

LA VEILLE JURIDIQUE

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

N° 134

Septembre 2025

EDITO

L'actualité en cette rentrée est bien chargée, tant sur le plan national qu'à l'échelle internationale. Chargée et difficile à déchiffrer, tant les règles qui régissaient notre collectif semblent fragilisées, ce qui contribue à l'incertitude. Depuis deux semaines, la France est sans gouvernement, avec des ministres démissionnaires qui expédient les affaires courantes, tandis que le Premier ministre est aussi ministre démissionnaire. Beau sujet de droit constitutionnel s'agissant des compétences qui lui sont propres et celles qu'il exerce au nom d'un gouvernement démissionnaire. Le 23 septembre, le Président de la République a reconnu l'État palestinien, s'inscrivant dans la « Déclaration de New York » du 12 septembre soutenue par 142 des 193 membres de

(Suite page 2)



CREOGN
CENTRE DE RECHERCHE
DE L'ECOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Edito

l'ONU. Mais le droit international public considère qu'un État doit posséder une autorité souveraine sur un territoire où vit une population permanente avec un gouvernement capable d'agir en interne et d'établir des relations avec des États tiers. Là encore, passé le discours, se pose la question de savoir si tous ces éléments sont réunis, s'agissant de la capacité de l'Autorité palestinienne à se libérer du Hamas, entrave à toute solution pacifique. S'il existe, désormais, un État palestinien, celui-ci doit être capable d'obtenir la libération des otages, faute de quoi le critère d'autorité sur un territoire n'est plus respecté. C'est sans doute dans les situations les plus complexes que le droit est mobilisé pour trouver les solutions, notamment pour éviter ou sortir du chaos. Là encore s'ouvre un champ inédit pour le juriste.

L'actualité juridique est plus « paisible » dans d'autres domaines. Le projet de loi transposant trois directives européennes (REC¹, NIS 2² et DORA³) semble progresser, près d'un an après sa présentation en Conseil des ministres et après avoir été adopté, en mars dernier, par le Sénat. Le 10 septembre 2025, le projet de loi Résilience a franchi une nouvelle étape, avec le vote en commission spéciale de l'Assemblée nationale. Il faut désormais espérer une promulgation avant la fin de l'année, la France ayant pris plus d'un an de retard dans la procédure de transposition. Dans le domaine de la

1. Directive sur la résilience des entités critiques.

2. Sécurité des réseaux et des systèmes d'Information.

3. *Digital Operational Resilience Act* : Règlement européen 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier.

Edito

cybersécurité, un événement met à l'honneur le CRGN puisque, le 16 octobre prochain, sortira la 3^e édition papier du Code de la cybersécurité (éditions Dalloz) qui est corédigé avec notamment des personnels actifs ou associés du Centre. Ce document augmente en volume chaque année, tant la matière s'enrichit avec le droit national et européen. L'implication de notre Centre de recherche, dès sa conception d'origine, souligne la reconnaissance de son expertise.

Bonne lecture de *La Veille juridique* !

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

L'enregistrement des plaintes : une obligation à inscrire dans le Code de déontologie de la police et de la gendarmerie nationales [6](#)

Droit de l'espace numérique

L'usage de l'intelligence artificielle dans le maintien de l'ordre : enjeux juridiques, dérives éthiques et encadrement nécessaire..... [15](#)

Discours du GAR (2S) Marc Watin-Augouard prononcé lors du colloque « Raviver le lien Armée - Nation autour de l'innovation technologique »..... [37](#)

Actualité pénale

La loi du 9 juillet 2025 créant l'homicide routier et visant à lutter contre la violence routière [62](#)

Police administrative

Un simple tableau transmis à la préfecture mais sans base légale constitue un traitement illicite..... [77](#)

Droit des collectivités territoriales et de la sécurité privée

Le cas des rodéos urbains motorisés en question : lorsque le maire supplée à l'impéritie publique..... [86](#)

Actualité institutionnelle européenne

L'Europe de la sécurité intérieure. Synthèse législative et institutionnelle (printemps - été 2025).....[101](#)

Marc-Antoine GRANGER

L'enregistrement des plaintes : une obligation à inscrire dans le Code de déontologie de la police et de la gendarmerie nationales

À l'évidence, il n'y a point de droit pénal sans victime¹. Dès lors, il n'est pas surprenant que la garantie des droits de cette dernière – définie comme celle qui a « *personnellement souffert du dommage directement causé par l'infraction* »² – constitue l'un des principes cardinaux de la procédure pénale, comme l'affirme l'article préliminaire du Code de procédure pénale (CPP)³. En dérivation de la loi pénale, le Code de déontologie de la police et de la gendarmerie nationales impose aux policiers et gendarmes nationaux d'accorder « *une attention particulière aux victimes* » et de veiller « *à la qualité de leur prise en charge tout au long de la procédure les concernant* »⁴. La qualité de cette prise en charge, notamment au moment de l'enregistrement des plaintes, contribue assurément à renforcer la nécessaire relation de confiance entre la population et

1. Voir, par exemple, BEAUSSONIE, Guillaume. La légitimité de la victime de l'infraction. In : RIBEYRE, Cédric. *La victime de l'infraction pénale*. Dalloz, coll. thèmes et commentaires, 2016, Paris, p. 49-57.

2. Article 2, alinéa 1^{er}, du Code de procédure pénale (CPP).

3. Selon le paragraphe II de l'article préliminaire du CPP, « *l'autorité judiciaire veille à l'information et à la garantie des droits des victimes au cours de toute procédure pénale* ».

4. Article R. 434-20 du Code de la sécurité intérieure (CSI).

Déontologie et sécurité

les forces publiques de sécurité intérieure⁵. C'est d'ailleurs pourquoi le législateur lui-même s'est fixé pour objectif d'améliorer « *le parcours des victimes (...) avec un traitement plus efficace et transparent des plaintes* »⁶. En guise d'illustration, les dispositions de l'article 12 de la Loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur (LOPMI) ont autorisé le dépôt de plainte par un moyen de télécommunication audiovisuelle⁷. Au demeurant, le Conseil constitutionnel a validé ces dispositions dans la mesure où le recours à la technologie se présente comme une simple option pour la victime et n'interdit jamais aux enquêteurs de procéder à une nouvelle audition classique, sans emploi du numérique⁸.

En pratique toutefois, le Défenseur des droits – autorité administrative indépendante⁹ participant à la protection non

5. Sur cette nécessaire relation de confiance, voir, par exemple, CE, Ass., 11 octobre 2023, *Amnesty international France et autres*, n° 454836, § 11. Pour un commentaire de cette décision, voir : GRANGER, Marc-Antoine. La pratique des contrôles d'identité au faciès devant le Conseil d'État. Note sous CE, Ass., 11 octobre 2023, *Amnesty international France et autres*, n° 454836. [La Veille juridique du CREOGN, novembre 2023, n° 118, p. 5-15.](#)

6. Point 2 du rapport sur la modernisation du ministère de l'Intérieur, annexé à la Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur (LOPMI).

7. Il s'agit de l'article 15-3-1-1 du CPP inséré par le 1° de l'article 12 de la LOPMI. Parallèlement, le décret n° 2024-139 du 23 février 2024 définit les modalités d'application de cet article 15-3-1-1 (voir les articles R. 2-25 à R. 2-29 du CPP).

8. Cons. const., décision n° 2022-846 DC du 19 janvier 2023, LOPMI, § 51.

9. Article 2 de la loi organique n° 2011-333 du 29 mars 2011 relative au Défenseur des droits.

Déontologie et sécurité

juridictionnelle des droits et libertés¹⁰ – est régulièrement saisi de réclamations liées à des refus d'enregistrement de plaintes. Il peut s'agir d'un « refus sec », ou d'un « refus déguisé » lorsque le policier rédige une main courante ou le gendarme un PV de renseignement judiciaire en lieu et place d'une plainte, alors même qu'elle constitue une simple mesure d'information ne donnant lieu – en principe – ni à enquête ni à transmission au Parquet. Cela étant précisé, dans son rapport annuel d'activité pour l'année 2024, le Défenseur des droits indique que « *les refus de plaintes allégués représentent cette année encore 8 % des réclamations traitées dans le domaine de la déontologie de la sécurité* »¹¹, sachant que, depuis 2022, ces réclamations sont tout de même en diminution¹². On peut aussi y lire que « *les difficultés rencontrées par les plaignants perdurent, notamment lorsque l'enregistrement de la plainte est soumis à une condition qui ne devrait pas s'appliquer* »¹³. Tel est le cas, par exemple, du gardien de la paix qui subordonne l'enregistrement de la plainte à la présentation de documents d'identité et à la

10. Le premier alinéa de l'article 71-1 de la Constitution de 1958 prévoit que « *le Défenseur des droits veille au respect des droits et libertés par les administrations de l'État, les collectivités territoriales, les établissements publics, ainsi que par tout organisme investi d'une mission de service public, ou à l'égard duquel la loi organique lui attribue des compétences* ».

11. DÉFENSEUR DES DROITS. *Rapport annuel d'activité 2024*, p. 81.

12. En 2022 et 2023, les refus de plaintes allégués représentaient respectivement 10 % et 9 % des réclamations traitées dans le domaine de la déontologie de la sécurité : DÉFENSEUR DES DROITS. *Rapport annuel d'activité 2022*, p. 83, et *Rapport annuel d'activité 2023*, p. 13.

13. DÉFENSEUR DES DROITS, *op. cit.* note 11, p. 81.

Déontologie et sécurité

justification d'une situation administrative régulière¹⁴. Par ailleurs, les refus de prise de plaintes figurent parmi les principaux signalements portés à la connaissance de l'Inspection générale de la gendarmerie nationale¹⁵ (IGGN) et de l'Inspection générale de la police nationale¹⁶ (IGPN). En 2023, ce sont ainsi 192 signalements qui ont été enregistrés par l'IGGN. Il reste que, la même année, seuls sept refus de prise de plaintes avérés ont été recensés par l'IGGN¹⁷.

Ces considérations liminaires illustrent combien la pratique du refus d'enregistrement des plaintes, bien qu'elle ne soit ni généralisée ni systématique, nuit à la crédibilité des institutions policière et « gendarmique », et porte atteinte à la protection effective des droits des victimes. À cet égard, il nous paraît utile de procéder à une réécriture du Code de déontologie de la police et de la gendarmerie nationales destinée à inscrire en toutes lettres l'obligation d'enregistrement des plaintes. Cette proposition part du constat suivant : si aucune interdiction explicite de refuser une plainte n'est aujourd'hui formulée dans le Code de déontologie (I), un tel refus constitue pourtant un manquement susceptible d'être

¹⁴. DÉFENSEUR DES DROITS. Décision n° 2024-150 du 22 octobre 2024. Dans cette affaire, le Défenseur des droits a recommandé au ministre de l'Intérieur d'adopter « une instruction générale visant à rappeler le cadre légal en matière du dépôt de plainte et d'accueil des victimes, et notamment le droit de toute personne de déposer plainte à l'unique condition que les faits dénoncés soient réprimés pénalement, indépendamment de la nationalité ou de la situation administrative des plaignants ainsi que le droit à bénéficier d'un interprète ».

¹⁵. IGGN. *Rapport annuel d'activité 2023*, p. 57.

¹⁶. IGPN. *Rapport annuel d'activité 2023*, p. 118.

¹⁷. IGGN, *op. cit.* note 15, p. 57.

Déontologie et sécurité

sanctionné disciplinairement (II).

I) L'obligation d'enregistrer une plainte : une exigence absente du Code de déontologie

Dans le Code de déontologie de la police et de la gendarmerie nationales, intégré aux articles R. 434-1 à R. 434-33 du Code de la sécurité intérieure (CSI), l'obligation d'enregistrement des plaintes est introuvable. Tout au plus, elle se profile en filigrane de certaines dispositions du Code et, en particulier, de celles des articles R. 434-2 et R. 434-20 du CSI.

