer leur communication avec les patients concernant les choix de traitement. Enfin, il est important de distinguer l'explicabilité de la transparence, laquelle se réfère simplement à la publication du code source, sans éclairer les mécanismes décisionnels sous-jacents.

Le développement de l'explicabilité en santé passe par une formation des médecins sur l'utilisation de l'IA, incluant des compétences en encodage et structuration des données. En 2019, la Conférence des doyens a introduit un module sur la médecine algorithmique pour les étudiants. L'IA est également priorisée dans

20. Raja Chatila est Professeur d'intelligence artificielle, de robotique et d'éthique à Sorbonne Université.

Droit de l'espace numérique

le développement professionnel continu.

c) Le principe du consentement éclairé du patient

Concernant le consentement pour la collecte des données de santé, le rapport souligne la nécessité d'une sensibilisation accrue des patients et des professionnels. Il est recommandé de maintenir le droit existant en matière de consentement, tout en établissant des bonnes pratiques pour garantir son effectivité. Pour l'utilisation d'algorithmes d'aide à la décision, une information préalable est conseillée, avec un pictogramme pour signaler leur utilisation.

Les patients devraient avoir la possibilité d'exiger une intervention humaine, et des aménagements pratiques du consentement prévu par le Code de la santé sont souhaités. Un dispositif séquentiel de recueil de consentement est proposé, ainsi que des mécanismes plus protecteurs pour les populations vulnérables. Enfin, le soutien de personnes de confiance et d'associations est recommandé pour accompagner les patients dans leurs décisions liées à l'usage d'algorithmes. Des recommandations pratiques sont proposées pour adapter le consentement aux traitements impliquant des algorithmes.

Le cadre de réflexion éthique sur IA en santé est en constante évolution, en réponse aux défis posés par l'intégration de ces technologies dans les soins médicaux. Voici les principaux principes et éléments qui composent ce cadre éthique.

Droit de l'espace numérique

1. Autonomie du patient

L'un des principes fondamentaux de l'éthique médicale est le respect de l'autonomie des patients. Cela implique :

- **un consentement éclairé** : Les patients doivent être pleinement informés des technologies d'IA utilisées dans leur diagnostic et traitement, y compris les bénéfices et les risques associés. Ils doivent également comprendre comment leurs données sont utilisées.

- **le droit à l'information** : Les patients ont le droit de comprendre comment les décisions concernant leur santé sont prises, en particulier lorsque celles-ci s'appuient sur des algorithmes.

2. Justice et équité

L'IA en santé doit être accessible à tous sans discrimination. Ce principe implique :

- **Équité d'accès** : Assurer que les nouvelles technologies ne creusent pas les inégalités en matière de soins de santé, mais contribuent à les réduire.

- **Contrôle des biais** : Les algorithmes doivent être conçus et testés pour éviter des biais qui pourraient affecter certaines populations de manière disproportionnée.

Droit de l'espace numérique

3. *Bienfaisance et non-malfaisance*

Ces principes exigent que les technologies d'IA soient utilisées pour le bien des patients :

- **Amélioration des soins** : L'utilisation de l'IA doit viser à améliorer les résultats de santé et à optimiser les interventions médicales.
- **Prévention des préjudices** : Il est crucial de s'assurer que l'utilisation de l'IA ne cause pas de dommages, que ce soit par des erreurs de diagnostic, des traitements inappropriés ou des atteintes à la vie privée.

4. *Transparence et explicabilité*

Pour renforcer la confiance des patients et des professionnels de santé dans les systèmes d'IA :

- **Transparence des algorithmes** : Les développeurs et les utilisateurs doivent être capables de comprendre comment et pourquoi une décision a été prise par une IA.
- **Explicabilité** : Les résultats fournis par les systèmes d'IA doivent être expliqués de manière claire pour permettre aux médecins et aux patients de faire des choix éclairés.

Droit de l'espace numérique

5. Engagement des parties prenantes

Un cadre éthique efficace doit impliquer divers acteurs :

- **Collaboration interdisciplinaire** : Les médecins, les informaticiens, les juristes et les éthiciens devraient travailler ensemble pour développer des systèmes d'IA qui répondent aux normes éthiques.

- **Implication des patients** : Les patients doivent être inclus dans le développement et l'évaluation des technologies d'IA pour s'assurer qu'elles répondent à leurs besoins et préoccupations.

Un cadre de réflexion éthique sur l'intelligence artificielle en santé est essentiel pour garantir que ces technologies améliorent réellement les soins sans compromettre les valeurs fondamentales de la médecine. En intégrant ces principes éthiques dans la conception et l'implémentation des systèmes d'IA, nous pouvons créer un avenir où l'innovation technologique et le respect des droits des patients vont de pair.

Droit de l'espace numérique

Général d'armée (2S) Marc Watin-Augouard

Les créations par l'intelligence artificielle (IA) sont-elles des œuvres de l'esprit ?

La reconnaissance des œuvres générées par l'IA pose la question de la titularité des droits d'auteur. Actuellement, dans la plupart des juridictions, seul l'être humain peut être reconnu comme titulaire de droits sur une œuvre.

L'IA a besoin de créations d'autrui pour s'entraîner (*input*). Mais l'IA produit aussi de nouvelles « créations » artificielles (*output*). Selon le blog de *Creative Diffusion*, « les algorithmes de générations d'images à partir de textes ont généré un volume aussi important en un an (15 milliards d'images) que le nombre total de photographies prises en 150 ans, entre 1826 et 1975 ». Et ce constat ne porte que sur 2023, la première année de « démocratisation » de l'IA générative. Les productions générées par l'IA, données de résultat, sont-elles des œuvres de l'esprit pouvant être protégées par le droit d'auteur ? Dans l'affirmative, qui est titulaire du droit ? Qu'en est-il si la création a été générée de manière autonome par une IA ?

La question a notamment été posée lors de la vente aux enchères du Portrait « d'Edmond de Belamy », membre inventé d'une famille bourgeoise du XIX^e siècle. Il s'agit de la première œuvre d'art conçue par un algorithme. Ce tableau a été vendu aux enchères chez Christie's à New York pour la somme de 432 500 dollars, le 25 octobre 2018. 15 000 portraits réalisés entre le Moyen Âge et le XX^e siècle ont été analysés par un premier logiciel. Le résultat a été

Droit de l'espace numérique

optimisé par un second, afin de rendre crédible une création d'origine humaine. L'auteur de ce tableau est un programme informatique, ce qui semble exclure les artistes.

Une œuvre exclusivement créée par l'IA est-elle protégeable ? La réponse à la question posée appelle un examen sur la contribution de l'humain à sa réalisation.

Le droit d'auteur s'applique au bénéfice des humains et non à une machine. Une production peut, on l'a dit, être qualifiée « d'œuvre de l'esprit » si elle est originale et est le fruit de l'intervention humaine. L'originalité est définie comme révélant l'empreinte de la personnalité de l'auteur, d'une démarche consciente. C'est la position de la Cour de justice de l'Union européenne a qui a affirmé que le droit d'auteur ne s'appliquait qu'à des œuvres originales, créations intellectuelles propres à leur auteur¹.

I) Les créations assistées par une IA

Elles s'appuient sur un outil qui est sous contrôle d'humains. L'IA dépend des instructions et objectifs fixés par des humains. La création est l'expression d'une personnalité, d'une sensibilité que n'a pas la machine qui est réduite à l'association de formes, de couleurs ou de sons. Elle ne crée pas d'œuvres originales, condition

¹. CJUE, arrêt du 16 juillet 2009, affaire C-5/08 *Infopaq International A/S contre Danske Dagblades Forening*.

Droit de l'espace numérique

exigée par le droit d'auteur. Les résultats de l'utilisation de l'IA ne peuvent être attribués qu'à l'auteur qui a une part créatrice dans l'œuvre dès lors qu'il choisit les données d'entraînement ou intervient sur l'IA en retravaillant la création générée.

Mais il faut rechercher ce qui relève réellement de la création humaine en ne considérant que la partie de l'œuvre qui lui est propre, si l'on se réfère à une décision de l'*US Copyright Office* (USCO). En 2023, le bureau américain du droit d'auteur a reconsidéré la protection du droit d'auteur qu'il avait accordée en 2022 à Kristina Kashtanova pour sa bande dessinée *Zarya of The Dawn*. S'il l'a reconnue comme l'auteur du texte de l'œuvre ainsi que de la sélection, de la coordination et de l'arrangement des éléments écrits et visuels de l'œuvre, il lui a dénié cette qualité pour les images qui « *ne sont pas le produit d'une paternité humaine* » puisqu'elles ont été fabriquées par Midjourney, générateur d'images d'intelligence artificielle. Il faudrait donc que l'humain agisse avec suffisamment de créativité sur le contenu généré par l'IA pour que toute l'œuvre soit regardée comme étant une œuvre originale protégée par le droit d'auteur. Pour l'heure, les créations issues de l'IA, sans apport de créativité humaine, ne sont pas protégeables par le droit d'auteur. Il faut donc les analyser au cas par cas en examinant les situations qui ouvrent des droits, celles qui les excluent et les œuvres hybrides.

Le 27 novembre 2023, le *Beijing Internet Court*, juridiction chinoise spécialisée dans les contentieux relatifs à Internet, a accordé une protection par le droit d'auteur à une œuvre d'art générée par

Droit de l'espace numérique

Stable Diffusion. C'est la première décision mondiale qui reconnaît ce droit à propos d'un portrait réalisé par l'IA par une personne nommée Li Yunkai. Ce portrait a été utilisé par un tiers pour illustrer un poème, sans faire mention de l'auteur. Ce dernier a été reconnu titulaire d'un droit d'auteur, car la précision des *prompts* ayant été à l'origine du portrait et de son décor traduisait un investissement intellectuel suffisant pour attribuer un droit d'auteur. Tel n'est pas le cas du développeur de l'IA générative qui n'a pas eu l'intention de créer l'image objet de la contestation.

II) Les œuvres exclusivement créées par une IA

Le portrait « d'Edmond de Belamy » semble entrer dans cette catégorie, dans la mesure où l'IA est intervenue seule, sans initiative créatrice. Hugo Casselles-Dupré, l'un des membres du groupe « Obvious » à l'origine du projet, s'interroge :

« On a le même type de commentaire que les photographes ont eu quand la photographie est apparue. Tout le monde leur disait "Ce n'est pas de l'art, c'est du travail d'ingénieur, c'est automatisé", etc. Or, on se rend compte aujourd'hui qu'il y a des photographes meilleurs que d'autres. De la même manière, avec l'IA, il y a des artistes meilleurs que d'autres ».

Pour l'US Copyright Office, une œuvre d'art créée de manière autonome par une IA ne peut pas être considérée comme une « œuvre d'auteur originale », car la paternité de l'œuvre doit être entièrement humaine et l'expression non humaine n'est pas éligible à la protection du droit d'auteur (*Ryan Abbott case*, 14 Février 2022).

Droit de l'espace numérique

L'œuvre en cause, *A Recent Entrance to Paradise*, représentait une voie ferrée dans un cadre luxuriant de végétation et de glycines, créée par un système d'IA. La demande de droit d'auteur, émanant de son inventeur, Stephen Thaler, indiquait que l'œuvre avait été créée « *de manière autonome* » par un algorithme informatique et indiquait donc « Creativity Machine » comme l'auteur de l'œuvre d'art, et Stephen Thaler comme propriétaire de l'œuvre d'art en vertu de sa « *propriété de la machine* ». L'Office a refusé d'enregistrer la revendication au motif qu'elle ne satisfaisait pas au deuxième volet de l'exigence d'originalité de la loi sur le droit d'auteur, qui prend en compte la « *paternité* ». Selon l'Office, la revendication n'avait pas la « *paternité humaine* » nécessaire pour étayer une revendication de droit d'auteur.

En août 2023, le tribunal de district des États-Unis pour le district de Columbia a confirmé le refus de l'USCO d'enregistrer l'œuvre générée par l'IA, soulignant le principe de longue date selon lequel la loi sur le droit d'auteur ne protège que les œuvres de création humaine. La Cour a cependant considéré qu'une participation humaine minimale pouvait atteindre le seuil peu élevé de la protection par le droit d'auteur.

Au Royaume-Uni, aux États-Unis et en Europe, les services responsables de la propriété intellectuelle ont déclaré qu'une IA ne peut pas être un « *inventeur* » au regard de la législation sur les brevets. Mais la Cour fédérale australienne a contredit l'Office australien des brevets : « *Aucune des dispositions de la loi sur les brevets de 1990 n'exclut un inventeur qui soit un dispositif ou un*

Droit de l'espace numérique

système d'intelligence artificielle non humain [...] Un inventeur reconnu par la loi peut être un système ou un dispositif d'intelligence artificielle. Mais un tel inventeur non humain ne peut être ni demandeur d'un brevet ni titulaire d'un brevet ». Autre exemple illustrant la frontière ténue qui protège le droit d'auteur : une œuvre créée par une IA spécialisée dans la génération d'images s'est vue récompensée d'un premier Prix à la « *Colorado State Fair Fine Art Competition* » de 2022. L'œuvre, *Théâtre d'opéra spatial*, a été créée par Midjourney. Elle est le résultat d'un travail de plus de 80 heures, depuis la génération de l'image par l'IA jusqu'à son impression sur toile. Certes un prix ne crée pas de droits au regard de la propriété intellectuelle, mais il peut semer le trouble.

On notera qu'au Royaume-Uni, le 1988 *Copyright Designs and Patent Act* (art 9.3) attribue les droits à la personne qui a pris les dispositions nécessaires pour créer ladite œuvre au moyen d'un ordinateur².

Dans l'hypothèse où la création originale est éligible au droit d'auteur, qui est bénéficiaire du droit d'auteur ? Aux auteurs des œuvres ayant servi au modèle d'entraînement, c'est-à-dire à ceux qui ont créé les données d'*input* ? Aux concepteurs du modèle d'apprentissage automatique ? Au propriétaire de l'IA ? A la personne qui a orienté la machine par ses *prompts* ? Au client

². Dans le cas d'une œuvre littéraire, dramatique, musicale ou artistique générée par ordinateur, l'auteur est considéré comme la personne par laquelle les dispositions nécessaires à la création de l'œuvre sont prises.

Droit de l'espace numérique

considéré comme le propriétaire de l'œuvre ?

La difficulté tient à la pluralité des bénéficiaires potentiels. Les propriétaires des bases de données estiment qu'ils doivent avoir une part dans les bénéfices réalisés. C'est le sens de la démarche du *New York Times* vis-à-vis d'OpenAI. Le concepteur du modèle d'apprentissage peut aussi considérer que l'œuvre n'aurait pas existé sans son intervention. Il faut donc examiner au cas par cas, à la lumière notamment du droit européen le plus récent, celui contenu dans l'*AI Act*.

Son considérant 88 souligne bien la pluralité des acteurs : « *Tout au long de la chaîne de valeur de l'IA, plusieurs parties fournissent souvent des systèmes, des outils et des services d'IA, mais aussi des composants ou des processus que le fournisseur intègre dans le système d'IA avec plusieurs objectifs, dont l'entraînement de modèles, le réentraînement de modèles, la mise à l'essai et l'évaluation de modèles, l'intégration dans des logiciels ou d'autres aspects du développement de modèles. Ces parties ont un rôle important à jouer dans la chaîne de valeur vis-à-vis du fournisseur du système d'IA à haut risque dans lequel leurs systèmes, outils, services, composants ou processus d'IA sont intégrés, et devraient fournir à ce fournisseur, en vertu d'un accord écrit, les informations, les capacités, l'accès technique et toute autre assistance nécessaires sur la base de l'état de la technique généralement reconnu, afin de lui permettre de se conformer pleinement aux obligations énoncées dans le présent règlement, sans compromettre leurs propres droits de propriété intellectuelle ou secrets d'affaires* ».

Droit de l'espace numérique

A peine « démocratisée », l'IA met le droit à l'épreuve. La propriété intellectuelle n'est pas le seul domaine concerné, mais elle soulève la question fondamentale de la créativité. L'IA générative repose sur des LLM (*large language model*) qui ont été constitués, dans la plupart des cas, par des œuvres protégées par le droit d'auteur sans qu'une compensation financière soit accordée aux créateurs. La création est en danger et, avec elle, la culture et la civilisation. On comprend pourquoi la propriété intellectuelle est un des thèmes majeurs débattus dans les instances internationales. Le Partenariat mondial sur l'intelligence artificielle, instance d'origine franco-canadienne qui est liée à l'Organisation de coopération et de développement économiques (OCDE) et à l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), comme l'Organisation mondiale de la propriété intellectuelle (OMPI), agissent en vue d'une bonne intelligence entre le créateur et l'IA.

Actualité pénale

Nathan Allix

**Cour de justice de l'Union européenne et exploitation
des données d'un téléphone en enquête : une
nécessaire évolution du droit français**

CJUE, grande chambre, 4 oct. 2024, C-548/21

Si l'arrêt du 4 octobre dernier rendu par la grande chambre de la Cour de justice de l'Union européenne présente une importance certaine, celui-ci s'inscrit dans une affaire on ne peut plus banale : les services douaniers autrichiens, à l'occasion du contrôle d'un colis, ont constaté la présence de 85 grammes de cannabis. Lors de la perquisition domiciliaire du destinataire du colis, suspecté d'avoir commis un délit passible d'un an d'emprisonnement en droit autrichien, les agents de police autrichiens ont, de leur propre chef, saisi le téléphone portable de l'intéressé, lequel a refusé de donner accès aux données de connexion. À nouveau sans intervention d'un juge ou du ministère public, les agents de police ont alors transmis le téléphone à un expert afin de tenter de le déverrouiller.

Le propriétaire du téléphone a alors introduit un recours devant une juridiction chargée de contester, *a posteriori*, la légalité de la saisie. Ce n'est qu'à cette occasion que l'intéressé a été informé des tentatives d'exploitation de son téléphone, la procédure antérieure s'étant déroulée sans qu'il soit tenu au courant des opérations en cours. Dans cette situation, la juridiction devant laquelle le recours était porté a jugé nécessaire d'adresser les trois questions

Actualité pénale

préjudiciables suivantes. Si on les synthétise et les reformule (notamment dans la mesure où les questions étaient posées au regard de la directive 2002/58, alors que cette dernière n'est applicable que quand l'accès aux communications électroniques passe par un fournisseur de services de telles communications, ce qui a conduit la Cour à y substituer la directive 2016/680, dite directive « Police – Justice » : arrêt, points 57 et s.), les questions se présentaient ainsi :

1° Le droit de l'Union, à travers la directive précédemment rappelée et le droit à la vie privée reconnu par la Charte des droits fondamentaux, impose-t-il que l'accès des autorités publiques aux données stockées dans les téléphones portables en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales soit limité à la lutte contre la « *criminalité grave* » ?

2° Le droit de l'Union, à travers les mêmes textes, permet-il une législation nationale autorisant les forces de police à obtenir, dans le cadre d'une enquête, un accès complet et non contrôlé aux données numériques stockées dans un téléphone portable, et ce, de leur propre initiative, sans l'autorisation d'une juridiction ou d'une autorité administrative indépendante ?

3° L'égalité des armes et le droit à un recours effectif, tels qu'ils résultent de la Charte des droits fondamentaux de l'Union européenne, s'opposent-ils à un droit national permettant l'exploitation des données numériques d'un téléphone portable sans que la personne concernée soit informée au préalable de la mesure en cause, ou, *a minima*, soit mise au courant *a posteriori* ?