En premier lieu, en écho aux dispositions des articles L. 411-1 et L. 421-2 du CSI, le premier alinéa de l'article R. 434-2 rappelle que la police et la gendarmerie nationales exercent leurs « *missions de sécurité intérieure* » sous l'autorité du ministre de l'Intérieur, et agissent « *dans le respect des règles du code de procédure pénale en matière judiciaire* ». Disons-le sans détour, ce renvoi aux règles du CPP est fondamental : il garantit à sa manière que la force publique agisse toujours pour « *l'avantage de tous* »¹⁸, c'est-à-dire ici au service de la justice, la police judiciaire étant l'antichambre de la répression pénale. En outre, ce renvoi emporte de nombreuses conséquences juridiques et, avant tout, il implique que la police judiciaire demeure constamment sous la direction et le contrôle de l'autorité judiciaire¹⁹. Surtout, pour ce qui nous intéresse dans le

¹⁸. Cette formule est consacrée par l'article 12 de la Déclaration des droits de l'Homme et du citoyen du 26 août 1789.

¹⁹. Il s'agit là d'une exigence légale prévue par le CPP, mais aussi d'une exigence

Déontologie et sécurité

cadre de ces lignes, ce renvoi signifie que les policiers et gendarmes nationaux doivent se conformer aux dispositions de l'article 15-3 du CPP, qui posent l'obligation de prendre les plaintes. Le premier alinéa de cet article est ainsi rédigé : « *Les officiers et agents de police judiciaire sont tenus de recevoir les plaintes déposées par les victimes d'infractions à la loi pénale, y compris lorsque ces plaintes sont déposées dans un service ou une unité de police judiciaire territorialement incompétents. Dans ce cas, la plainte est, s'il y a lieu, transmise au service ou à l'unité territorialement compétents* ».

En second lieu, l'obligation de prendre les plaintes laisse planer son aura sur les dispositions précitées de l'article R. 434-20, qui exigent des policiers et gendarmes nationaux une prise en charge qualitative des victimes. Ce rattachement de l'obligation étudiée à l'article R. 434-20 est, notamment, visible à la lecture de la version commentée du Code de déontologie, diffusée par le ministère de l'Intérieur à l'ensemble de son personnel. En effet, selon le commentaire de l'article R. 434-20 du CSI, « *la première obligation du policier ou du gendarme est de prendre les plaintes en vertu de*

constitutionnelle consacrée de façon prétorienne par le Conseil constitutionnel. Pour quelques développements à ce sujet, voir, notamment : GRANGER Marc-Antoine. Constitution et sécurité intérieure. Essai de modélisation juridique, prix de thèse du Conseil constitutionnel, LGDJ, Bibliothèque constitutionnelle et de science politique, tome 138, 2011, Paris, p. 245 et s., et GRANGER, Marc-Antoine. La sécurité publique sous contrôle juridictionnel : polices et autorité judiciaire dans la jurisprudence constitutionnelle depuis la décision Fouille des véhicules de 1977. In : *Annuaire du droit de la sécurité et de la défense*, vol. 7, Mare & Martin, 2022, p. 41-51.

Déontologie et sécurité

l'article 15-3 du code de procédure pénale. Dans l'hypothèse où le fait dénoncé ne constitue pas une infraction pénale, la victime doit être orientée vers d'autres administrations ou structures idoines »²⁰.

II) Le refus d'enregistrer une plainte : un manquement sanctionné disciplinairement

Malgré l'absence de formalisation expresse de l'obligation de prendre les plaintes dans le Code de déontologie, tout manquement en la matière constitue une faute susceptible d'être sanctionnée disciplinairement. Tel est précisément l'apport de la jurisprudence administrative. En ce sens, deux décisions méritent plus particulièrement d'être citées.

D'une part, il s'agit d'un arrêt rendu le 19 octobre 2007 par le Conseil d'État. Les faits de l'espèce sont simples : le 27 décembre 1997, un commandant de la police nationale, qui se trouvait sur le point de terminer son service, a refusé d'enregistrer la plainte que voulait déposer le père d'une enfant de trois ans, lequel venait d'être victime d'une agression lors de l'exercice d'un droit de visite et d'hébergement de celle-ci. Par ailleurs, cet officier n'a donné aucune suite à l'interpellation qui avait été faite de trois personnes à cette occasion. Sans même mentionner les dispositions juridiques applicables – ce qui est regrettable –, le Conseil d'État juge que « ce comportement constituait une faute de nature à justifier le prononcé

²⁰. MINISTÈRE DE L'INTÉRIEUR. *Code de déontologie de la police nationale et de la gendarmerie nationale*, p. 20.

Déontologie et sécurité

d'une sanction disciplinaire »²¹.

D'autre part, à propos d'une sanction infligée à un chef de patrouille de la gendarmerie nationale ayant refusé de recevoir des plaintes déposées par les victimes d'infractions pénales, la cour administrative d'appel de Versailles considère, dans un arrêt du 16 novembre 2017, que ces faits caractérisent un manquement susceptible de justifier une sanction disciplinaire, l'intéressé ayant méconnu « *ses obligations d'officier de police judiciaire chargé de constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs (...), ainsi que de recevoir les plaintes déposées par les victimes d'infractions »²².*

Pour être complet, précisons que le choix de la sanction disciplinaire infligée aux officiers de police judiciaire (OPJ) et agents de police judiciaire (APJ) de la police et de la gendarmerie nationales refusant de prendre une plainte obéit à une appréciation nécessairement très casuistique de la part de l'autorité disciplinaire, qui prendra en compte, notamment, le caractère isolé ou non des manquements, ainsi que les éventuelles responsabilités de l'agent. En toute hypothèse, il importe que la sanction soit proportionnée à la gravité des manquements reprochés, d'autant que le juge administratif exerce ici un contrôle normal²³. Par exemple, le juge administratif de

²¹. CE, 19 octobre 2007, n° 280956.

²². CAA de Versailles, 16 novembre 2017, n° 16VE02646.

²³. Dans sa célèbre décision Dahan rendue le 13 novembre 2013 (n° 347704), l'Assemblée du contentieux du Conseil d'État considère « *qu'il appartient au juge de l'excès de pouvoir, saisi de moyens en ce sens, de rechercher si les faits reprochés à un agent public ayant fait l'objet d'une sanction disciplinaire constituent des fautes*

Déontologie et sécurité

Nice a récemment décidé que l'autorité militaire de premier niveau n'a pas pris une sanction disproportionnée en infligeant la sanction de dix jours d'arrêts avec dispense d'exécution à un gendarme affecté à la brigade de proximité de Mandelieu-La-Napoule, qui a refusé d'enregistrer la plainte d'une victime de 78 ans, tout en tenant des « *propos singulièrement grossiers* »²⁴.

En définitive, dans une perspective de clarification du droit applicable, et en complément des dispositions du CPP et de la Charte d'accueil du public et de l'assistance des victimes²⁵, le pouvoir réglementaire pourrait utilement ajouter un second alinéa à l'article R. 434-20 du CSI, ainsi rédigé : « *Les officiers et agents de police judiciaire de la police nationale et de la gendarmerie nationale sont tenus de recevoir les plaintes déposées par les victimes d'infractions à la loi pénale, en application de l'article 15-3 du code de procédure pénale* ». L'implicite serait ainsi rendu explicite, au bénéfice d'une meilleure accessibilité du droit et d'une protection renforcée des agents des forces publiques de sécurité intérieure comme des victimes.

de nature à justifier une sanction et si la sanction retenue est proportionnée à la gravité de ces fautes » (cons. 5). Ainsi, depuis cette décision, le juge exerce un entier contrôle juridictionnel sur les sanctions disciplinaires prises à l'encontre des agents publics en vérifiant que ces sanctions sont proportionnées à la gravité des fautes commises.

24. TA Nice, 12 novembre 2024, n° 2301143.

25. L'article 5 de la Charte de l'accueil du public et de l'assistance des victimes, applicable aux policiers et gendarmes nationaux, dispose que « *les services de police nationale et de gendarmerie nationale sont tenus de recevoir les plaintes déposées par les victimes d'infractions pénales, quel que soit le lieu de commission* ».

Sandrine RICHARD

L'usage de l'intelligence artificielle dans le maintien de l'ordre : enjeux juridiques, dérives éthiques et encadrement nécessaire

Depuis quelques années, l'intelligence artificielle (IA) s'impose comme une technologie clé de la transformation numérique des institutions, y compris dans le domaine sensible du maintien de l'ordre. Capable de traiter d'immenses volumes de données, de détecter des schémas invisibles à l'œil humain et de proposer des recommandations en temps réel, l'IA suscite un intérêt croissant au sein des forces de sécurité. En France, la Gendarmerie nationale n'échappe pas à cette dynamique, explorant des solutions allant de la vidéosurveillance algorithmique à l'analyse prédictive des comportements à risque.

Cependant, cette évolution soulève de nombreuses interrogations. Si l'IA peut accroître l'efficacité opérationnelle, elle peut également générer des dérives majeures : atteintes à la vie privée, surveillance de masse, biais algorithmiques, décisions opaques... À l'heure où la confiance entre citoyens et institutions sécuritaires est un enjeu crucial, l'usage de technologies potentiellement intrusives dans un cadre régalien pose des défis de taille en matière de droit, d'éthique et de gouvernance.

La question centrale qui se pose est alors la suivante : **comment encadrer l'usage croissant de l'IA par les forces de l'ordre tout en garantissant le respect des principes fondamentaux de l'État de**

Droit de l'espace numérique

droit ? Cet article propose d'examiner ce dilemme à la lumière des usages actuels de l'IA dans le champ sécuritaire, des implications juridiques et éthiques qui en découlent, et des voies possibles pour assurer un déploiement responsable et encadré de ces technologies.

I. L'usage croissant de l'intelligence artificielle dans les missions de maintien de l'ordre

I.1. Une diversité croissante des technologies utilisées

L'IA se déploie dans les services de sécurité à travers des outils de plus en plus diversifiés. Parmi les plus emblématiques figure la **vidéosurveillance intelligente**¹, capable d'analyser en temps réel les flux vidéo afin de détecter des comportements considérés comme suspects : attroupements, mouvements rapides, abandon d'objets, etc. Cette technologie, fondée sur l'apprentissage automatique, a été expérimentée dans plusieurs villes françaises, notamment dans le cadre de grands événements ou de dispositifs de vidéoprotection urbaine.

Autre technologie emblématique : la **reconnaissance faciale**, qui permet d'identifier une personne à partir d'une image capturée dans l'espace public. Bien que son usage reste pour l'instant très

¹. CNIL. Les caméras « augmentées » ou algorithmiques dans l'espace public [en ligne]. *Site de la CNIL*, 18 novembre 2024. Disponible sur : <https://www.cnil.fr/fr/cameras-augmentees-espaces-publics>

Droit de l'espace numérique

encadré en France, plusieurs pays l'ont adoptée de manière plus large, provoquant de vifs débats sur les libertés publiques.

Par ailleurs, les forces de l'ordre utilisent de plus en plus des **algorithmes prédictifs**, destinés à anticiper les risques d'infraction ou de trouble à l'ordre public à partir de données historiques (zones géographiques à forte délinquance, périodes à risque, etc.). Ces systèmes, comparables au PredPol américain, soulèvent des craintes de stigmatisation de certaines populations ou quartiers.

Enfin, l'usage de **drones autonomes**, de **robots patrouilleurs** ou d'**outils d'analyse sémantique** sur les réseaux sociaux constitue d'autres exemples de l'extension de l'IA dans les activités régaliennes.

I.2. Des finalités orientées vers l'anticipation et l'efficacité

L'objectif principal de ces outils est double : **anticiper** les événements perturbateurs et **rendre plus efficace** le déploiement des moyens humains et matériels. En identifiant en amont les lieux ou moments à risque, l'IA permet une allocation optimisée des forces sur le terrain. Elle favorise aussi la **réduction des délais de réaction**, en fournissant des alertes ou recommandations en temps réel à partir de données massives.

Elle offre également un appui décisionnel précieux pour les chefs de dispositifs, en croisant de multiples paramètres : météo, flux de foule, antécédents locaux, événements à venir, etc. Ce potentiel technologique séduit donc les décideurs sécuritaires, dans un contexte où les effectifs sont contraints et les exigences accrues.