Actualité pénale

Les réponses à ces trois questions peuvent être rapidement synthétisées. D'abord, l'accès des autorités publiques aux données stockées dans les téléphones portables dans le cadre d'une procédure d'enquête n'est pas limité aux infractions les plus graves (arrêt, point 97), mais il appartient au législateur national « *de définir de manière suffisamment précise les éléments, notamment la nature ou la catégorie des infractions concernées, devant être pris en compte* » (arrêt, point 99). Ensuite, et sauf en cas d'urgence (arrêt, point 104), l'accès aux données contenues sur le téléphone doit faire l'objet d'une autorisation préalable « *soit par une juridiction, soit par une autorité administrative indépendante* » (arrêt point 102). Enfin, les autorités nationales ayant reçu l'autorisation en question doivent informer l'intéressé des motifs sur lesquels l'autorisation repose, à moins que cette information ne soit susceptible de compromettre les enquêtes menées par ces autorités (arrêt, point 120).

I) L'exploitation d'un téléphone portable en droit positif

À titre introductif, l'empilement des mesures pouvant impliquer un téléphone portable est tel qu'il ne paraît pas inutile de revenir, même rapidement, sur les autres mesures qui se distinguent, plus ou moins nettement, de celle objet de la présente affaire. L'exercice peut certes sembler scolaire : il n'est toutefois pas inutile dans la mesure, à la fois, où des décisions rendues dans le domaine d'autres mesures permettent d'éclairer la présente décision (en particulier s'agissant des géolocalisations), et où d'autres mesures sont susceptibles d'être directement concernées par le présent arrêt (accès à distance aux correspondances stockées par la voie des

Actualité pénale

communications électroniques accessibles au moyen d'un identifiant informatique et captation des données informatiques).

On pense, bien sûr, aux opérations de géolocalisation, bien que celles-ci puissent porter sur d'autres objets qu'un téléphone, en particulier un véhicule, et que la différence avec l'exploitation des données se trouvant sur le téléphone portable soit claire. Pour mémoire, la géolocalisation au sens strict concerne la localisation en temps réel, le recueil *a posteriori* des données de géolocalisation qui seraient détenues, principalement, par les opérateurs téléphoniques relevant des réquisitions prises sur le fondement des articles 60-1 et 77-1-1 du Code de procédure pénale (CPP) selon que l'on se trouve en enquête préliminaire ou de flagrance (Cass. crim., 2 nov. 2016, n° 16-82.376 sur cette dernière hypothèse). La géolocalisation en temps réel, quant à elle, admise de longue date pendant l'instruction, est possible durant la phase d'enquête depuis l'entrée en vigueur de la loi du 28 mars 2014 et est régie par les articles 230-32 à 230-44 du CPP.

Par une décision proche du présent arrêt, la Cour de justice de l'Union européenne a considéré, d'une part, que seules les infractions les plus graves justifient la réquisition des données de connexion auprès d'un opérateur téléphonique et, d'autre part, que l'autorisation d'une telle mesure par le ministère public contrevient au droit de l'Union (CJUE, *H.K. c. Prokuratuur*, 2 mars 2021, C-746/18. Sur les conséquences en droit français : Cass. crim., 12 juill. 2022, n° 21-83.710). Pour la présente affaire, l'arrêt *H.K. c. Prokuratuur* est éclairant d'au moins deux façons. D'une part, la limitation des

Actualité pénale

réquisitions aux données de connexion aux infractions les plus graves diffère de la solution retenue s'agissant de l'exploitation des données se trouvant sur un téléphone portable (cf. *infra*), sans que la raison de cette différence ne paraisse évidente au regard de la gravité des mesures ainsi que de leur intérêt pour permettre la manifestation de la vérité. D'autre part, le présent arrêt ne se prononçant pas directement sur ce point, l'arrêt *H.K. c. Prokuratuur* rend certain le fait que le ministère public ne constitue pas, pour la Cour de justice de l'Union européenne, une « *juridiction* », le Parquet n'étant, selon la Cour, pas jugé suffisamment indépendant (à l'égard du pouvoir exécutif) et impartial (dans la mesure où il a vocation à exercer les poursuites) pour autoriser et contrôler les mesures les plus attentatoires aux libertés individuelles.

On peut également penser aux interceptions de correspondances émises par la voie des communications électroniques : admises de façon très limitée durant la phase d'enquête, elles ne sont, hors de l'instruction, envisageables qu'en matière de délinquance et de criminalité organisées (CPP, art. 706-95, renvoyant sur le champ d'application aux articles 706-73 et 706-73-1 du CPP). Si l'opération se rapproche davantage de celle objet du présent arrêt, elle s'en distingue aisément dans la mesure, d'une part, où elle ne porte que sur les communications et, d'autre part, où elle consiste en une interception en temps réel et sans passer par une recherche sur le téléphone impliqué. Sans rentrer dans le détail d'un régime qui emprunte largement aux articles 100-1 à 100-8 du CPP, applicables durant l'information, cette mesure est, dans le cadre des mesures d'enquête spéciales, initiée par le procureur mais est autorisée, et

Actualité pénale

contrôlée, par le JLD.

Entre opération de géolocalisation et d'interception des correspondances, on peut encore envisager, dans le champ de la criminalité et de la délinquance organisées, la mise en place d'*IMSI Catcher* (CPP, art. 706-95-20) : ce dispositif, principalement destiné à recueillir les données permettant « *l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur, ainsi que les données relatives à la localisation d'un équipement terminal utilisé* » (I de l'article) peut également être utilisé pour intercepter les correspondances. Si l'opération est toujours autorisée, pendant la phase d'enquête, par le juge des libertés et de la détention (JLD) (706-95-12, 1°. Pour l'information, l'opération est autorisée par le juge d'instruction), la durée d'interception des correspondances est alors réduite à quarante-huit heures, renouvelable une fois.

Enfin, plus proche encore, dans sa matérialité, de l'exploitation d'un téléphone portable, mais également limitée au domaine des articles 706-73 et 706-73-1, on trouve en enquête (CPP, art. 706-95-1), comme durant l'information (CPP, art. 706-95-2), « *l'accès, à distance et à l'insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique* ». Cette fois, l'accès aux communications ne se fait plus en temps réel mais continue à ne pas nécessiter un accès physique au téléphone. On peut également penser à la captation des données informatiques (CPP, art. 706-102-1), qui consiste à mettre en place un dispositif permettant d'enregistrer, de conserver et de transmettre les informations telles qu'elles s'affichent sur un écran, telles qu'elles sont stockées, telles

Actualité pénale

qu'elles sont saisies ou telles qu'elles sont reçues et émises par des périphériques, ce qui permet, notamment, de contourner les difficultés liées au cryptage des conversations. La mesure est assez similaire à l'exploitation des données se trouvant sur un téléphone portable dans la mesure où elle permet potentiellement l'accès à toutes les données se trouvant sur le matériel. Elle est toutefois nettement plus attentatoire aux libertés individuelles, dans la mesure où elle permet, à distance et à l'insu de celui qui utilise le dispositif, d'avoir connaissance, en temps réel ou *a posteriori*, de l'ensemble des données, même effacées, qui auraient transité par le matériel objet de la mesure pendant la durée de celle-ci. Dans un cas comme dans l'autre, ces techniques spéciales d'enquête sont systématiquement autorisées par un juge du siège, JLD en enquête et juge d'instruction pendant l'information (même si pendant l'information, un officier de police judiciaire – OPJ – peut requérir la Direction générale de la sécurité intérieure (DGSI) dans la perspective de la mise en place de cette mesure, si sa commission rogatoire le permet : Cass. crim., 5 mars 2024, n° 23-84.626).

À côté de toutes ces mesures se trouve, au cœur de la présente affaire, l'exploitation des données se trouvant sur un téléphone portable. Cette mesure est peut-être la plus simple à comprendre : elle consiste à accéder aux données se trouvant sur un téléphone portable dont sont en possession les enquêteurs, que ce soit notamment dans le cadre d'une perquisition ou à sa suite, ou lorsque le propriétaire du téléphone en question a été interpellé ou placé en garde à vue. Dans la première hypothèse, l'article 57-1 du CPP, qui prévoit que les OPJ, ou sous leur contrôle les adjoints de police

Actualité pénale

judiciaire (APJ), peuvent « *au cours d'une perquisition [...] accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système* », permet bien d'accéder aux données présentes sur un téléphone portable, ou accessibles depuis ce téléphone, qui serait trouvé au cours d'une perquisition. À l'exception de cette hypothèse, aucune disposition textuelle ne prévoit l'exploitation d'un téléphone portable qui serait en possession des enquêteurs. C'est dans ce contexte que la Cour de cassation a décidé d'appliquer le régime des perquisitions à l'exploitation des données d'un téléphone portable (Cass. crim., 12 janv. 2021, n° 20-84.045), ce qui signifie, en enquête de flagrance, que la mesure peut être décidée par un OPJ, sous le contrôle du ministère public, en enquête préliminaire que la mesure doit être, en l'absence de consentement de l'intéressé, autorisé par le JLD (CPP, art. 76, al. 4 et 76-3). Bien que les perquisitions soient entourées de certaines garanties, c'est donc un régime relativement souple qui est prévu par le droit français, lequel apparaît, à plusieurs égards, incompatible avec les réponses apportées par la Cour de justice de l'Union européenne.

II) Les modifications rendues nécessaires par l'arrêt

Ce sont en réalité les trois réponses apportées par la Cour de justice aux questions qui lui étaient posées qui peuvent conduire à penser que le droit français n'est pas en conformité avec le droit de l'Union, particulièrement les deux premières.