Droit de l'espace numérique

I.3. Des expérimentations accélérées, mais controversées

L'usage de l'IA par les forces de sécurité s'est accéléré dans le cadre de certains événements majeurs. Ainsi, la **loi du 19 mai 2023 relative aux JO de Paris 2024**² a autorisé, à titre expérimental et temporaire, la mise en œuvre de systèmes de **vidéosurveillance algorithmique** pour détecter des événements prédéfinis. Cette évolution, bien qu'encadrée, a suscité des **réserves importantes de la part de la Commission nationale de l'informatique et des libertés** (CNIL) et de nombreuses Organisations non gouvernementales (ONG), qui y voient un précédent dangereux vers une surveillance généralisée.

Par ailleurs, certaines collectivités locales expérimentent déjà, dans le cadre de partenariats publics-privés, des dispositifs de sécurité intelligents sans toujours disposer d'un **cadre juridique clair**.

Ce flou alimente une inquiétude croissante dans l'opinion publique, attachée aux principes de proportionnalité et de nécessité dans l'usage des technologies de surveillance.

II. Enjeux juridiques : l'encadrement indispensable

L'introduction de l'IA dans le domaine du maintien de l'ordre

². LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions. *Légifrance*, dossiers législatifs. Disponible sur : <https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000046777392/>

Droit de l'espace numérique

interroge profondément le cadre juridique français et européen. Bien que certains outils utilisés soient innovants, les principes qui doivent encadrer leur emploi restent ceux de l'État de droit : légalité, proportionnalité, transparence et respect des droits fondamentaux. Or, l'utilisation de technologies intelligentes soulève de nombreux défis juridiques liés à la collecte, au traitement et à l'interprétation des données, notamment personnelles.

II.1. Un cadre juridique déjà en place, mais souvent insuffisant

Plusieurs textes de loi encadrent l'usage des données et des technologies dans le secteur public :

⇒ **Le Règlement général sur la protection des données (RGPD)**, applicable depuis mai 2018, impose des obligations strictes en matière de traitement de données personnelles : licéité, transparence, minimisation, durée de conservation limitée, sécurité du traitement, etc.

Concernant, à titre d'exemple, la reconnaissance faciale : de manière générale, les traitements biométriques, y compris la reconnaissance faciale, sont interdits sauf exceptions par les textes européens. **Le RGPD érige en principe, en son [article 9](#)³ l'interdiction des**

3. MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE. Le règlement général sur la protection des données (RGPD), mode d'emploi [en ligne]. *Site du ministère*, 7 août 2025. Disponible sur : <https://www.economie.gouv.fr/entreprises/gerer-son-entreprise-au-quotidien/assurer-sa-cybersecurite-et-la-protection-de-ses/le#>

Droit de l'espace numérique

traitements de données biométriques. De tels traitements ne peuvent être mis en œuvre que sur la base d'exceptions limitativement énumérées (consentement explicite des personnes, nécessité de protection de leurs intérêts vitaux, motifs d'intérêt public important, ...) et en adoptant des mesures appropriées aux risques en cause (exigence de proportionnalité).

⇒ L'article 10 de la **directive « police-justice »** ([directive \(UE\) 2016/680](#)) prévoit, par ailleurs, que le **traitement des données biométriques et génétiques est autorisé « uniquement en cas de nécessité absolue »**. Pour la Cour de justice de l'Union européenne ([décision C-205/21 du 26 janvier 2023](#)), le terme de « *nécessité absolue* » requiert une appréciation particulièrement rigoureuse et doit s'entendre comme « *une condition renforcée de nécessité du traitement de données* ». Il doit ainsi répondre à une finalité « *déterminée, explicite et légitime* » et ne viser que les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard desdites finalités (cf. le principe de [minimisation](#)).

⇒ En droit national, la **Loi Informatique et Libertés** (modifiée pour intégrer le RGPD dite [loi n° 78-17 du 6 janvier 1978, mod. 1^{er} juin 2019](#))⁴ et le **Code de la sécurité intérieure** posent les bases de l'utilisation des outils de surveillance (lus précisément, les articles [L 242-4](#) et [L 243-3](#) du Code de la sécurité intérieure interdisent

⁴. CNIL. La loi Informatique et Libertés. *Site de la CNIL* [en ligne]. 15 novembre 2024. Disponible sur : <https://www.cnil.fr/fr/le-cadre-national/la-loi-informatique-et-libertes>

Droit de l'espace numérique

expressément l'usage de dispositifs de reconnaissance faciale placés sur des drones et au sein de caméras embarquées dans des véhicules).

Les autorités administratives indépendantes, **en particulier la CNIL**, jouent un rôle crucial dans la régulation des expérimentations et l'évaluation de leur impact sur les libertés individuelles.

Ce texte national prévoit, néanmoins, que certains traitements de données biométriques **peuvent être autorisés par décret pris après avis motivé et publié de la CNIL**. Il s'agit notamment des traitements mis en œuvre pour le compte de l'État agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes (articles [31-II](#) et [32](#) de la Loi Informatique et Libertés).

Cependant, dans le cas des technologies fondées sur l'IA, ces textes restent **généraux** et **souvent inadaptés** face à la rapidité de l'innovation. Par exemple, le RGPD interdit en principe les décisions automatisées ayant un effet juridique significatif, sauf exception – mais qu'en est-il d'un outil prédictif utilisé pour décider du renforcement des effectifs dans un quartier ?

II.2. Des risques juridiques majeurs pour les libertés fondamentales

Les principaux risques juridiques tiennent à la **violation de droits fondamentaux** garantis tant par la Constitution que par les textes européens :

Droit de l'espace numérique

- **Droit à la vie privée** (article 8 de la Convention européenne des droits de l'Homme) : la captation et l'analyse de données personnelles dans l'espace public, y compris par vidéosurveillance intelligente, doivent être justifiées, proportionnées et strictement nécessaires ;
- **Liberté d'aller et venir, liberté de manifester, présomption d'innocence** : l'usage de l'IA ne doit pas créer un climat de suspicion généralisée, ni permettre un profilage de certaines catégories de population ;
- **Principe de légalité** : toute limitation des libertés doit être fondée sur un texte clair, précis, et accessible. Or, de nombreuses expérimentations se situent à la limite du droit, parfois dans des « zones grises » juridiques.

Par ailleurs, l'usage de systèmes algorithmiques dans des processus décisionnels publics pose la question de la **transparence**. Comment contester une décision fondée sur un algorithme, si celui-ci est opaque ou protégé par le secret industriel ?

II.3. Jurisprudence et prises de position récentes

Face à ces dérives potentielles, plusieurs juridictions et autorités ont rappelé les exigences du droit :

- Le **tribunal administratif de Marseille**⁵, dans une décision du 27 février 2020, a censuré l'usage de la reconnaissance faciale dans les

⁵. Tribunal administratif de Marseille, 9ème ch., 27 février 2020, n° 1901249.

Droit de l'espace numérique

lycées de la région PACA, jugeant que cette expérimentation n'était pas proportionnée à l'objectif poursuivi. Cette décision confirme la position de la CNIL sur le dispositif. En effet, saisie d'une demande de conseil par la région PACA sur l'expérimentation en question, la CNIL avait, dans son communiqué du 29 octobre 2019, indiqué au vu de l'analyse d'impact sur la protection des données (AIPD), que le dispositif envisagé était illégal et contraire aux principes de proportionnalité et de minimisation des données posés par le RGPD. Par ailleurs, la CNIL avait appelé à un débat démocratique sur le sujet et y a contribué fin 2019 en présentant les éléments techniques, juridiques et éthiques à prendre en compte ;

– La **Cour de justice de l'Union européenne** (CJUE)⁶, dans plusieurs arrêts récents (notamment *La Quadrature du Net e.a contre Premier ministre e.a.*, Décision 6 octobre 2020), a fortement limité la possibilité de conservation massive et indifférenciée des données de connexion ;

– La **CNIL**, quant à elle, a régulièrement appelé à la **prudence** sur les usages de l'IA sécuritaire. Dans un avis du 16 mars 2023, elle s'est montrée très critique à l'égard des projets de vidéosurveillance algorithmique dans les transports, soulignant les risques de surveillance disproportionnée⁷.

6. ARRÊT DE LA COUR (grande chambre), ECLI:EU:C:2020:791 [en ligne]. *InfoCuria Jurisprudence*, 6 octobre 2020. Disponible sur : <https://curia.europa.eu/juris/document/document.jsf?docid=232084&7>

7. CNIL, Délibération du 16 mars 2023, n° 2023-025 [en ligne] , doctrine.fr. Disponible sur : <https://www.doctrine.fr/d/CNIL/2023/CNILTEXT000048925274>

Droit de l'espace numérique

– Le **Défenseur des droits**⁸ a également alerté, dans plusieurs rapports publiés en 2020 et 2024 sur les risques de discrimination induits par certains systèmes d'IA utilisés à des fins sécuritaires ou administratives.

Ces décisions illustrent bien la **nécessité d'un encadrement spécifique** : les technologies nouvelles, si elles peuvent être compatibles avec les principes du droit, nécessitent des textes adaptés, une supervision renforcée et une évaluation indépendante.

Le respect du droit est une condition essentielle à la légitimité de l'action des forces de l'ordre. Mais, au-delà du droit, l'usage de l'IA soulève aussi des questions éthiques majeures : sur la transparence des algorithmes, les biais discriminatoires ou encore l'acceptabilité sociale de ces technologies. C'est ce que nous allons explorer dans le prochain chapitre.

III. Enjeux éthiques : risques de dérives et vigilance nécessaire

L'*AI Act* constitue un cadre européen pour l'usage de l'intelligence artificielle. Adopté le 21 mai 2024 et publié le 12 juillet 2024, il entrera progressivement en vigueur entre 2025 et 2027. Inspiré de

8. DÉFENSEUR DES DROITS. *Algorithmes, systèmes d'IA et services publics : quels droits pour les usagers ? Points de vigilance et recommandations* [en ligne]. Rapport, 2024. Disponible sur : https://www.defenseurdesdroits.fr/sites/default/files/2024-11/DDD_rapport_algorithmes-systemes-d-IA-et-services-publics_2024_20241025.pdf

Droit de l'espace numérique

l'approche du RGPD, il fixe des règles harmonisées pour encadrer l'IA dans l'Union européenne, avec un accent particulier sur les systèmes de reconnaissance faciale et d'identification biométrique.

a) Reconnaissance faciale : interdiction de principe et exceptions

Principe : l'usage de la reconnaissance faciale « en temps réel » dans les espaces publics à des fins répressives est interdit.

Les exceptions sont limitées (sous autorisation judiciaire ou administrative indépendante) :

- recherche de victimes (enlèvement, traite, exploitation sexuelle, personnes disparues) ;
- prévention de menaces graves et imminentes (terrorisme, sécurité des personnes) ;
- localisation de suspects d'infractions graves (terrorisme, trafic de stupéfiants, homicide, etc.).

Les États membres devront préciser les modalités d'application de ces exceptions.

b) Systèmes classés « à haut risque »

L'AI Act considère comme IA à haut risque :

- la reconnaissance et la catégorisation biométriques ;
- la reconnaissance des émotions ;
- les systèmes utilisés par les autorités répressives pour le profilage ou l'évaluation de risques (ex. prédiction d'infractions ou

Droit de l'espace numérique

identification de victimes).

c) Obligations associées aux systèmes à haut risque

Les concepteurs et utilisateurs doivent mettre en place :

- un système de gestion des risques (identification, évaluation, traitement des risques) ;
- des tests en conditions réelles ;
- des exigences de qualité des données ;
- une documentation technique complète ;
- une traçabilité/journalisation des opérations ;
- et surtout, une supervision humaine effective lors de l'utilisation.

En résumé, l'*AI Act* impose un encadrement strict et gradué de l'IA dans la sécurité et la justice : interdiction de principe pour la reconnaissance faciale en temps réel, exceptions encadrées au cas par cas, et exigences renforcées pour les systèmes à haut risque.

Si le cadre juridique vise à encadrer objectivement l'usage de l'IA, les réflexions éthiques permettent de poser les limites morales et sociétales à ne pas franchir. Dans le domaine du maintien de l'ordre, les dérives potentielles de l'IA sont d'autant plus préoccupantes qu'elles concernent directement des droits fondamentaux et la relation de confiance entre les citoyens et les institutions. Trois grands enjeux éthiques se détachent : les **biais algorithmiques**, la **transparence des systèmes** et l'**acceptabilité sociale**.

Droit de l'espace numérique

III.1. Les biais algorithmiques : un danger de discrimination systémique

Contrairement à une idée reçue, l'IA n'est pas neutre. Elle dépend des données sur lesquelles elle a été entraînée et des modèles statistiques choisis par ses concepteurs. Si ces données sont biaisées – ce qui est souvent le cas en matière de sécurité (concentration des contrôles dans certains quartiers, surreprésentation de certains profils...) – l'algorithme tendra à reproduire, voire à amplifier ces biais.

Plusieurs études internationales ont mis en lumière des cas de discrimination algorithmique :

- Le système **PredPol** aux États-Unis⁹ a été critiqué pour avoir concentré la surveillance policière dans des quartiers pauvres et à majorité afro-américaine, simplement parce que les données historiques de criminalité y étaient plus nombreuses ;
- Des **logiciels de reconnaissance faciale** ont montré des taux d'erreur très élevés pour les visages non caucasiens, exposant certains groupes à un risque accru d'erreurs d'identification¹⁰.

9. GOSSELIN, Camille. *La police prédictive. Enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique* [en ligne]. IAU île-de-France, avril 2019, 39 p. Disponible sur : https://www.institutparisregion.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf

10. CLÉMENÇON, Stéphane, MAXWELL, Winston. Pourquoi les algorithmes de reconnaissance faciale ne peuvent pas être parfaitement équitables sur tous les fronts en même temps [en ligne]. *Telecom Paris*, 6 octobre 2020. Disponible sur : <https://www.telecom-paris.fr/algorithmes-reconnaissance-faciale-pas-equitables>

Droit de l'espace numérique

En France, de telles dérives pourraient alimenter un **sentiment d'injustice**, voire de **profilage ethnique automatisé**, ce qui serait incompatible avec les principes d'égalité et d'impartialité qui fondent l'action publique.

III.2. La transparence et l'explicabilité des systèmes

Une autre dimension éthique majeure concerne le **manque de transparence** des algorithmes utilisés. De nombreux outils fondés sur l'apprentissage automatique sont des « boîtes noires », dont même les concepteurs ne comprennent pas toujours le fonctionnement précis. Pour les agents de terrain comme pour les citoyens, cette opacité est problématique.

Dans une démocratie, toute action de l'État – *a fortiori* en matière régaliennne – doit pouvoir être justifiée et expliquée. Si un citoyen est interpellé ou fiché sur la base d'un signalement algorithmique, il doit pouvoir comprendre **comment** et **pourquoi** cette décision a été prise. Or, l'utilisation de technologies opaques entre en conflit avec le **principe de redevabilité** des pouvoirs publics¹¹.

Des initiatives émergent autour du concept d'« **IA explicable** », mais elles restent encore limitées dans le domaine de la sécurité. L'enjeu est ici de garantir une **supervision humaine effective** et un contrôle

¹¹. MEYER, Erik, TORDEUX BITKER, Marianne. *Pour une intelligence artificielle au service de l'intérêt général*. Avis du Conseil économique, social et environnemental, janvier 2025, 224 p. Disponible sur : https://www.lecese.fr/sites/default/files/pdf/Avis/2025/2025_02_IA.pdf

Droit de l'espace numérique

démocratique des outils utilisés.

III.3. L'acceptabilité sociale et la crainte d'un glissement sécuritaire

Au-delà des aspects techniques ou juridiques, l'usage de l'IA en matière de maintien de l'ordre soulève un enjeu fondamental de **confiance**. Si les citoyens ont le sentiment d'être surveillés en permanence par des machines, sans possibilité de contestation ou de recours, cela peut profondément altérer la relation entre la population et les forces de l'ordre.

Les débats autour de la **reconnaissance faciale** ou de la **vidéosurveillance algorithmique** lors des grands événements (ex. : JO de Paris 2024¹²) ont montré un rejet fort d'une partie de la population, notamment en raison de la crainte d'une dérive vers une société de surveillance.

Ce rejet peut s'expliquer par plusieurs facteurs :

- la **complexité technique** des outils, qui rend leur fonctionnement difficilement compréhensible ;
- le **manque de transparence** dans les conditions de mise en œuvre ;
- l'**absence de débat public** ou de contrôle indépendant préalable.

De plus, l'usage de l'IA à des fins de sécurité risque d'alimenter un **glissement sécuritaire** : si ces outils permettent d'anticiper certains

¹². CNIL, *op.cit.* note 1.

Droit de l'espace numérique

comportements, jusqu'où ira-t-on dans la **prédiction et la prévention** ? Quelles garanties pour éviter que l'on passe d'une logique de sanction à une logique de **soupçon permanent** ?

L'encadrement juridique ne suffit pas, et l'analyse éthique montre les risques réels que pose un usage incontrôlé de l'IA. Dès lors, une approche globale est nécessaire : il faut construire un cadre de gouvernance adapté, associer les acteurs institutionnels et civils, et développer une culture d'usage responsable de l'IA dans les forces de l'ordre. Ce sont les pistes que nous explorerons dans le prochain chapitre.

IV) Vers un encadrement responsable et souverain de l'intelligence artificielle sécuritaire

Face aux risques juridiques et éthiques identifiés, il est impératif de poser les bases d'un **cadre clair, démocratique et souverain** pour l'usage de l'IA par les forces de sécurité intérieure. L'objectif n'est pas de freiner l'innovation, mais de s'assurer qu'elle s'inscrit pleinement dans les valeurs républicaines : respect des libertés, transparence, responsabilité et contrôle démocratique. Trois leviers principaux se dégagent pour garantir un usage responsable de l'IA dans le maintien de l'ordre : **l'encadrement réglementaire, la mise en place de structures de gouvernance éthique et la formation des acteurs de terrain**¹³.

¹³. PREMIER MINISTRE, SECRÉTARIAT GÉNÉRAL DES AFFAIRES EUROPÉENNES. Mari Draghi remet son rapport sur la compétitivité européenne à Ursula von der Leyen. Site du SGAE. Disponible sur : <https://sgae.gouv.fr/sites/SGAE/accueil/a-propos-du-sgae/actualites/mario-draghi-remet-son-rapport-s.html>

Droit de l'espace numérique

IV.1. Vers un encadrement réglementaire spécifique et évolutif

Le premier levier est juridique : il est urgent de compléter le cadre existant par des **textes spécifiques dédiés à l'usage de l'IA dans les missions de sécurité publique**. Cela suppose de sortir des logiques d'expérimentations ponctuelles, souvent encadrées par des arrêtés ou des dispositifs temporaires, pour bâtir une loi-cadre stable fixant les conditions de recours, les garanties minimales et les obligations des forces de l'ordre.

Une telle loi pourrait s'inspirer :

- du **projet de règlement européen sur l'IA (AI Act)**, qui classe les usages de l'IA selon leur niveau de risque, avec un encadrement renforcé pour les usages « *à haut risque* », dont font partie ceux liés à la sécurité et à la surveillance ;
- des **recommandations de la CNIL**, du Conseil d'État ou du Défenseur des droits, qui insistent tous sur la nécessité de **définir des finalités claires**, d'évaluer les impacts sur les libertés, et de prévoir des **mécanismes de contrôle indépendant**.

Un cadre normatif adapté permettrait de **sécuriser juridiquement les agents**, de garantir la **légalité des dispositifs** et de rassurer la population.

IV.2. Instaurer des comités d'éthique dans les institutions sécuritaires

Le deuxième levier est organisationnel : l'émergence d'une IA

Droit de l'espace numérique

sécuritaire appelle à la création de structures de réflexion et de contrôle éthique internes aux institutions concernées. Ces comités éthiques, à l'instar de ceux qui existent déjà dans le domaine médical ou de la recherche scientifique, pourraient :

- évaluer les projets d'IA en amont de leur déploiement ;
- vérifier leur conformité aux principes éthiques et juridiques ;
- associer des profils pluridisciplinaires : gendarmes, juristes, ingénieurs, sociologues, représentants de la société civile, etc.

Une telle structure existe déjà à titre expérimental au sein du **ministère de l'Intérieur** : le **Comité d'éthique de la sécurité intérieure (CESI)**, mis en place en 2021, pourrait servir de modèle ou être renforcé dans ses missions. Ce type de dispositif permettrait de favoriser une gouvernance partagée et une meilleure lisibilité de l'action publique.

IV.3. Former et acculturer les forces de l'ordre à l'usage responsable de l'intelligence artificielle

Enfin, un troisième levier – souvent sous-estimé – concerne la formation des agents et l'intégration d'une **culture de l'éthique numérique** dans les pratiques quotidiennes. L'IA n'est pas un outil neutre : son efficacité dépend de son **intégration raisonnée** dans les processus décisionnels¹⁴.

¹⁴. AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION. Recommandations de sécurité pour un système d'IA générative [en ligne]. *Site de l'ANSSI*, 29 avril 2025. Disponible sur : <https://cyber.gouv.fr/publications/recommandations-de-securite-pour-un-systeme-dia-generative>

Droit de l'espace numérique

Les gendarmes et policiers doivent donc être :

- formés à comprendre les **fonctionnalités, les limites et les biais** des outils algorithmiques ;
- sensibilisés aux **obligations légales et déontologiques** liées à la manipulation de données sensibles ;
- capables d'**exercer leur discernement humain** face aux recommandations d'un système automatisé.

Intégrer ces enjeux dans les **programmes de formation initiale et continue**, au sein de l'Académie militaire de la gendarmerie nationale (AMGN) ou du Centre national de formation de la police judiciaire (CNFPJ), serait une avancée majeure. Il en va de la **responsabilisation des utilisateurs**, mais aussi de la **légitimité des institutions** face à la société.

L'IA peut être un atout majeur pour les forces de l'ordre, à condition d'en faire un usage éclairé, proportionné et respectueux des droits fondamentaux. Les pistes présentées dans ce chapitre montrent que la **régulation est possible** sans freiner l'innovation. Il reste à construire, collectivement, une **IA de la sécurité à la fois efficace, éthique et démocratique**.

L'intégration de l'IA dans les missions de maintien de l'ordre représente une évolution technologique majeure pour les forces de sécurité intérieure, dont la Gendarmerie nationale. À la promesse d'une meilleure efficacité opérationnelle, d'une anticipation accrue des risques et d'une optimisation des ressources, répondent de **profonds enjeux juridiques, éthiques et démocratiques**. Cette tension entre **innovation technologique** et **respect des droits**

Droit de l'espace numérique

Fondamentaux ne peut être ignorée ni traitée à la marge.

L'analyse menée dans cet article montre clairement que l'IA ne peut pas être considérée comme un simple outil neutre. Elle est porteuse d'enjeux systémiques : biais algorithmiques, atteintes à la vie privée, opacité décisionnelle, perte de confiance du public... Ces risques, bien réels, nécessitent une réponse ferme, fondée sur les **principes de l'État de droit**, et sur une **approche éthique proactive**.

Face à ces défis, plusieurs leviers d'action s'imposent :

- un **encadrement juridique spécifique**, clair et adaptable, permettant de sortir des expérimentations ponctuelles pour construire un cadre stable et sécurisé ;
- la **création de comités éthiques internes**, capables de garantir la conformité des projets technologiques avec les valeurs républicaines ;
- une **formation adaptée des forces de l'ordre**, pour qu'elles puissent manier ces outils avec discernement, en pleine conscience des enjeux humains et démocratiques qu'ils impliquent.

La Gendarmerie nationale, par sa tradition de proximité, de rigueur et de réflexion stratégique, a un rôle clé à jouer dans la définition d'un **modèle français et européen d'intelligence artificielle sécuritaire**, à la fois performant et respectueux des libertés. Il ne s'agit pas de refuser la modernité, mais de **l'humaniser**, pour que l'IA reste un **outil au service de la République**, et non une menace pour ses fondements.