Ainsi, à la question qui lui était posée quant à la nécessité de limiter

Actualité pénale

l'accès par les autorités publiques aux données stockées sur un téléphone à la lutte contre la « *criminalité grave* » (arrêt, point 30, 1), notamment au regard du droit à la vie privée et au respect des données personnelles, la Cour de justice, tout en estimant qu'il n'y a pas lieu de limiter l'exploitation des données se trouvant sur un téléphone par les enquêteurs à la « *criminalité grave* », considère qu'une telle limitation risquerait de conduire à « *un accroissement du risque d'impunité pour de telles infractions compte tenu de l'importance que peuvent avoir de telles données pour les enquêtes pénales* » (arrêt, point 97. On ne reviendra pas ici sur les interrogations quant à la cohérence de cette solution avec celle retenue par la Cour de justice, s'agissant des réquisitions de données de connexion¹). Toutefois, la Cour, rappelant qu'il résulte de l'article 52 paragraphe 1 de la Charte des droits fondamentaux que toute limitation à un droit fondamental consacré par la Charte, en l'espèce le droit à la vie privée et à la protection des données personnelles, doit non seulement être nécessaire et proportionnée à la poursuite d'objectifs d'intérêt général, mais aussi être prévue par la loi, considère qu'il incombe au législateur de définir de manière suffisamment précise les infractions permettant le recours à l'exploitation des données d'un téléphone portable, notamment au regard de la nature ou des catégories d'infraction concernées (arrêt, points 98 et 99). La Cour souligne, en outre, que la mesure ne peut concerner qu'une personne à l'égard de laquelle il existe des

¹. Sur ce point, voir : AUROY, Benoît. « Procédure pénale et exploitation d'un téléphone portable : le développement de la protection européenne », D. 2024.2099, § I.

Actualité pénale

éléments objectifs et suffisants permettant de considérer qu'elle est suffisamment impliquée dans l'infraction, réalisée, en cours ou projetée, à l'occasion de laquelle la mesure est mise en œuvre (arrêt, point 101).

Force est alors de constater que le droit français n'est, sur ce point, pas en conformité avec le droit de l'Union. Le constat est évident hors du domaine de l'article 57-1 du CPP, aucun texte ne prévoyant alors le recours à la mesure (par exemple pour exploiter les données se trouvant sur le téléphone d'une personne placée en garde à vue). Même dans le champ de cet article, il n'est pas certain que les exigences européennes soient respectées. La question se présente un peu différemment durant l'enquête de flagrance ou durant l'enquête préliminaire. En effet, en enquête de flagrance, la mesure prévue à l'article 57-1 du CPP est toujours possible, à l'initiative d'un OPJ (ou sous son contrôle d'un APJ). On pourrait certes arguer que la flagrance n'est possible qu'en matière de crime ou de délit puni d'emprisonnement (CPP, art. 53 et 67). Un tel encadrement, particulièrement lâche, peut sembler insuffisant pour respecter l'exigence de la Cour de justice selon laquelle la loi doit définir de façon « *suffisamment claire et précise* » l'infraction (arrêt, point 98).

L'affaire est, paradoxalement, moins claire en enquête préliminaire. Certes, à la différence de l'enquête de flagrance, le domaine de cette enquête n'est pas limité par la gravité de l'infraction. Mais l'enquête préliminaire se caractérisait traditionnellement par l'absence de faculté de contrainte : si ce caractère a été largement infléchi, il en subsiste certaines reliques. En particulier, dans cette

Actualité pénale

enquête, les perquisitions ne peuvent être réalisées qu'avec l'assentiment de l'intéressé ou, à défaut, et uniquement pour les crimes ou les délits punis de trois ans ou plus (ou pour la recherche de certains biens), avec l'autorisation du JLD (CPP, art. 76, al. 4). Finalement, le champ des infractions rendant possible le recours aux perquisitions de l'article 57-1 du CPP en enquête préliminaire paraît mieux défini.

Quoi qu'il en soit, dans de nombreuses hypothèses, il n'est pas discutable que l'exploitation des données se trouvant sur un téléphone se réalise actuellement en l'absence de toute base légale, rendant nécessaire une intervention législative pour encadrer cette mesure.

Il en va d'autant plus ainsi que la réponse de la Cour de justice de l'Union européenne à la deuxième question qui lui était posée fait également apparaître des insuffisances du droit français actuel.

À reprendre la solution dégagée par la Cour : il importe que « *lorsque l'accès des autorités nationales compétentes aux données à caractère personnel comporte le risque d'une ingérence grave, voire particulièrement grave, dans les droits fondamentaux de la personne concernée, cet accès soit subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante* » (arrêt, point 102). Ce n'est qu'en cas « *d'urgence dûment justifié[e]* » (arrêt, point 104) que la Cour admet un contrôle *a posteriori*, lequel doit alors « *intervenir dans de brefs délais* ».

Actualité pénale

La principale raison de cette exigence de contrôle est explicitée par la Cour, qui la met en lien avec la nécessité, évoquée à l'occasion de la première question qui lui était posée, d'assurer un respect concret, dans chaque affaire, du principe de proportionnalité découlant de l'article 52. À suivre le raisonnement de la Cour, pour que ce contrôle soit effectif et permette la protection des libertés individuelles escomptées, il importe que le contrôle préalable soit effectué par une juridiction ou par une entité administrative indépendante, dont on rappelle qu'elle ne peut être, selon la jurisprudence habituelle de la Cour (cf. *supra*), le ministère public.

À nouveau, il apparaît certain que le droit français applicable en matière d'exploitation des données se trouvant sur un téléphone portable n'est pas conforme aux exigences de la Cour. L'affaire est entendue en enquête de flagrance, les forces de l'ordre pouvant avoir recours à cette mesure de leur propre initiative. L'analyse n'apparaît cette fois pas beaucoup plus positive s'agissant de l'enquête préliminaire. Ainsi, par exemple, si l'exploitation du téléphone a lieu à l'occasion d'une garde à vue : par renvoi de l'article 77 aux articles 62-2 à 64-1 du CPP, le régime de la garde à vue est presque intégralement aligné sur celui applicable en enquête de flagrance, aboutissant au même constat de non-conformité. Ce n'est que lorsque l'exploitation se réalise au titre de l'opération prévue à l'article 57-1 (cf. *supra*) que le droit français peut sembler conforme au droit de l'Union. En effet, en enquête préliminaire, les services d'enquêtes ne sont, en application de l'article 76-3 du CPP, autorisés à recourir à cette opération que dans les conditions prévues à l'article 76 du même Code : or,

Actualité pénale

précisément, ainsi qu'il a été vu, en l'absence de consentement de la personne visée par la mesure, l'article 76 alinéa 4 dispose notamment que cette mesure ne peut intervenir que sur décision écrite et motivée du JLD. Dans ce cadre très précis, on pourrait donc éventuellement considérer que le droit français paraît conforme aux deux premières réponses apportées par la Cour.

Il n'en reste pas moins que cette éventuelle conformité serait, en tout état de cause, particulièrement limitée, si bien qu'à nouveau une réforme des règles applicables apparaît nécessaire pour confier à un juge du siège, à savoir très probablement le JLD², le rôle de contrôler *a priori* et, en cas d'urgence, *a posteriori* et à bref délai, la nécessité et la proportionnalité de la mesure.

S'agissant enfin de la troisième question, relative à la nécessité d'informer la personne concernée de l'existence de la mesure d'exploitation, la Cour de justice estime, en substance, qu'il résulte des articles 13 et 54 de la directive 2016/680 ainsi que du droit à un recours effectif consacré par l'article 47 de la Charte des droits fondamentaux que les autorités d'enquête devraient normalement informer la personne concernée par la mesure de celle-ci, dès lors

2. Voir, néanmoins, sur l'idée de créer un « *juge de l'enquête* » : AUDIBERT, Matthieu. Inconstitutionnalité différée des réquisitions de données informatiques par le procureur de la République dans le cadre de l'enquête préliminaire : le jour d'après. *Lexbase Pénal*, 23 déc.embre 2021, n° 44 . Voir également : L'exploitation d'un téléphone portable revue par la Cour de justice de l'Union européenne . *AJ Pénal* 2024.567.

Actualité pénale

que cela « *n'est pas susceptible de compromettre les enquêtes menées par ces autorités* » (arrêt, point 120), la Cour estimant que cette information est nécessaire à l'exercice des recours prévus par la directive précitée.

Précisant son propos, la Cour souligne qu'une « *réglementation nationale qui exclurait, de manière générale, tout droit à obtenir de telles informations ne serait pas conforme au droit de l'Union* » (arrêt, point 121). À nouveau, et sans entrer dans le détail, le droit français apparaît largement lacunaire sur cette question.

On l'aura compris, le droit français applicable en matière d'enquête suppose une refonte réelle, pour encadrer, à se limiter au domaine du présent arrêt, les hypothèses dans lesquelles l'exploitation des données se trouvant sur un téléphone portable est possible, pour prévoir un contrôle, normalement *a priori*, effectué par un juge du siège et organiser, dans la mesure du possible, l'information de la personne concernée par la mesure. On peut, à cet égard, formuler deux remarques conclusives.

D'une part, l'analyse de la Cour devrait s'appliquer *a fortiori* à des mesures permettant l'exploitation des données se trouvant sur un téléphone d'une façon plus intrusive encore que *via* l'appréhension physique du téléphone : accès à distance et à l'insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique et, d'une façon plus marquée encore, captation des données informatiques. Toutefois, dans un cas

Actualité pénale

comme dans l'autre, les risques de contrariété du droit français avec la présente décision de la Cour de justice semblent limités (à supposer, en tout cas, que la Cour ne retienne pas des exigences plus élevées s'agissant de ces mesures, ce qui est loin d'être certain) : ainsi qu'il a été vu, en effet, le droit national est heureusement bien plus défini et restrictif s'agissant de ces mesures de sorte que, pour l'essentiel, le droit national semble en conformité avec les réponses apportées par la Cour, au moins en ce qui concerne les deux premières questions.