Droit de l'espace numérique

ANNEXE

Liste des Comités / instances existants

➡ Comité d'éthique de la défense (Comedef) / Ministère des Armées :

- Avant-garde pour un usage éthique de l'IA en contexte militaire / Examine l'intégration de l'IA dans les systèmes d'armes, formule des recommandations

- C'est une instance centrale pour les questions de défense. Moins claire si elle se penche sur la reconnaissance faciale dans le maintien de l'ordre intérieur, mais elle établit des principes applicables

- Site Web : <https://www.defense.gouv.fr/actualites/comite-dethique-defense-usage-lia-ethique-proportionne?>

➡ Comité de l'intelligence artificielle générative / Gouvernement français / Premier ministre / Ministères concernés (Économie, Numérique, etc.) :

- Vise à produire des recommandations concrètes sur l'IA générative : stratégie, innovation, régulation

- Pas exclusivement « sécurité », mais traite d'éthique de l'IA. Peu focalisé sur les usages répressifs, mais utile pour les principes généraux

- Site Web : <https://www.economie.gouv.fr/comite-intelligence-artificielle-generative?>

Droit de l'espace numérique

➡ **Comité d'éthique de la police municipale de Paris / Ville de Paris :**

- Surveille le respect de la déontologie par la police municipale. Peut rendre des avis sur les usages (dont potentiellement l'IA si appliquée à la police municipale)
- Instance locale, utile pour le niveau municipal, mais pas national
- Site Web : [https://www.paris.fr/pages/un-comite-d-ethique-de-la-police-municipale-pour-veiller-au-respect-des-regles-de-deontologie-20310?](https://www.paris.fr/pages/un-comite-d-ethique-de-la-police-municipale-pour-veiller-au-respect-des-regles-de-deontologie-20310?__track=page)

➡ **Comité éthique et pédagogique / École nationale de l'administration pénitentiaire (ENAP) :**

- Porte un regard sur les situations complexes et déontologiques dans la formation, y compris l'éthique professionnelle
- Plus orienté formation/pédagogie, moins sur l'usage opérationnel de l'IA dans le maintien de l'ordre
- Site Web : [https://www.enap.justice.fr/le-comite-ethique-et-pedagogique?](https://www.enap.justice.fr/le-comite-ethique-et-pedagogique?__track=page)

➡ **Comité d'éthique et de déontologie (CED) / Santé publique France :**

- Bien qu'il ne soit pas centré sur la sécurité intérieure, il touche aux usages technologiques, données, éthique, ce qui peut être pertinent pour des usages de l'IA dans la sécurité publique ou sanitaire
- Site Web : [https://www.santepubliquefrance.fr/a-propos/notre-organisation/une-organisation-au-service-des-programmes/comite-d-ethique-et-de-deontologie-ced?](https://www.santepubliquefrance.fr/a-propos/notre-organisation/une-organisation-au-service-des-programmes/comite-d-ethique-et-de-deontologie-ced?__track=page)

Droit de l'espace numérique

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

Nous reproduisons ici le discours du Général d'armée (2S) Marc Watin-Augouard, prononcé lors du colloque Souveraine Tech - Armée/Nation/Innovation dont le thème était « Raviver le lien Armée-Nation autour de l'innovation technologique », le 12 septembre 2025 à Saint-Malo

« Mesdames et messieurs,

Nous vivons un moment extraordinaire !

Extraordinaire parce que nous sommes ici ensemble à Saint-Malo, ville qui symbolise la défense, la souveraineté :

- La citadelle de Vauban et les cicatrices du siège d'août 1944 en sont les témoins architecturaux ;
- La souveraineté sur la mer a été gagnée avec les corsaires de Surcouf et de Duguay Trouin ;
- La souveraineté de la défense a été symbolisée par la fondation, dans cette ville, en 1998, de la politique européenne de défense qui, selon Tony Blair et Jacques Chirac, devait pouvoir s'exercer en dehors du cadre de l'OTAN et manifester la capacité politique et stratégique de l'UE d'agir en parfaite autonomie.

Saint-Malo est aussi la ville de Chateaubriand qui, dans ses *Mémoires d'outre-tombe*, évoquait avec lyrisme sa ville natale et son attachement à la défense : « *Né dans les combats, élevé sur les remparts de Saint-Malo, j'ai vu la mer avant de voir la campagne ; j'ai entendu le canon avant d'entendre la cloche.* »

Ce passage illustre à merveille le lien intime entre Chateaubriand et

Droit de l'espace numérique

Saint-Malo, ville fortifiée tournée vers l'océan, où le bruit des armes et la rigueur du vent marin ont façonné son imaginaire et son esprit de résistance.

Oui, nous vivons un moment extraordinaire, car nous sommes les témoins mais surtout les acteurs d'une métamorphose cybernétique. Cette expression surprend sans doute par son caractère ésotérique, tant l'expression « *transformation numérique* » est courante. Mais celle-ci est bien peu représentative de la réalité, telle qu'elle est vécue et le sera encore davantage dans la décennie à venir.

Nous traversons une période historique pour l'humanité, car les questions existentielles de la place de l'humain, de son intelligence, de sa liberté d'action et de pensée dans une société de l'information, se trouvent posées en des termes inédits.

Trop nombreux sont ceux qui ne comprennent pas encore que le monde cesse de progresser de manière quasi linéaire. Au sein du cyberspace, la progression est exponentielle. Les mutations sont de plus en plus impactées par des technologies de rupture qui se succèdent et se stimulent mutuellement à un rythme accéléré.

Nous vivons à l'ère de l'infiniment rapide, de l'infiniment grand et de l'infiniment petit, grandeurs peu accessibles à la perception habituelle que nous avons du monde physique avec son cadre espace-temps, sa matérialité.

Quelques exemples suffisent à illustrer cette accélération et ce changement de dimension :

- Quatre ordinateurs étaient connectés en 1969 ; plus de 500

Droit de l'espace numérique

milliards de machines le seront en 2030, grâce à l'Internet des objets ;

– Cette année-là, sera produit l'équivalent du contenu de mille milliards de disques durs d'un téraoctet. La donnée est et sera davantage encore une richesse pour son détenteur, pour celui qui l'exploite ;

– La gravure des semi-conducteurs va approcher le nanomètre, soit le milliardième de mètre ;

– La puissance de calcul s'exprimera en exaflops, soit un milliard de milliards d'opérations par seconde.

Ces chiffres échappent à nos repères, nos références.

Le cyberspace est étranger à nos sens, invisible, intouchable. Les technologies actuelles et futures sont plus difficilement compréhensibles par les humains.

L'ère nucléaire avait déjà amorcé cette distanciation, avec ses mythes et ses réalités. Avec la physique quantique, notre représentation newtonienne du monde s'efface. « *Être ou ne pas être* », la question binaire shakespearienne serait aujourd'hui formulée en « être et être, en même temps et à des endroits différents ».

Entre l'incompréhension et l'appréhension, il n'y a guère de distance. L'appréhension est le terreau du rejet de la technologie, car il est plus courant de refuser ce que l'on ne comprend pas. Mais elle est aussi source de comportements qui s'apparentent à la « politique de l'autruche ». La facilité, l'accessibilité sont des pièges qui réduisent notre vigilance, nous font baisser la garde, en même temps que nous sommes conscients du danger.

Droit de l'espace numérique

Un bouleversement cybernétique

Ce bouleversement que nous vivons est cybernétique – avec le sens que donnait Norbert Wiener – car le terme « numérique » ne caractérise pas suffisamment l'effet « réseau » qui permet de relier par 120 000 autonomes systèmes plus de cinq milliards d'habitants de la planète, d'échanger des données en s'affranchissant des distances et des délais.

Ce terme « numérique » n'exprime pas la complexité, l'impact systémique d'un tel réseau sur l'ensemble des activités humaines. Le cyberspace n'est pas un espace à part, contrairement à ce que croyait John Perry Barlow dans sa Déclaration d'indépendance d'Internet (1996) ; c'est un substrat numérique qui s'intrique désormais dans les milieux terrestre, maritime, aérien et spatial. Il est à l'immatériel ce que le système nerveux est à notre corps de chair. Nouveau domaine militaire, le cyber est partout, dans tout, pour tous, contre tous et sans doute déjà en tous. Il est objet et sujet de la cybersécurité, épée et bouclier.

Une métamorphose

Ce bouleversement n'est pas une mutation, ni même une révolution. Ce n'est pas une marche nouvelle dans l'escalier de l'humanité, comme dirait le poète ; c'est une métamorphose qui s'apparente à celle de la chenille lorsqu'elle devient papillon. Cette chenille rampe initialement sur un espace à deux dimensions : c'est la société traditionnelle que nous avons connue pour les plus anciens d'entre nous. Puis vient la nymphose, le cocon, cette impression que nous

Droit de l'espace numérique

avons d'être dans un monde fini grâce à la mondialisation, mêlée à la perception que notre corps social change, sous l'influence d'Internet, du web, des réseaux sociaux, de l'intelligence artificielle.

Soudain, en un temps très court, le papillon apparaît et découvre un nouveau monde, une nouvelle dimension. Nous allons, dans la décennie qui vient, connaître cette phase, rupture profonde à laquelle beaucoup de nos décideurs ne sont pas préparés et n'ont pas engagé notre pays, nos entreprises, nos administrations dans la dynamique qu'elle exige. Nos organisations, nos process ne sont plus adaptés. La formation, malgré les progrès accomplis dans l'enseignement supérieur, est loin de préparer les futures générations, alors que depuis ce mois de septembre, la formation à l'intelligence artificielle est obligatoire dans toutes les écoles de Chine, tandis qu'elle est modestement introduite dans les programmes de 4ème et de seconde en France. Alors que la convergence entre sciences dures et sciences humaines et sociales devrait inspirer notre modèle éducatif, le cloisonnement demeure encore une réalité. Le juriste doit désormais avoir une culture scientifique, l'ingénieur comprendre le droit, la sociologie. Oui, nos offres de formation répondent encore aux besoins des XIX^e et XX^e siècles !

La métamorphose cybernétique impose vitesse, agilité, transversalité, qualités qui ne sont pas encore partagées par des élites trop souvent déconnectées et confrontées à Internet qui « *dérange l'ordre établi* », pour reprendre l'expression de Laure Belot, dans son ouvrage *La déconnexion des élites*.

Droit de l'espace numérique

Les leviers de la métamorphose se conjuguent

Les leviers de la métamorphose cybernétique se conjuguent. L'informatique dans les nuages (*cloud computing*) permet de stocker les données et donc de ne pas fixer de limite à leur création, sous réserve de multiplier les data centers pour répondre à la croissance des données, notamment nécessaires au développement des applications d'intelligence artificielle (35 nouveaux *data centers* prévus en France d'ici à 2030). Ajoutons parmi les leviers les mégadonnées (le *big data*), la chaîne de blocs (*blockchain*), le métavers, l'Internet des objets (IOT), la multiplication des systèmes cyberphysiques, avec la convergence entre l'informatique opérationnelle et l'informatique de gestion (OT/IT), la « *robolution* », pour reprendre l'expression de Bruno Bonnell, la cobotique et, bien sûr, le calcul quantique dont on peut raisonnablement prévoir l'émergence d'ici cinq à dix ans. Le quantique sera une rupture, si l'on considère qu'un calculateur quantique demandera une seconde pour accomplir une action qu'un ordinateur opère en dix mille ans. Parmi les conséquences, la fin du chiffrement classique et l'obligation, dès à présent, de recourir à un chiffrement post-quantique qui résiste à une future attaque quantique. Au regard des exigences de défense et de sécurité, c'est une question urgente de souveraineté !

L'intelligence artificielle, technologie transversale

Il nous faut aujourd'hui porter un regard particulier sur l'intelligence artificielle qui est sans doute la technologie transversale qui enrichit

Droit de l'espace numérique

toutes les autres. Elle est l'aboutissement d'Internet. L'IA, c'est une expression à la mode, depuis la sortie de ChatGPT, en novembre 2022. Mais l'IA – nous devrions dire les IAs – trouve son origine avec Alan Turing (1950), le sommet du Dartmouth College (1956). À l'exception de son application dans les systèmes experts, elle a connu des « hivers », faute de pouvoir disposer à la fois d'une puissance de calcul et d'une quantité de données suffisantes.

Ces deux conditions sont aujourd'hui réunies, tandis que les systèmes « neuronaux » (IA connexionniste) permettent l'apprentissage automatique profond (*deep learning*). L'IA se diversifie (d'où le pluriel) : elle peut être prédictive (cf. le *big data*), générative, en produisant texte, image, son. Depuis quelques mois se développe l'IA agentique qui est capable de produire des actions et le discours porte désormais sur l'IA générale, voire la « super IA ». La première serait égale à l'intelligence humaine et serait capable d'agir dans un environnement complexe, sans être compartimentée dans un type d'action. Il est vraisemblable qu'elle soit d'actualité dans les cinq ans à venir. Geoffrey Hinton, prix Nobel de physique, prix Alan Turing et pionnier de l'IA, prédit qu'il y a 50 % de chances que l'IA devienne plus intelligente que l'humain.

Léopold Aschenbrenner, licencié par OpenAI en avril 2024, a publié, en juin 2024, *La décennie à venir*, mémoire dans lequel il estime qu'il est plausible que, d'ici à 2027, les modèles soient capables de faire le travail d'un chercheur/ingénieur en IA, en mesure d'automatiser tous les métiers cognitifs. 2028 sera, selon lui, l'année de l'automatisation de la recherche en IA.

Droit de l'espace numérique

Mais il annonce aussi une intelligence artificielle « *surhumaine* ». Cette perspective inquiétante à plus d'un titre pourrait être freinée par le « *mur de la donnée* » (sauf à développer des données synthétiques), par le mur de la puissance de calcul, du nombre de connexions entre neurones, ce que l'on qualifie de lois d'échelle, de *scaling laws*.

Les besoins colossaux en énergie, en eau, l'impact sur l'environnement pourraient être, sinon un obstacle, du moins un frein à la progression que l'on dit inexorable de l'IA. Certains évoquent un « *nouvel hiver* » de l'IA avec l'éclatement d'une « *bulle* » comme celle qu'a connue Internet il y a quelques années.

L. Aschenbrenner nous prédit un scénario « *brusque, intense, mondial* ». A Princeton, Arvind Naranayan et Sayash Kapoor prétendent que l'IA est « *une technologie normale* ». Qui croire ?

Quoi qu'il en soit, la question n'est pas de savoir si on atteindra cet objectif – hypothèse controversée – mais si certains États, par le biais de leur Big Tech, mettent tout en œuvre pour y parvenir, ici par une politique libertarienne de déréglementation, là par un asservissement au parti communiste, mais avec, dans les deux cas, la volonté de dominer le monde.

L'humanité est condamnée à maîtriser l'IA. Déjà, l'IA générative est une menace pour la propriété intellectuelle et donc la création d'origine humaine, dans sa richesse et sa diversité. L'IA générative abaisse la frontière entre le vrai et le faux, comme le montrent les hypertrucages non signalés comme tels (*deepfakes*). L'IA générale et, plus encore, la super IA appellent un alignement, c'est-à-dire le respect des valeurs de ses concepteurs afin de limiter leur

Droit de l'espace numérique

autonomie. Cet alignement est un des sujets traités par le Partenariat mondial sur l'intelligence artificielle, dont la dernière réunion a eu lieu à Paris, en février 2025. Mais le plan d'action américain sur l'IA de juillet dernier semble s'éloigner de toute contrainte, tandis que la Chine, au même moment, lors de la conférence internationale sur l'intelligence artificielle de Shanghai (*World Artificial Intelligence Conference WAIC*) semble prendre une voie plus conforme à une approche collective. Le monde à l'envers !

Un enjeu pour l'Etat

Geoffrey Hinton pense que les gouvernements sont la seule entité assez puissante pour ralentir cette évolution.

Ils sont en effet en première ligne pour contenir la démesure des géants la Big Tech qui, malgré des discours rassurants, pourraient être des « apprentis sorciers ». Il a raison ! Si l'État n'a pas la capacité de défendre les intérêts fondamentaux de la Nation, de protéger les personnes et les biens, de venir en aide aux victimes, son existence même sera remise en cause. « L'ubérisation » de l'État n'est pas une hypothèse à exclure. Sa souveraineté interne va dépendre de son « reformatage » à l'ère numérique. Alors que l'on dit Internet sans frontière, l'État demeure un échelon essentiel, parce qu'il est le seul garant de l'essentiel.

Les États, je l'ai dit, doivent protéger le citoyen contre le libertarisme et le collectivisme, contre le mercantilisme numérique et le totalitarisme numérique d'une société de surveillance.

Mais il faut compter aussi sur les citoyens qui pourraient sans doute

Droit de l'espace numérique

prouver que l'acceptabilité sociale des nouvelles technologies a ses limites.

Le citoyen est comme la chèvre de monsieur Seguin, naïf, désireux de liberté, d'indépendance et de nouveauté.

L'internaute est souvent attiré par les promesses séduisantes des plateformes numériques : accès gratuit, personnalisation, communauté, innovation... sans toujours mesurer les risques de surveillance, de profilage, de dépossession des données, de manipulation. La chèvre est dévorée par le loup numérique.

La condition première de la maîtrise de la métamorphose numérique est une prise de conscience des enjeux par un citoyen, aujourd'hui encore, trop crédule. « Science sans conscience n'est que ruine de l'âme », écrivait Rabelais. La conscience, c'est la représentation mentale de la réalité, la capacité d'en mesurer les influences, les effets. Sans elle, le citoyen ne peut recouvrer une souveraineté numérique, aujourd'hui grandement altérée par l'économie de l'attention, moteur des GAMAM (Google, Apple, Meta, Amazon, Microsoft) et ATBXH (Alibaba, Tencent, Baidu, Xiaomi, Huawei) par l'action de prédateurs, délinquants, criminels organisés, États voyous.

Le citoyen, premier échelon de la souveraineté numérique

L'expression « souveraineté du citoyen » est lâchée ! Je sais qu'elle fait hurler les défenseurs de l'approche classique de la souveraineté, celle de Jean Bodin ou de Carré de Malberg.

Ces puristes m'opposent le texte de la Constitution de la V^e

Droit de l'espace numérique

République qui précise, dans son article 3, que la souveraineté est nationale, ce que confirme le Conseil constitutionnel, en 1976, à l'époque du Minitel... en affirmant que la souveraineté ne peut être que nationale. Elle n'est pas divisible, selon les tenants de la doctrine, et ne saurait en tout état de cause être un attribut de la citoyenneté. J'admets volontiers leur raisonnement qui s'appuie sur des textes et une interprétation ancienne, bien antérieure à la métamorphose cybernétique. Je note que le Conseil – d'État, dans son étude annuelle 2024, fait un pas en ma direction en évoquant « *une citoyenneté active, condition de la souveraineté* ». Le mot citoyen revient 354 fois dans le rapport. Je ne sais si mon audition par la commission du rapport a eu un impact, mais je note le glissement sémantique.

En vérité, les auteurs de la Constitution ignoraient tout de ce qui est aujourd'hui notre présent et notre futur. Rédigeraient-ils les textes aujourd'hui de la même manière ? Je ne le crois pas.

Il est nécessaire de reconstruire le principe de souveraineté en partant du bas, du citoyen et en remontant, selon l'architecture – que je qualifiais, avant 2022, de « poupées russes » – partant de la plus petite et, par enveloppements successifs, finissant par la plus grande. L'image de l'artichaut serait peut-être plus pertinente (celle de l'oignon étant déjà prise pour le logiciel Tor). Partons cependant des poupées slaves, c'est plus politiquement correct... En bas, la petite poupée, c'est vous, c'est moi, c'est nous ! Si nous ne préservons pas notre libre arbitre, notre capacité à discerner, à penser, à décider, nous serons de zombies, des esclaves de l'espace numérique. « *Je pense, donc je suis* ». « Nous dépensons, donc nous suivons ». Nous dépensons, car nous payons avec nos données ce qui

Droit de l'espace numérique

semble gratuit. Nous suivons les algorithmes, le code qui fait loi, selon le professeur américain Lawrence Lessig.

Le seul remède est l'acculturation, la connaissance, le discernement, la montée en compétence, chacun à son niveau.

Mais comment y parvenir si les personnes morales publiques et privées au sein desquelles nous réalisons l'essentiel de nos actes individuels et collectifs ne sont pas, elles aussi, souveraines dans leur organisation, leurs décisions, leurs prestations ? Si elles sont perméables aux influences, aux attaques ? Si la liberté d'association, celle du commerce et de l'industrie sont entravées malgré elles, comment « l'homo cyberneticus » peut-il encore revendiquer une sphère d'autonomie, d'intimité ? Celui qui possède le pouvoir numérique est maître du libre-arbitre des individus. Inutile de poursuivre la métamorphose cybernétique si elle s'opère sans nous, contre nous !

Poursuivons notre escalade ! Comment les personnes morales peuvent-elle agir librement si l'État n'est pas souverain, alors que la doctrine des Big Tech est, depuis leur fondation, tournée vers la réduction du rôle de l'État, voire sa disparition ?

Comment la France peut-elle être souveraine si l'Union européenne est une passoire ?

Il n'en est pas de même quand celle-ci a l'ambition d'offrir au « cyber monde libre » une troisième voie, un chemin, une troisième voix, un discours, qui propose une alternative entre le libéralisme et le collectivisme, entre le business roi et le parti communiste dominateur. L'Europe conforte les souverainetés nationales, et elle le prouve depuis plusieurs années au travers d'une législation

Droit de l'espace numérique

numérique partagée qui protège les données à caractère personnel, les réseaux, conforte la résilience, renforce la lutte contre la cybercriminalité. Mais il lui arrive aussi, hélas, de manquer les grands rendez-vous de l'histoire numérique, qu'il s'agisse de la 5G, des semi-conducteurs, de l'IA. L'union fait la force, mais la force de l'Union serait d'être, elle-même, un peu plus souveraine dans sa démarche. Mon architecture de souveraineté est sans doute contestable, mais elle nous invite à replacer l'humain au cœur de toute politique, de toute stratégie. De bas en haut, de l'expression des besoins à l'élaboration d'une vision, elle nous oblige à reformuler les vraies questions, celles qui sont aujourd'hui existentielles, de ne pas être hors sol et, surtout, de communiquer vers le citoyen, d'expliquer les enjeux de la métamorphose cybernétique, dont il doit être acteur et non consommateur.

Cette approche atypique montre que chacun est détenteur, protecteur, défenseur d'une parcelle de la souveraineté. Celle-ci est divisible dès lors qu'elle est un agrégat, le résultat d'une addition – hélas aussi de soustractions – d'effets liés à des décisions, à des abstentions. La souveraineté qui ignore le citoyen est le propre des dictatures.

Défense et technologies

Protéger l'humain est, bien évidemment, l'objectif premier de la défense. Depuis la « révolution militaire » du XVI^e siècle, les forces armées ont épousé et, souvent anticipé, les grandes ruptures technologiques.

L'artillerie, les armes à feu portatives, le génie ont mis un terme à la

Droit de l'espace numérique

période féodale, conduit au passage de l'ost, avec le ban et l'arrière-ban, à des unités plus professionnelles. La Grande Guerre avec les chars, l'aviation, les gaz toxiques, les transmissions, a précédé la Seconde Guerre mondiale qui a introduit le radar, l'avion à réaction et, surtout, l'arme atomique.

La technologie influence directement la stratégie, si l'on se réfère à la dissuasion nucléaire, la « Guerre des étoiles ». Plus près de nous, la première guerre du Golfe (1991) avec la « Révolution dans les affaires militaires » a transformé profondément l'art de la guerre par l'usage innovant des technologies, notamment le GPS, les missiles guidés, les drones de reconnaissance. De cette époque est née l'illusion du « zéro mort », la distance et la haute précision réduisant, dit-on, l'engagement humain.

Cette surestimation du pouvoir des technologies peut avoir un effet démobilisateur chez le citoyen à qui on explique que le nucléaire empêche la guerre, que les armes pilotées à distance, avec l'appui de l'intelligence artificielle, évitent le retour des cercueils.

Les conflits contemporains contredisent cette vision idyllique, comme le soulignent la guerre en Ukraine et les guerres au Moyen-Orient qui nous obligent à reconsidérer la « guerre totale », avec son cortège de souffrances humaines, bien éloignées des « dividendes de la paix ».

Les conflits contemporains démontrent que les technologies s'ajoutent à l'arsenal mais ne le réduisent pas. À l'ère nucléaire, le fantassin est toujours le combattant du dernier mètre, à la force des baïonnettes.