D'autre part, d'une façon prudente, un auteur a pu estimer que, dans l'attente d'une réforme législative, « *le détenteur d'un téléphone portable serait malavisé de s'opposer aux enquêteurs qui souhaiteraient accéder aux données qu'il contient. Faut-il rappeler que, dans un arrêt du 7 novembre 2022, l'assemblée plénière de la Cour de cassation a confirmé que le refus de communiquer aux policiers le code de déverrouillage d'un téléphone pouvait constituer le délit prévu par l'article 434-15-2 du code pénal* », rappelant justement que « *s'agissant des infractions qui sanctionnent une forme d'insoumission aux forces de l'ordre, la jurisprudence tient largement pour indifférente à la consommation du délit les suites procédurales de l'affaire* »³. On se permettra néanmoins un certain désaccord avec cette analyse. En effet, dans la principale affaire rappelée par l'auteur au soutien de sa position, la Cour de cassation avait considéré que les infractions de rébellion et d'outrage étaient

3. AUROY, Benoît, *op. cit.* note 1, *in fine*.

Actualité pénale

caractérisées alors même qu'elles avaient eu lieu à l'occasion d'un contrôle d'identité, illicite comme ne s'inscrivant pas dans le cadre d'une enquête de flagrance (Cass. crim., 1^{er} sept. 2004, n° 04-80.362). S'il est vrai qu'il résulte de cet arrêt que l'irrégularité d'une mesure réalisée dans le cadre d'une enquête n'exclut pas la constitution d'une infraction constituée à l'occasion de cette mesure, on peut néanmoins penser qu'il en va différemment lorsque l'infraction consiste précisément à refuser une mesure qui serait, du fait des conditions de sa réalisation, contraire aux droits fondamentaux de la personne tels que reconnus par le droit de l'Union européenne.

Jérôme Millet

De l'anonymat des policiers et des gendarmes

(Note sous CE, 18 octobre 2024, n° 475283)

1. Dans son édition du 25 novembre 2024, *Le Figaro* révèle que, « dans la nuit du 29 au 30 octobre dernier, le procureur général de Douai est prévenu in extremis par la police que quatre individus stationnés dans sa rue s'apprêtent à s'en prendre à lui. Poursuivis en voiture, ils sont finalement interpellés à Roubaix. Il s'agit de quatre Algériens âgés de 20 à 40 ans, dont trois sous OQTF, avec des casiers judiciaires, pour certains extrêmement chargés »¹. L'enquête depuis menée pourrait fournir une nouvelle illustration des tentatives d'intimidation, voire de menaces, des services judiciaires dans le contexte de la lutte contre le narcotrafic. L'ancien ministre de l'Intérieur et des Outre-mer, Gérald Darmanin, avait pu rappeler, le 10 avril 2024, devant la commission d'enquête sur l'impact du narcotrafic en France², que « la drogue est la plus grande menace sécuritaire que notre pays et que le monde vont connaître (...) la situation est extrêmement préoccupante ». Or, comme chacun sait, l'indépendance de l'autorité judiciaire, dont le Président de la

1. GONZALÈS, Paule. Intimidation, menaces... ces magistrats français sous la pression des délinquants. *Le Figaro*, 25 novembre 2024, p. 12.

2. Rapport n° 588 des sénateurs Jérôme DURAIN et Etienne BLANC de la commission d'enquête sur *L'impact du narcotrafic en France et les mesures à prendre pour y remédier*, 7 mai 2024.

Police administrative

République est le garant³, implique que les magistrats puissent exercer leurs missions « *sans redouter que leurs décisions ou actions ne donnent lieu à des représailles ou des menaces à l'encontre de leur personne ou de leurs proches* », selon le communiqué de presse du Conseil supérieur de la magistrature du 8 novembre 2024⁴. Si les réflexions relatives à la déontologie de la sécurité sont importantes, autrement dit si la question : qui gardera les gardiens ? est fréquemment examinée, celle relative à la protection des forces de l'ordre ou de l'autorité judiciaire, autrement dit, la question : qui protégera les protecteurs ? l'est moins.

2. Il est vrai que le droit a accru la transparence de l'administration et le Code des relations entre le public et l'administration prévoit ainsi que « *toute personne a le droit de connaître le prénom, le nom, la qualité et l'adresse administratives de l'agent chargé d'instruire sa demande ou de traiter l'affaire qui la concerne ; ces éléments figurent sur les correspondances qui lui sont adressées (...)* » (art. L. 111-2). Issue de l'article 4 de la loi du 12 avril 2000, cette disposition vise précisément à lever l'anonymat de l'administration dans ses relations avec les administrés. Le texte réserve, certes, un certain nombre d'exceptions si des motifs intéressant la sécurité publique ou la sécurité des personnes le justifient.

3. L'article 64 de la Constitution dispose en effet que « *le Président de la République est garant de l'indépendance de l'autorité judiciaire* ».

4. CONSEIL SUPÉRIEUR DE LA MAGISTRATURE. Communiqué du 8 novembre 2024. Disponible sur : <http://www.conseil-superieur-magistrature.fr/publications/avis-et-communications/communique-du-8-novembre-2024>

Police administrative

3. Les faits de l'espèce remontent au 23 septembre 2017 et ne sont guère originaux : des fonctionnaires de police du commissariat du 15^e arrondissement de Paris interviennent chez un particulier à l'occasion d'un conflit de voisinage et rédigent, par la suite, quelques lignes sur le registre de main courante. Ce particulier, M. A..., demande, le 2 avril 2021, au préfet de police la communication de l'extrait du registre de main courante. L'administration ne communique à l'intéressé, le 18 mars 2021, qu'une version du document sollicité dans laquelle l'identité des fonctionnaires de police concernés avait été occultée. Pour cette raison, le requérant saisit la Commission d'accès aux documents administratifs (CADA), laquelle considère que le document sollicité est communicable au demandeur dans sa version non occultée, à condition toutefois que le préfet de police ne dispose pas d'éléments particuliers tenant à la personnalité du demandeur ou au contexte de sa demande, appréciés à la lumière de la sensibilité du contexte sécuritaire, laissant craindre que la divulgation de l'identité des agents concernés pourrait, en l'espèce, conduire à des représailles ciblées sur ces derniers⁵. Le tribunal administratif de Paris, saisi de la décision de refus du préfet de police, rejette la demande de communication du document sans occultation de l'identité de ces fonctionnaires. M. A... se pourvoit finalement en cassation contre le jugement du tribunal administratif du 27 avril 2023.

5. CADA, avis 20213925 - Séance du 22/07/2021.

Police administrative

4. Le Conseil d'État a estimé, dans un arrêt rendu le 18 octobre 2024, que les noms et prénoms des fonctionnaires de police figurant sur l'extrait du registre de main courante, établie par ces agents dans l'exercice de leurs missions, ne sont pas communicables⁶. Le juge administratif estime, en effet, que cette communication serait de nature à porter atteinte à la sécurité publique ou à la sécurité des personnes, eu égard à la qualité de fonctionnaires de police des intéressés. En se prononçant ainsi pour rejeter la demande d'annulation du refus du préfet de police de communiquer l'extrait du registre de main courante sans occultation de l'identité de ces agents, le TA de Paris n'a pas entaché son jugement d'erreur de droit. Pour son raisonnement, le Conseil d'État mobilise le Code des relations entre le public et l'administration. Son article L. 311-1 prévoit que, « *sous réserve des dispositions des articles L. 311-5 et L. 311-6, les administrations mentionnées à l'article L. 300-2 [l'Etat, les collectivités territoriales, les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission] sont tenues de publier en ligne ou de communiquer les documents administratifs qu'elles détiennent aux personnes qui en font la demande (...)* ». Mais, aux termes de l'article L. 311-5 du même Code : « *Ne sont pas communicables : / [...] 2° Les autres documents administratifs dont la consultation ou la communication porterait atteinte : / [...] d) A la sûreté de l'État, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations [...]* ».

6. CE, 18 octobre 2024, n° 475283, AJDA 2024, p. 1992.

Police administrative

5. Déjà, en 2017, le Conseil d'Etat avait jugé que la communication de la liste des noms, prénoms, fonctions et numéros de matricules des agents, officiers, gendarmes et/ou policiers affectés au Centre automatisé de constatation des infractions routières (CACIR) n'était pas communicable, ces informations étant susceptibles, eu égard à la qualité de fonctionnaires de police et de militaires de la gendarmerie des intéressés, de porter atteinte à la sécurité publique ou à la sécurité des personnes (CE, 15 décembre 2017, *Ministère de l'Intérieur c/ B...*, n° 405845, Rec., p. 613). De même, le rapporteur public de cette affaire devant le Conseil d'État, Laurent Domingo, rappelle que pour le même motif tiré du risque d'atteinte à la sécurité publique ou la sécurité des personnes, le juge administratif a retenu une solution comparable pour les fonctionnaires affectés dans les six pôles de la Mission interministérielle de vigilance et de lutte contre les dérives sectaires (Miviludes) (CE, 11 juillet 2016, *Premier ministre c/ Association Ethique et Liberté*, n° 392586, Rec. p. 334)⁷.

6. Il existe deux situations au moins où l'anonymat des policiers et des gendarmes est prévu.

D'une part, l'arrêté du 7 avril 2011 relatif au respect de l'anonymat de certains fonctionnaires de police et militaires de la gendarmerie nationale qui liste les services et unités « *dont les missions exigent,*

7. 10^{ème} et 9^{ème} chambres réunies. Conclusions de M. Laurent DOMINGO, rapporteur public. Disponible sur : https://www.conseil-etat.fr/fr/arianeweb/CRP/conclusion/2024-10-18/475283?download_pdf

Police administrative

pour des raisons de sécurité et en application de l'article 39 sexies de la loi du 29 juillet 1881 susvisée, le respect de l'anonymat des fonctionnaires et des militaires qui y servent ». La Chambre criminelle de la Cour de Cassation a déjà fait une interprétation jugée extensive⁸ de l'article 39 sexies de la loi du 29 juillet 1881⁹ à l'occasion d'une affaire dans laquelle un journal avait publié des informations qui, sans indiquer son identité, permettaient d'identifier un policier appartenant à un groupe désigné par l'arrêté de 2011 comme devant bénéficier de l'anonymat pour des raisons de sécurité. Des poursuites sont alors engagées contre le directeur de la publication sur le fondement de l'article 39 sexies de la loi du 29 juillet 1881. La Cour a pu estimer que l'interdiction « *n'est pas limitée à la révélation des nom et prénom des personnes concernées mais s'applique à la diffusion d'informations qui en permettent l'identification* »¹⁰.

D'autre part, en séance publique à l'occasion de l'adoption de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, le Sénat a adopté un amendement du

8. CONTE, Philippe. Note sous Crim., 12 décembre 2017, n° 17-80.818 et n° 17-80.821, Droit pénal, mars 2018, comm. 46, p. 33.

9. « *Le fait de révéler, par quelque moyen d'expression que ce soit, l'identité des fonctionnaires de la police nationale, de militaires, de personnels civils du ministère de la défense ou d'agents des douanes appartenant à des services ou unités désignés par arrêté du ministre intéressé et dont les missions exigent, pour des raisons de sécurité, le respect de l'anonymat, est puni d'une amende de 15 000 euros* ».

10. Crim., 12 décembre 2017, n° 17-80.818 et n° 17-80.821.

Police administrative

Gouvernement garantissant l'anonymat des officiers de police judiciaire procédant aux visites domiciliaires, ce que la commission de l'Assemblée nationale a étendu à tous les agents en charge des visites.

7. Au cours des deux décennies écoulées, le législateur a sensiblement renforcé la possibilité de recourir à l'anonymat des policiers et des gendarmes dans le cadre de leur mission de police judiciaire.

D'abord, la loi du 23 janvier 2006 relative à la lutte contre le terrorisme¹¹ a permis au procureur général près la Cour d'appel de Paris d'autoriser nominativement les officiers et agents de police judiciaire, affectés dans les services de police judiciaire spécialement chargés de la lutte contre le terrorisme, à procéder aux investigations relatives aux infractions liées aux actes de terrorisme, « *en s'identifiant par leur numéro d'immatriculation administrative* »¹².

Ensuite, cette disposition a été étendue par la loi du 28 février 2017 relative à la sécurité publique¹³. L'article 15-4 du Code de procédure pénale dispose en effet que les agents de la police nationale et de la gendarmerie nationale peuvent être autorisés à ne pas être identifiés par leurs noms et prénoms lorsque la révélation de leur identité est susceptible de mettre en danger leur vie ou leur

11. Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

12. Article 706-24 du Code de procédure pénale.

13. Loi n° 2017-258 du 28 février 2017 relative à la sécurité publique.

Police administrative

intégrité physique, ou celles de leurs proches dans les actes de procédure judiciaire :

- portant sur un crime ou un délit puni d'au moins trois ans d'emprisonnement compte tenu des conditions d'exercice de sa mission ou de la nature des faits qu'ils sont habituellement amenés à constater ;
- portant sur un délit puni de moins de trois ans d'emprisonnement, en raison de circonstances particulières dans la commission des faits ou de la personnalité des personnes mises en cause.

Enfin, depuis la loi du 23 mars 2019¹⁴, les officiers ou agents de police judiciaire peuvent s'identifier par leur numéro d'immatriculation administrative lorsqu'ils reçoivent une plainte.

8. Les policiers et les gendarmes ne sont pas les seuls agents à pouvoir bénéficier de l'anonymat. Ainsi, selon l'article 55 *bis* du Code des douanes, les agents des douanes peuvent être autorisés par leur responsable hiérarchique à ne pas être identifiés par leurs noms et prénoms mais à utiliser le numéro de leur commission d'emploi, leur qualité et leur service ou leur unité d'affectation à l'occasion de la mise en œuvre de leurs pouvoirs de recherche, de constatation et de poursuite ou lorsqu'ils sont requis sur le fondement du Code de procédure pénale. De même, afin de préserver l'anonymat des agents de l'administration fiscale lorsque les circonstances de la

¹⁴. Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice dont l'article 42 modifie l'article 15-3 du Code de procédure pénale.

Police administrative

procédure le justifient, la loi de finances pour 2020 a prévu la possibilité de recourir à un numéro d'immatriculation administrative¹⁵. Ainsi, « *dans le cadre des procédures de contrôle, de recouvrement et de contentieux (...), tout agent des finances publiques peut être autorisé à ne pas être identifié par ses nom et prénom lorsque, compte tenu des conditions d'exercice de sa mission et des circonstances particulières de la procédure, la révélation de son identité à une personne déterminée est susceptible de mettre en danger sa vie ou son intégrité physique ou celles de ses proches* »¹⁶. Le recours à un numéro d'immatriculation en lieu et place des noms et prénoms de l'agent, doit être autorisé nominativement par le directeur du service déconcentré ou du service à compétence nationale dans lequel l'agent est affecté.

9. En mars 2022, le député Jean-Louis Theriot a déposé une proposition de loi visant à protéger les forces de l'ordre par une systématisation de leur anonymat dans les actes de procédure judiciaire¹⁷. Elle prévoyait que, dans l'exercice de leurs fonctions judiciaires, les officiers et agents de la police nationale et de la gendarmerie nationale soient identifiés par leur numéro d'immatriculation administrative. En contrepartie, l'identification

15. Loi n° 2019-1479 du 28 décembre 2019 de finances pour 2020, art. 174.

16. Article L. 286B du Livre des procédures fiscales.

17. Proposition de loi n° 5167 déposée par visant à protéger les forces de l'ordre par une systématisation de leur anonymat dans les actes de procédure judiciaire, déposée le mardi 15 mars 2022.

Police administrative

des policiers et des gendarmes serait garantie grâce à l'interface de levée de l'anonymat des agents de la police et de la gendarmerie nationales et des douanes dans les actes de procédure (IDPV) mise en place pour « *identifier un agent apparaissant dans un acte de procédure sous un numéro d'immatriculation administrative* »¹⁸. Si cette loi n'a pas encore prospéré, elle constitue une piste de réflexion dans l'apaisement des inquiétudes des agents de la force publique et dans l'objectif de protection de forces de police et de gendarmerie qui « *sont, par la nature de leur mission, structurellement exposées à des risques de rancœur de la part des personnes qu'elles ont vocation à contrarier* »¹⁹.

18. Article 1^{er} alinéa 2 de l'arrêté du 30 mars 2018 portant création d'un traitement de données à caractère personnel dénommé « *interface de levée de l'anonymat des agents de la police et de la gendarmerie nationales et des douanes dans les actes de procédure* » (IDPV).

19. Conclusions de Mme Aurélie BRETONNEAU sous CE, 15 décembre 2017, *Ministère de l'Intérieur c/ B...*, n° 405845, Rec., p. 613. Disponible sur : <https://www.conseil-etat.fr/fr/arianeweb/CRP/conclusion/2017-12-15/405845?>

Actualité institutionnelle européenne

Pierre BERTHELET

L'Europe de la sécurité intérieure

Synthèse législative et institutionnelle (été 2024 - hiver 2024)

L'Europe de la sécurité intérieure entre dans une période de transition. Pas de nouvelles propositions législatives de grande ampleur (en raison notamment du processus de nomination de la nouvelle Commission). Ce sont surtout les normes de *soft law* qui dominent, en premier lieu les textes du Conseil de l'Union européenne, très prolifique ces derniers mois. Celles-ci reflètent **les grandes préoccupations du moment en matière de sécurité intérieure à l'échelle européenne** : terrorisme et extrémisme violent (1), lutte contre l'immigration clandestine (2) et renforcement des frontières Schengen (3), cybersécurité, nouvelles technologies et IA (4), lutte contre la cybercriminalité (5) et, enfin, l'approfondissement de la coopération policière et judiciaire (6) pour lutter en particulier contre la criminalité transnationale organisée.

1. Terrorisme et extrémisme violent

Dans son rapport sur l'état de la menace terroriste en Europe (TE-SAT 2024)¹, Europol recense 120 actes terroristes dans l'Union

¹. *Europol's annual EU Terrorism Situation and Trend Report (TE-SAT)*, 12 décembre 2024.

Actualité institutionnelle européenne

européenne (UE) en 2023. Parmi ces 120 attaques, 98 ont été exécutées avec succès, 9 ont échoué et 13 ont été contrecarrées. La majorité des attaques terroristes se sont déroulées en France (80) et en Italie (30).

Europol signale une augmentation par rapport à l'année 2022 (28 attentats) et à l'année 2021 (18 attentats). 426 individus ont été appréhendés pour des délits liés au terrorisme dans 22 États membres, ce chiffre représentant une hausse par rapport à 2022 (380) et 2021 (388). Plus de la moitié des arrestations ont été effectuées en Espagne (84), en France (78), en Belgique (75) et en Allemagne (51).

Surtout, la majorité des arrestations ont été réalisées dans le cadre de dossiers liés au terrorisme djihadiste (334), marquant une hausse notable par rapport à l'année précédente (266). À ce propos, Europol observe un « *pont idéologique* » entre les groupes d'extrême droite violente et la propagande djihadiste. L'attaque récente à Magdebourg semble illustrer les liens entre les différentes formes de terrorisme et un brouillage des distinctions entre les types de violence, ce qui confirme l'analyse du rapport de 2024. Ce dernier met en évidence **une convergence entre les groupes extrémistes de droite violents et les groupes djihadistes** au sens d'« *hybridation idéologique* », les djihadistes ayant une fascination pour l'accélérationnisme suprématisse.

Europol souligne par ailleurs le danger des « *revenants* », c'est-à-dire les combattants djihadistes partis au Moyen-Orient et souhaitant rentrer en Europe. Il s'inquiète en particulier du fait que certains d'entre eux peuvent utiliser **les flux migratoires illégaux pour rentrer plus facilement**.

Actualité institutionnelle européenne

À ce sujet, le Conseil de l'UE a approuvé, le 16 décembre 2024, des conclusions sur le renforcement des liens entre les aspects extérieurs et intérieurs de la lutte contre le terrorisme et l'extrémisme violent². Ce document vise principalement à développer davantage une approche globale et coordonnée de l'UE, en prenant en compte à la fois les dimensions nationales et internationales de cette menace. Le Conseil se déclare résolu à promouvoir les synergies et à prévenir les redondances. Le document propose des mesures concrètes, telles que l'accroissement de la coopération avec des pays tiers stratégiques, la promotion des échanges d'informations, le renforcement des capacités des États membres et la révision de la définition juridique des infractions terroristes.