Mais il y a sans doute un changement d'échelle à venir. Léopold

Droit de l'espace numérique

Aschenbrenner – que j'ai cité à propos de son essai *La décennie à venir* – nous dit – je le cite – que « *la puissance militaire et le progrès technologique ont été étroitement liés historiquement, et avec un progrès technologique extraordinairement rapide viendront des révolutions militaires concomitantes. Les essais de drones et les roboarmées seront un gros problème, mais ce n'est qu'un début ; nous devrions nous attendre à des types d'armes complètement nouveaux, des nouvelles armes de destruction massive à la défense antimissile invulnérable basée sur le laser, en passant par des choses que nous ne pouvons pas encore imaginer. Comparé aux arsenaux d'avant, la superintelligence, ce sera comme si les militaires du XXI^e siècle combattaient une brigade de chevaux et de baïonnettes du XIX^e siècle* ».

Le cyber dans la guerre

Sans attendre de vérifier cette prophétie, le cyber entre, dès à présent, dans la guerre avec des actions hybrides, l'intelligence artificielle automatise des décisions tactiques, les drones deviennent l'ennemi du combattant. Ce qui change depuis près d'un demi-siècle, c'est sans doute l'inversion de la source inspiratrice. À l'origine de nombreuses technologies, duales par la suite, les forces armées sont devenues clientes de technologies civiles. Bien que le cyber ne soit pas totalement étranger au financement du Pentagone, à partir de 1957, il est de conception civile, au sein des universités de Los Angeles, Santa Barbara, Stanford.

Aujourd'hui le cyber est dans la guerre, arme nouvelle. On ne gagne

Droit de l'espace numérique

pas la guerre avec les armes cyber mais on peut la perdre si on en est dépourvu.

Les sauts technologiques majeurs impactent les doctrines militaires et l'organisation de la défense, notamment militaire. Plus que jamais, notre capacité repose sur une base industrielle et technologique de défense (BITD), sur une limitation de nos dépendances, dès lors que les enjeux stratégiques sont identifiés. Plus que jamais, la puissance de notre complexe militaro-industriel est une condition de notre souveraineté à l'échelle nationale ou européenne.

La contribution du secteur privé à l'effort de défense est une réalité dans toutes les guerres modernes. Néanmoins, la guerre en Ukraine montre une évolution notoire en raison de la participation d'acteurs non étatiques avec une relative autonomie par rapport à la chaîne de décision. Les acteurs de la Big Tech apportent leur concours avant ou pendant les hostilités pour contribuer à la cyberdéfense ukrainienne. Pour autant, l'engagement des Big Tech est-il la marque de leur soutien à l'Ukraine ou la guerre serait-elle la continuité de leur politique commerciale avec l'introduction d'autres moyens que ceux des États ? Bien souvent, ces entreprises ont agi en dehors d'un contrat gouvernemental par la prise de décisions indépendantes. Cette contribution peut créer de tensions et des incertitudes, comme en témoigne l'apport essentiel de Starlink après la cyberattaque visant le réseau satellitaire KSAT. Les prises de positions d'Elon Musk, à géométrie variable, rendent fragiles ces coopérations qui peuvent cesser ou s'infléchir au gré des circonstances.

Droit de l'espace numérique

C'est dans ces circonstances que l'on mesure combien la question de la souveraineté est liée à celle des dépendances technologiques.

Technologies et lien Armée-Nation

La guerre de haute intensité pose en des termes nouveaux la question du lien Armée-Nation. La doctrine de dissuasion nucléaire, il faut le reconnaître, a pu laisser croire qu'il n'y aurait plus de conflit. Le maintien d'une conscription inégalitaire et la défense opérationnelle du territoire sans réels moyens ont entretenu la fiction d'un peuple en armes. Les interventions militaires, en dehors du territoire national, ont nourri l'illusion que le rôle des forces armées était réduit à celui de la continuité de la politique étrangère avec l'introduction d'autres moyens.

Les réductions drastiques du format des armées – par ceux-là mêmes qui appellent aujourd'hui à leur renforcement – ont eu pour effet de créer des déserts militaires, certains départements ayant la gendarmerie pour seule représentation des forces armées. Sentinelle redonne de la visibilité mais dans les zones urbaines et non dans la profondeur du territoire.

D'où une certaine distanciation entre la France et son armée, distanciation que les technologies renforcent. Elles ont été une des raisons ayant poussé les décideurs politiques et militaires à choisir la voie de la professionnalisation. Si, autrefois, le laboureur-chasseur ou le marin-pêcheur pouvait devenir rapidement soldat, le service des armes requiert aujourd'hui des compétences qui ne sont pas innées et qui s'acquièrent après une longue formation.

Droit de l'espace numérique

De là à penser que le métier des armes serait une externalisation d'une défense collective aux mains des militaires, il n'y a qu'un pas. Le lien Armée-Nation évoque une fracture, une altérité qu'il convient de compenser par l'établissement d'une relation, d'un pont, d'un harpon. Dans le discours public et institutionnel, l'expression « lien Armée-Nation » désigne la relation entre les forces armées et la société civile. Pourtant, cette formulation mérite d'être interrogée, car elle repose sur une conception implicite de séparation entre l'armée et la Nation, alors même que l'armée est issue de la Nation, en est une composante organique et en incarne certains des principes fondamentaux. La réserve n'est pas un lien armée-Nation, elle est l'armée à temps partiel.

Je n'ai jamais compris le sens de cette expression, sinon pour sa puissance incantatoire cherchant à masquer un vrai ou un faux problème. Elle est souvent employée par ceux qui veulent faire croire qu'ils cherchent à réparer après avoir détruit.

L'esprit de défense

Plutôt que de parler de lien armée-Nation, je préfère évoquer l'esprit de défense et la capacité de résilience qui ne sont pas le propre des membres des forces armées mais doivent être partagés par tous. C'est le ciment et non le lien. C'est l'attachement et non le lien. L'esprit de défense est directement lié à la menace, telle qu'elle est perçue par les citoyens. Aujourd'hui, une prise de conscience semble naître au sein de la Nation.

Droit de l'espace numérique

Le cyber relance l'esprit de défense

Les technologies numériques devraient, me semble-t-il, raviver la flamme de l'esprit de défense chez nos concitoyens, parce qu'ils sont de plus en plus conscients d'être la cible directe ou indirecte d'actions hybrides qui frappent la couche physique, la couche logique, la couche des protocoles et la couche sémantique ou cognitive d'internet.

Ils perçoivent chaque jour davantage que la cybercriminalité est la criminalité du XXI^e siècle – thème du 1^{er} Forum InCyber (FIC) en 2007. Jamais le prédateur n'a été aussi proche de sa victime, jamais il n'a été aussi éloigné de ses poursuivants. Depuis le conflit en Ukraine, au moins, les citoyens prennent conscience des liens entre les cyberattaques et les conflits qui se déroulent parfois loin de nos frontières. Ils savent que ce que l'on qualifie de cyberinfraction, en dehors d'un conflit armé, peut être le fait d'États qui utilisent les « banderilles numériques » pour mieux nous saigner, à défaut de pouvoir nous mettre à mort. La mise en application de la directive européenne sur la sécurité des réseaux d'information (NIS 2) et du règlement sur la cyberrésilience (REC) devrait accélérer leur acculturation, car ces textes vont avoir une incidence très forte, dans la capillarité du tissu économique et social et pas uniquement au sein des entités essentielles et importantes.

L'esprit de défense et la posture de résilience devraient se renforcer, à cause des technologies numériques mais aussi grâce aux technologies numériques qui sont un bouclier. Ainsi, l'IA est aussi bien une alliée des cyberdéfenseurs, comme elle est une complice

Droit de l'espace numérique

par fourniture de moyens des cyberattaquants.

La symbiose entre la lutte contre la cybercriminalité et la cyberdéfense, y compris dans ses composantes offensives, illustre parfaitement un continuum défense/sécurité qui se manifeste de manière éclatante dans le cyberespace. La frontière entre ce qui relève de « l'ordinaire », la sécurité intérieure, et de « l'extraordinaire », la cyberdéfense, est particulièrement poreuse du fait de la connexité des actions.

Le concept de *continuum* s'applique parfaitement au cyberespace, parce qu'il est sans frontière et associe dans une même zone grise le délinquant, le terroriste ou le « guerrier ». Dans le cyberespace, défense et sécurité intérieure sont désormais comme deux « sœurs siamoises », ayant chacune leur caractère mais partageant un tronc commun. Sauf dans l'hypothèse d'un conflit armé nous engageant directement, les attaques entrant dans le champ de la cyberdéfense sont aussi des infractions qui relèvent de la compétence de la justice et des services spécialisés de la police et de la gendarmerie.

Dans le monde réel, des théâtres d'opérations, des bassins criminogènes, des « quartiers sensibles » sont identifiés, tandis que des espaces échappent aux prédateurs ou sont faiblement affectés par leurs actions. Les champs de la lutte contre la cybercriminalité et de la cyberdéfense s'interpénètrent, offrant un territoire unifié au profit de tous les prédateurs. La lutte contre la cybercriminalité ne s'arrête pas là où commence la cyberdéfense. Dans le cyberespace, il n'y a pas de route dédiée à la circulation militaire, ni de « champ de bataille » ou de « zone de sécurité prioritaire ». Le principe du « best effort », qui préside au fonctionnement d'Internet, mélange tous les

Droit de l'espace numérique

flux, sans tenir compte de leurs contenus civils ou militaires. Dans le monde réel, les modes d'action du criminel sont généralement distincts de celui du guerrier, même si le guerrier peut être aussi un criminel (crime de guerre, mercenariat, etc.). Cela tient aux armes employées. Au criminel, le « 11,43 » ; au guerrier, le char d'assaut, le navire de combat ou l'avion de chasse. Dans le cyberspace, il y a des « armes lourdes » et des « armes de poing », mais la répartition n'est pas aussi nette.

S'il est vrai que les cyberdélinquants poursuivent des objectifs différents de ceux des cyberterroristes ou des « cyberguerriers », ils utilisent parfois les mêmes armes, empruntent les mêmes réseaux. Par exemple, une attaque par déni de service peut être le fait de délinquants qui cherchent un profit en opérant un chantage sur un opérateur de commerce en ligne, d'entreprises qui veulent affaiblir un concurrent, de terroristes qui veulent désorganiser les secours simultanément à un attentat, ou le fait d'agresseurs qui veulent affaiblir ou paralyser le fonctionnement d'un État.

Ce n'est pas le mode d'action mais le mobile qui permet de différencier des actions conduites par des prédateurs « multicartes ». La qualification d'une attaque dépend aussi de son intensité, de sa complexité, de la nature de la cible et de l'effet produit. Certaines actions sont si sophistiquées qu'elles nécessitent des moyens humains, matériels et financiers colossaux.

Le *continuum* ne conduit pas à la confusion des genres, les différents modes d'action dans le cyberspace suivant des règles du jeu qui ne sauraient être confondues.

Droit de l'espace numérique

Dans ce contexte, les citoyens se tournent vers les acteurs régaliens en espérant qu'ils seront capables d'empêcher un chaos que chacun imagine, eu égard à la pénétration du numérique dans tous les secteurs clés de la vie quotidienne. C'est d'ailleurs la question essentielle pour l'État qui doit cesser d'être l'État Providence pour redevenir l'État Gendarme, pour reprendre l'expression chère aux juristes. Il en va de sa légitimité.

Les forces armées, c'est-à-dire les armées et la gendarmerie, présentent l'avantage de couvrir, chacune dans son domaine de compétence, l'ensemble du spectre, de la lutte contre la cybercriminalité à la cyberdéfense offensive. Elles ne sont pas les seules à être engagées, puisqu'il n'y a pas de solution sans une coopération de tous les acteurs civils et militaires de l'État. Je pense en particulier à la justice, à la police nationale, aux services de renseignement, aux douanes. Il n'y a pas non plus de solution sans une coopération public/privé, compte tenu de la place éminente tenue par les offreurs de cybersécurité. Mais je crois que les forces armées ont prouvé qu'elles étaient à la pointe de l'épée.

La gendarmerie l'a montré en étant, avec le FIC, à l'avant-garde de la lutte contre la cybercriminalité, les armées ont pleinement pris en compte les enjeux cyber, au moins depuis la loi de programmation militaire de 2013 et ce que je qualifie de « magistère » de Jean-Yves Le Drian. Nous sommes ici en Bretagne. Quelle région peut illustrer davantage la mutation des armées, avec le pôle d'excellence cyber, le centre DGA-MI de Bruz, les grandes écoles militaires, Saint-Cyr, Navale, l'ENSTA ? Ce leadership n'échappe pas au regard de nos concitoyens, en tout cas ceux qui sont les plus avertis. Les candidats

Droit de l'espace numérique

à la réserve cyber de la gendarmerie et des armées sont nombreux, ce qui prouve, me semble-t-il, qu'il y a une dynamique. C'est peut-être la réserve qui est l'avant-garde d'un mouvement dans la profondeur. « Aux armes citoyens ! formez vos cyberbataillons ! ». Le numérique n'offre pas un lien mais une contribution réciproque armée-Nation.