Ces conclusions ont été approuvées peu après d'autres dressant les grandes orientations en vue d'une nouvelle stratégie de lutte contre le terrorisme pour les cinq prochaines années³. Divers aspects sont abordés par le Conseil de l'UE, tels que l'utilisation à des fins répressives des données des voyageurs empruntant les transports maritimes et terrestres, la prévention des liens entre la criminalité organisée et le terrorisme, la mise en place de mesures à l'encontre de fournisseurs de services en ligne non collaboratifs, y compris les grandes plateformes, ainsi que la détection de l'infiltration de terroristes dès les premières étapes de leur entrée dans l'Union.

2. Doc. du Conseil n° 16175/24, 16 décembre 2024.

3. Doc. du Conseil n° 16820/24, 12 décembre 2024.

Actualité institutionnelle européenne

Des solutions pratiques sont envisagées, notamment l'alignement des activités des pôles de connaissances de l'Union européenne (« *EU Knowledge Hub* »)⁴ sur les exigences politiques en matière de radicalisation, l'optimisation du cadre juridique pour permettre une procédure accélérée d'expulsion, ou encore une plus grande harmonisation de l'utilisation des « *indicateurs de sécurité* » du Système d'information Schengen (SIS).

En matière de messagerie financière, la Commission a publié, le 13 novembre 2024, un rapport sur l'application de l'accord UE-USA entré en vigueur le 1^{er} août 2010⁵. Selon elle, cet accord relatif au traitement et au transfert des données de messagerie financière de l'UE vers les États-Unis dans le cadre du programme de surveillance du financement du terrorisme (*Terrorist Finance Tracking Program*, ou TFTP) fonctionne bien. Il est efficace pour obtenir rapidement des informations précises et fiables. Il contribue ainsi à la détection et à la surveillance des terroristes ainsi que de leurs réseaux de soutien à l'échelle mondiale. En parallèle, les garanties prévues par l'accord en matière de protection de la vie privée sont préservées et la Commission se réjouit de la transparence dont font preuve les autorités américaines en matière de partage d'informations.

4. Voir BERTHELET, Pierre. Synthèse législative et institutionnelle (mai 2024 - août 2024). *La Veille juridique du CRGN*, n° 125, septembre 2024, p. 84-86. Disponible sur : <https://www.calameo.com/read/0027192922915f7c4706f>

5. COM(2024) 522 final.

Actualité institutionnelle européenne

2. Lutte contre l'immigration clandestine

Un plan d'action a été élaboré par la Commission au début de l'été, destiné à concrétiser le Pacte sur l'asile et la migration, qui a été approuvé par le Conseil de l'UE et par le Parlement européen en mai 2024⁶. Ce plan d'action comprend un calendrier et une feuille de route afin qu'un tel Pacte devienne opérationnel d'ici la mi-2026. Il définit dix composantes destinées à faciliter la mise en œuvre d'un cadre réglementaire particulièrement dense et complexe pour les États membres. Il établit le cadre d'un programme de travail collaboratif pour les deux années à venir, incluant les résultats juridiques et opérationnels, les mécanismes de dialogue, ainsi que le soutien opérationnel et financier approprié. Le plan adopte une approche pragmatique en mettant l'accent sur les éléments essentiels que les États membres doivent prendre en compte lors de l'élaboration de leurs plans nationaux de mise en œuvre.

Concernant l'instrumentalisation de la migration, une communication a été présentée le 11 novembre 2024⁷. Ce document décrit comme **menace hybride pour l'Union la manipulation des flux migratoires par la Russie et la Biélorussie** pour déstabiliser les frontières extérieures de l'UE et affaiblir l'unité européenne. Plusieurs mesures sont préconisées, notamment un contrôle renforcé des frontières, la possibilité pour les États membres

6. COM(2024) 251 final.

7. COM(2024) 570 final.

Actualité institutionnelle européenne

impactés de faire usage de mesures exceptionnelles en raison de la gravité et de la persistance de la menace, l'application du Pacte sur la migration et l'asile, en premier lieu le règlement relatif aux situations de crise et de force majeure, le renforcement de la lutte contre le trafic de migrants et de celle contre la désinformation, en utilisant les moyens offerts par le *Digital Services Act*, l'appui opérationnel des agences européennes (notamment Frontex et Europol) aux régions frontalières de l'Est de l'UE, ainsi que le soutien financier à leur profit par le biais de l'instrument de gestion des frontières et de la politique des visas (IGFV)⁸.

Par ailleurs, le Conseil de l'UE a approuvé le 12 décembre 2024 des conclusions visant à adopter **une approche plus rigoureuse en matière de visas**⁹. Diverses mesures sont actuellement envisagées : le renforcement du principe de réciprocité, l'intégration systématique de la lutte contre l'immigration dans les interactions avec les pays tiers partenaires, l'analyse des données statistiques pour repérer les pays tiers qui adoptent une attitude permissive, la consultation régulière de la base de données européenne sur les visas (VIS) et l'inclusion sur la liste blanche (dispense de visa) uniquement en cas de conduite exemplaire de ces pays tiers. Il est souligné par le Conseil la nécessité de prendre pleinement en considération les dimensions de la migration et de la sécurité intérieure dans le domaine de la politique étrangère. Celui-ci

8. Règlement (UE) 2021/1148.

9. Doc. du Conseil n° 16801/24, 12 décembre 2024.

Actualité institutionnelle européenne

souligne l'importance pour l'UE de mettre en place des mesures supplémentaires afin de limiter les opportunités de « *visa shopping* », en particulier à travers une coopération locale renforcée et mieux coordonnée dans le cadre de l'espace Schengen.

3. Frontières Schengen

Les représentants des États membres de l'UE sont convenus à l'unanimité d'abolir, à compter du 1^{er} janvier 2025, les contrôles de personnes aux frontières intérieures terrestres entre la Bulgarie et la Roumanie et le reste de l'espace Schengen, ainsi qu'entre ces deux pays. Une décision a été prise en ce sens par le Conseil de l'Union, le 11 décembre. Elle fait suite à une décision du 30 décembre 2023 visant à lever les restrictions aux frontières intérieures aériennes et maritimes en mars 2024.

Peu avant la tenue de ce Conseil, la Commission a présenté concomitamment, le 8 octobre 2024, deux propositions de règlement visant à assurer **une meilleure fluidité aux frontières extérieures de l'espace Schengen**. La première proposition présente de nouvelles dispositions qui autorisent les voyageurs à générer et à conserver leurs données d'identification de voyage sous forme numérique¹⁰. Les données des passeports et des cartes d'identité sont converties en format numérique dans le cadre de la

¹⁰. COM(2024)671 final.

Actualité institutionnelle européenne

création des authentifiants de voyage numériques (*Digital Travel Credentials*, ou DTC). L'initiative entend ainsi garantir une traversée plus efficace des frontières pour les citoyens de l'Union en utilisant les DTC, ce qui permet d'éviter les longs contrôles manuels.

La standardisation prévue par cette proposition vise à assurer que tous les citoyens ont accès à des systèmes numériques fiables et compatibles, ce qui permet d'éviter la fragmentation des solutions au niveau national.

La deuxième proposition, complémentaire à la première, entend établir une application appelée *EU Digital Travel*¹¹. Cette application, qui consiste à **pré-enregistrer les données de voyage sous forme numérique**, permettra à ses détenteurs de soumettre préalablement leurs documents de voyage aux garde-frontières. Il est prévu que le système soit pleinement opérationnel d'ici l'année 2030.

Une autre proposition de règlement a été soumise par la Commission le 4 décembre 2024, portant pour sa part sur l'entrée en fonction du Système d'Entrée/Sortie (EES) qui est un système européen automatisé destiné à enregistrer les entrées et les sorties des ressortissants de pays tiers aux frontières de l'UE¹². L'objectif de cette proposition est d'assurer un déploiement progressif des activités de ce système à grande échelle visant à identifier et à

¹¹. COM(2024) 671 final.

¹². COM(2024) 567 final.

Actualité institutionnelle européenne

recenser à l'échelle de l'UE les passagers se présentant aux points de passage. Le constat est, qu'à l'heure actuelle, tous les États membres ne sont pas encore prêts. Dès lors, la proposition entend leur accorder **une certaine flexibilité pour initier l'utilisation de l'EES** en fonction de leur degré de préparation, ainsi que pour faciliter les ajustements techniques et opérationnels lors du lancement de l'exploitation de ce système.

4. Cybersécurité, IA et sécurité intérieure

Le Conseil de l'UE a approuvé, le 6 décembre 2024, des conclusions dans lesquelles il reconnaît que **l'Agence de l'Union européenne pour la cybersécurité (ENISA)** joue un rôle crucial dans l'écosystème de cybersécurité de l'UE¹³. Toutefois, il note en parallèle que son efficacité doit être renforcée par une meilleure définition de son mandat, une allocation adéquate de ressources, et une coopération accrue avec les autres acteurs. Il préconise dès lors une réforme de son mandat, notamment rationalisant les tâches qui lui sont attribuées, eu égard au fait que les responsabilités de l'ENISA ont été considérablement élargies par des initiatives législatives récentes, comme le règlement sur la cyberrésilience, le règlement sur la cybersolidarité et la directive SRI 2.

À propos de la directive SRI 2¹⁴, un règlement d'application a récemment été adopté. Ce document donne un ensemble de

¹³. Doc. du Conseil n° 16527/24, 6 décembre 2024.

¹⁴. Directive (UE) 2022/2555.

Actualité institutionnelle européenne

précisions pour la gestion des risques, les protocoles de gestion des incidents et les exigences de notification.

Concernant l'intelligence artificielle (IA), le Conseil de l'UE a approuvé, le 13 décembre 2024, des conclusions dans lesquelles il estime que cette technologie a un potentiel important pour transformer le domaine de la justice¹⁵. L'IA peut améliorer l'efficacité, l'efficience et l'accessibilité des procédures judiciaires en automatisant certaines tâches courantes, en facilitant l'analyse de la jurisprudence, en aidant à la prise de décision et en offrant des services tels que l'interprétation en temps réel.

Toutefois, le Conseil considère que son utilisation doit être encadrée par des garanties pour respecter les droits fondamentaux et les principes éthiques. S'il estime que l'IA peut assister les professionnels de la justice, elle ne doit pas remplacer le rôle humain dans la prise de décision finale. Aussi le texte souligne-t-il l'importance du règlement sur l'IA (*IA Act*)¹⁶, qui classe certains systèmes d'IA utilisés dans le domaine de la justice comme étant à haut risque. Le texte met en évidence l'importance de la transparence, de la responsabilité, de la surveillance et de la fiabilité des systèmes d'IA. Il insiste, en outre, sur la nécessité de former les praticiens du droit et le personnel administratif à l'utilisation de l'IA, afin de réduire les déficits de compétences numériques et de renforcer la sensibilisation aux risques associés à

¹⁵. Doc. du Conseil n° 16933/24, 16 décembre 2024.

¹⁶. Règlement (UE) 2024/1689.

Actualité institutionnelle européenne

ces technologies.

De son côté, Europol a adopté **un rapport sur l'utilisation de l'IA par les forces de police**¹⁷. Le rapport explore plusieurs applications de l'IA dans le domaine de la police : l'analyse de données, le renseignement de sources ouvertes (Open Source Intelligence, ou OSINT), le traitement du langage naturel, la criminalistique numérique, la vision par ordinateur, la biométrie et l'IA générative. L'IA peut être utilisée pour l'analyse de données complexes, la surveillance vidéo, la reconnaissance faciale, la détection d'anomalies, la traduction linguistique et l'allocation de ressources. Toutefois, son utilisation doit être encadrée par des considérations éthiques, ainsi que par un engagement en faveur de la transparence, de la responsabilité et de la protection des droits fondamentaux.

5. Lutte contre la cybercriminalité

Dans le rapport sur la situation de la cybercriminalité en Europe pour l'année 2024 (IOCTA 2024), Europol insiste sur **la menace croissante que représente la cybercriminalité**¹⁸. Il souligne la progression continue et la complexification grandissante de ce phénomène. Les principales menaces mises en évidence dans le

¹⁷. EUROPOL. *AI and policing*, 23 septembre 2024.

¹⁸. EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA) 2024*, 26 juillet 2024.

Actualité institutionnelle européenne

rapport, telles que les attaques de rançonnement, l'exploitation sexuelle des enfants en ligne, la fraude en ligne et les paiements, sont toutes liées par des éléments communs, tels que le trafic illicite de données personnelles, l'utilisation de cryptomonnaies et le *dark web*.

En outre, la montée en puissance de l'utilisation de l'IA par les cybercriminels suscite une inquiétude particulière, car elle offre de nouvelles opportunités pour lancer des attaques plus complexes et plus insidieuses.

En parallèle, Europol souligne le fait que **le « Home Routing » pose un défi majeur à l'interception légale par les forces de police¹⁹**. Cette technologie consiste pour les fournisseurs de services de télécommunications à continuer à fournir des services à leurs clients lorsqu'ils voyagent à l'étranger, en acheminant leurs communications *via* leur réseau domestique plutôt que celui du pays visité. Toutefois, une telle technologie complique l'interception légale car les données des communications sont traitées par le réseau domestique du client, et non par celui du pays visité. Les forces de police sont dépendantes du niveau de coopération des fournisseurs de services du pays d'origine de la communication. Qui plus est, les demandes d'entraide judiciaire peuvent prendre jusqu'à 120 jours, ce qui est trop long pour les interceptions d'urgence. Le thème de l'interception des communications a fait l'objet d'un

¹⁹. EUROPOL. *Position paper: Home routing and risks to lawful interception*, 4 juillet 2024.

Actualité institutionnelle européenne

important rapport d'un groupe d'experts, dénommé Groupe de Haut niveau²⁰. Ce rapport souligne l'importance d'établir un cadre juridique européen harmonisé pour garantir un accès légal aux données. L'accent est placé sur la collaboration entre les États membres, les institutions de l'UE et les prestataires de services de communication, dans le but d'établir un équilibre entre la sécurité et la sauvegarde de la protection des données. Il préconise également la mise en place **d'un dispositif de sanctions dissuasives à l'égard des fournisseurs qui refusent de coopérer** avec les autorités, notamment en ce qui concerne la conservation et la communication des données.

Dans des conclusions approuvées en décembre 2024, le Conseil de l'UE invite la Commission à élaborer, avant le deuxième trimestre de 2025, un plan d'action détaillé pour la mise en place de mesures appropriées, incluant des dispositions législatives.

6. Coopération policière et judiciaire pénale

Le Conseil de l'UE a approuvé, le 10 octobre 2024, des conclusions dans lesquelles il considère que, bien que la criminalité environnementale soit une priorité de l'UE dans la lutte contre la grande criminalité organisée, elle ne bénéficie pas du même degré

²⁰. *Concluding report of the High-Level Group on access to data for effective law enforcement*, 15 novembre 2024. Disponible sur : https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en?filename=Concluding%20Report%20of%20the%20HLG%20on%20access%20to%20data

Actualité institutionnelle européenne

d'engagement de la part de toutes les parties prenantes par rapport à d'autres domaines criminels prioritaires²¹. Ces conclusions énumèrent ainsi un ensemble de mesures à mettre en place. Figurent parmi celles-ci, le fait d'encourager la formation et le développement de compétences spécialisées, de favoriser l'emploi du *European Multidisciplinary Platform Against Criminal Threats* (EMPACT), de renforcer la lutte contre le financement criminel et de s'appuyer sur la société civile. Enfin, elles suggèrent de stimuler les réseaux existants, tels que IMPEL, REPE, EUFJE et EnviCrimeNet. Surtout, elles préconisent de s'inspirer, en tant que bonnes pratiques existant au niveau national, du **Commandement pour l'environnement et la santé (CESAN) de la Gendarmerie**.

Quant au collège européen de police, il a présenté son rapport annuel d'activité pour l'année 2024²². Il dresse une évaluation globalement positive de l'agence en dépit de défis significatifs, comme la gestion des ressources et l'accès à certains publics cibles. Il mentionne des réussites opérationnelles, en particulier une participation importante aux sessions de formation et une satisfaction élevée parmi les participants. Les formations les plus prisées ont trait aux thèmes relatifs à la criminalité grave et organisée, à la cybercriminalité, à la criminalité en col blanc, aux droits fondamentaux et à la protection des données, ainsi qu'à la

21. Doc. du Conseil n° 14182/24, 10 octobre 2024.

22. CEPOL. *Consolidated Annual Activity Report*, 9 septembre 2024. Disponible sur : <https://www.cepola.europa.eu/publications/consolidated-annual-activity-report>

Actualité institutionnelle européenne

lutte contre le terrorisme.

Pour ce qui est de la dixième série d'évaluations mutuelles, elle s'est concentrée sur la mise en œuvre de la directive du 3 avril 2014 concernant la décision d'enquête européenne (DEE)²³. Un rapport final a été publié, permettant d'identifier des points forts, des défis et des recommandations pour améliorer son application²⁴. L'évaluation a reconnu que la DEE est un instrument précieux pour la coopération judiciaire en matière pénale. Certains États membres ont mis en place des pratiques efficaces, comme la désignation d'une autorité chargée de coordonner l'exécution des DEE et la possibilité pour les victimes d'introduire des demandes de collecte de preuves. En revanche, plusieurs défis ont été identifiés dans la mise en œuvre de la DEE, comme le fait que **de nombreuses décisions d'enquête sont incomplètes, imprécises ou incohérentes**. Des problèmes de traduction et des difficultés à comprendre les faits et les mesures demandées sont aussi signalés. De surcroît, des divergences existent entre les États membres concernant les modalités de transmission de la DEE, notamment leur acceptation par voie électronique. Enfin, des divergences sont à noter quant à l'utilisation de la visioconférence pour entendre les personnes poursuivies durant les procédures judiciaires.

Le rapport contient dès lors plusieurs recommandations, comme

²³. Directive 2014/41/UE.

²⁴. Doc. du Conseil n° 15834/1/24, 10 décembre 2024.

Actualité institutionnelle européenne

améliorer la formation des praticiens, notamment les compétences linguistiques, et étudier la possibilité de publier un manuel ou des lignes directrices sur son application.

Rédacteurs

- **Le Général d'armée (2S) Marc Watin-Augouard** est ancien directeur du CRGN et fondateur du FIC (ex- Forum international de la cybersécurité, aujourd'hui Forum InCyber)
- **Marc-Antoine Granger** est maître de conférences HDR en droit public à l'Université Côte d'Azur, directeur des études de la licence de droit, membre du Centre d'Etudes et de Recherche en Droit Administratif, Constitutionnel, Financier et Fiscal (CERDACFF) et du conseil d'administration de l'Association française de droit de la sécurité et de la défense (AFDSD)
- **Jérôme Millet** est administrateur de l'État, docteur en droit, membre du conseil d'administration de l'Association française de droit de la sécurité et de la défense (AFDSD)
- **Nathan Allix** est docteur en droit privé, maître de conférences à l'Université Paris-Est Créteil (Paris XII)
- **Sandrine Richard** est ancien avocat au Barreau de Paris, expert en intelligence économique, en éthique des affaires (dont l'éthique de l'IA) et *Advisory Board*, lieutenant-colonel de la réserve citoyenne, membre de la Chaire Humanités Numériques du CRGN
- **Pierre Berthelet** est docteur en droit, chercheur associé à l'Université de Grenoble (UGA-CESICE), à l'Université d'Aix-Marseille (CERIC) et au CRGN

Directeur de publication :

Colonel David BIÈVRE

Rédacteur en chef :

G^{al} d'armée (2S) Marc WATIN-AUGOUARD

Équipe éditoriale :

Odile NETZER

Le CRGN n'entend donner aucune approbation ni improbation aux opinions émises dans les articles. Ces opinions doivent être considérées comme propres à leurs auteurs.