Une couche physique non maîtrisée

L'esprit de défense est proportionnel à la proximité et à l'intensité de la menace, s'agissant des atteintes à la couche logique d'internet.

Mais il est une menace qui me semble sous-estimée et qui requiert une mobilisation de tous : celle qui vise les infrastructures numériques. Câbles sous-marins, satellites, fibres, relais, datacenters, n'ont rien de virtuel. Demandons à des responsables de la défense ou de la sécurité dans un département, une zone de défense, de présenter la carte des infrastructures numériques, de leurs interconnexions, et celle de leurs liens avec le réseau électrique. Elle n'existe pas, faute d'avoir été réalisée. Et pourtant, il est simple pour un agresseur de couper un câble, de scier un réseau de fibres, d'incendier un relais. Ces faits sont hélas quotidiens. Aujourd'hui, la défense des territoires numériques est en friche. C'est sans doute un domaine qui pourrait redonner un nouveau souffle à une défense opérationnelle des territoires rénovée. Elle impliquerait naturellement la gendarmerie qui est responsable de la sécurité publique sur plus de 95 % du territoire métropolitain et d'Outre-mer. Mais elle serait aussi une opportunité pour les armées

Droit de l'espace numérique

de revitaliser l'Organisation territoriale interarmées de défense, l'OTIAD.

Bien évidemment, la réserve opérationnelle, mais aussi la réserve citoyenne seraient des acteurs clés, comme le sont les opérateurs qui agissent sur leur propre réseau sans qu'il y ait une véritable réflexion systémique.

Le système de traitement automatisé de données (STAD) le plus fragile

J'achève mon propos avec un regard porté sur la couche sémantique cognitive, celle du sens, du contre-sens, du faux sens, du non-sens. Le système de traitement automatisé de données le plus extraordinaire, le plus inégalable, j'en suis certain, mais aussi le plus sensible est notre cerveau. Pour le protéger, pas de SOC, pas de « *threat intelligence* », de management des voies (APM) ou des identités d'accès (IAM), de *Big data*, d'IA, d'analyse comportementale, pas de groupe d'intervention rapide, de centre européen de compétences, d'unité conjointe de cybersécurité. Les seuls antivirus ou firewall sont la culture générale, le discernement, l'esprit critique, aujourd'hui laminés par une instruction publique qui néglige les fondamentaux au profit d'un zapping culturel déraciné.

Dans un espace numérique marqué par la multitude, la victime connaît la solitude.

Cette victime doit être au cœur des préoccupations de l'État, car c'est la mission première de celui-ci. S'il l'oublie, il perdra sa légitimité. Aujourd'hui, la désinformation – c'est-à-dire le fait de

Droit de l'espace numérique

diffuser des informations inexactes dans le but de tromper et de causer un préjudice – est devenue une véritable arme de guerre. En effet, dans les conflits contemporains, elle peut être utilisée pour influencer l'opinion publique, semer le doute, démoraliser et, parfois, masquer les réalités du terrain. Ses techniques sont variées : manipulation d'images, utilisation de faux comptes sur les réseaux sociaux, déclarations tronquées ou sorties de leur contexte, faux sites web... elle est partout et prend de multiples formes. Le Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), le ministère de l'Europe et des Affaires étrangères, les armées, les services s'en saisissent, agissent et manœuvrent sur un champ de bataille inédit, bien que la guerre psychologique soit déjà ancienne. Chacun, cependant, doit avoir conscience qu'il est cible et acteur dans ce combat collectif. Gérald Bronner est pessimiste. Selon lui, *« l'humanité est entrée dans l'ère de la post-réalité et cela va mal finir »*.

Comme l'exprimait le Général de Gaulle, *« en notre temps, la seule querelle qui vaille est celle de l'homme. C'est l'homme qu'il s'agit de sauver, de faire vivre et de développer »*. Oui, en notre temps de métamorphose cybernétique, il faut sauver l'homme contre les prédateurs de toutes natures, de le faire vivre dans un monde nouveau, de lui faire traverser une nouvelle Renaissance propice à un développement et non à un asservissement.

C'est cela qu'il faut défendre ! Les technologies ne suffisent pas ! Il nous faut mobiliser, connecter trois organes essentiels : le cerveau, le cœur et les tripes. C'est-à-dire l'intelligence, l'humanité et le courage ! »

Actualité pénale

Nathan Allix

La loi du 9 juillet 2025 créant l'homicide routier et visant à lutter contre la violence routière

La loi n° 2025-622 du 9 juillet 2025 créant l'homicide routier et visant à lutter contre la violence routière a été adoptée un peu moins de deux ans après qu'une proposition de loi portant le même intitulé a été déposée (le 17 octobre 2023), largement influencée par les demandes de victimes d'infractions routières ou de leurs familles, ainsi que par les conclusions du comité interministériel de sécurité routière du 17 juillet 2023. Pour mémoire, ce dernier avait notamment fait le constat que si le nombre de morts et de blessés graves sur les routes était resté globalement stable lors des dix années précédentes, la part des usagers vulnérables gravement blessés avait augmenté sur cette période.

Cette loi pourra susciter des réactions contrastées. Certains pourront lui reprocher de n'être, pour l'essentiel, qu'une loi symbolique ne modifiant que peu de choses à la répression déjà en place s'agissant des dommages corporels ou des atteintes à la vie causés par l'inconscience, voire par l'indifférence à la sécurité des autres, de certains conducteurs. D'autres salueront une loi soucieuse de la perception des victimes et de leurs proches et permettant, en outre, certaines améliorations plus substantielles.

I) Des modifications terminologiques et symboliques

L'innovation la plus visible de la loi du 9 juillet dernier, qui apparaît

Actualité pénale

dès le titre de la loi, consiste en la création d'un homicide routier. Ainsi que plusieurs observateurs ont pu le faire valoir alors que la loi n'en était qu'au stade de proposition, la création est en trompe-l'œil : le nouvel article 221-18 du Code pénal, qui dispose que « *le fait, pour le conducteur d'un véhicule terrestre à moteur, de causer, dans les conditions et selon les distinctions prévues à l'article 121-3, la mort d'autrui sans intention de la donner constitue un homicide routier* », définit ce délit dans les mêmes termes que les anciens alinéas 2 et suivants de l'article 221-6-1 du même Code, qui aggravait jusqu'à présent la répression de l'homicide involontaire commis par le conducteur d'un véhicule terrestre à moteur dans certaines circonstances (sur l'évolution de ces circonstances, cf. *infra* II). Pour l'écrire plus clairement, ce qui était hier une circonstance aggravante de l'homicide involontaire est devenu une infraction à part entière, désormais qualifiée d'homicide routier.

D'une façon peut-être moins visible, la même modification a été opérée pour les atteintes involontaires à l'intégrité des personnes : lorsque ces atteintes sont causées par le conducteur d'un véhicule terrestre à moteur, les anciennes circonstances aggravantes prévues par les articles 222-19-1 alinéa 2 et suivants et 222-20-1 alinéa 2 et suivants du Code pénal, selon que l'incapacité totale de travail est supérieure ou non à trois mois, sont devenues, aux articles 221-19 et 221-20 du même Code, les blessures routières ayant entraîné une incapacité totale de travail supérieure à trois mois et les blessures routières ayant entraîné une incapacité totale de travail inférieure ou égale à trois mois.

Les conséquences de cette modification sont d'autant plus limitées

Actualité pénale

que les peines encourues n'ont pas été modifiées : lorsqu'une seule des circonstances énumérées par ces articles est caractérisée, l'homicide routier est puni de sept ans d'emprisonnement et de 100 000 euros d'amende, les blessures routières ayant entraîné une incapacité totale de travail supérieure à trois mois de cinq ans et de 75 000 euros d'amende, celle ayant entraîné une incapacité totale de travail inférieure à trois mois de trois ans et de 45 000 euros d'amende. Lorsque deux circonstances ou plus sont retenues, les peines sont respectivement portées à dix ans d'emprisonnement et à 150 000 euros d'amende, sept ans d'emprisonnement et à 100 000 euros d'amende et cinq ans d'emprisonnement et à 75 000 euros d'amende. Dans ces différentes hypothèses, la répression demeure inchangée par rapport aux circonstances aggravantes de l'homicide involontaire et des blessures involontaires jusque-là prévues.

C'est dire que l'évolution est bien avant tout d'ordre terminologique et symbolique. L'exposé des motifs de la proposition de loi ne s'en cachait d'ailleurs pas, affirmant :

Cette proposition de loi vise ainsi à instaurer des qualifications spécifiques, distinctes de l'homicide involontaire et de l'atteinte involontaire à l'intégrité de la personne. Elle caractérise l'homicide causé par le conducteur d'un véhicule terrestre à moteur comme homicide routier, ainsi que les atteintes involontaires contre les personnes comme blessures routières, dès lors que le conducteur responsable a commis une faute importante, telle qu'un grand excès de vitesse, la consommation d'alcool ou de stupéfiants ou encore un délit de fuite.

En effet, dans de telles circonstances, la qualification

Actualité pénale

“ involontaire ” semble inadaptée. Elle est très mal vécue par les victimes et familles de victimes, qui demandent de longue date la création de cette qualification.

Par ailleurs, la création de ces infractions autonomes et spécifiques sont nécessaires pour mieux responsabiliser les auteurs de ces comportements volontairement dangereux au volant. En changeant, la loi permettra désormais de renforcer la perception de la gravité des comportements à l'origine de l'accident et la reconnaissance du statut des victimes

À cet égard, plusieurs remarques apparaissent possibles.

À l'origine de la modification opérée se trouve la volonté affirmée de ne plus qualifier d'« *involontaires* » les infractions commises par des conducteurs n'ayant pas respecté certaines règles essentielles de prudence imposées par le Code de la route. L'idée sous-jacente, à lire l'exposé des motifs, est double : d'une part, éviter un qualificatif heurtant les victimes et leurs familles, lorsque le comportement adopté ne relève pas de l'inattention mais de la véritable indifférence à la vie, ou à l'intégrité, d'autrui ; d'autre part, faire prendre conscience aux auteurs de ces comportements de la gravité de leur attitude en « *renforçant la perception de la gravité* » de celle-ci.

L'idée est ainsi d'isoler, au sein des atteintes aux personnes causées par une faute de conduite, celles qui relèvent d'une méconnaissance délibérée des règles de sécurité imposées par le Code de la route (voir plus précisément sur ce point le Rapport n° 2104 enregistré à la Présidence de l'Assemblée nationale le 23 janvier 2024). L'idée se

Actualité pénale

comprend bien mais conduit à un résultat un peu étrange, au moins du point de vue du plan du Code. En effet, toutes les atteintes aux personnes causées par la faute d'un conducteur de véhicule motorisé n'ont pas été exclues des qualifications d'homicide involontaire et d'atteintes involontaires : lorsqu'aucune des circonstances énumérées par les articles 221-18 et suivants du Code pénal ne sont réunies, ces comportements continuent de relever des articles 221-6-1, 222-19-1 et 222-20-1 du Code pénal, et d'être respectivement qualifiés d'homicides involontaires et d'atteintes involontaires à l'intégrité des personnes.

D'abord, afin de consacrer la spécificité des nouvelles infractions, ces dernières ont été réunies au sein d'un unique chapitre. Or, jusque-là, les articles 221-1 et suivants du Code pénal étaient consacrés exclusivement aux atteintes, volontaires ou non, à la vie (ainsi qu'aux disparitions forcées), et les articles 222-1 et suivants aux atteintes à l'intégrité physique ou psychique des personnes. Les nouveaux délits créés relevant à la fois des atteintes à la vie et à l'intégrité physique, le nouveau chapitre 1^{er} ter du titre II du livre II du Code pénal rompt avec ce découpage et conduit à inclure des atteintes à l'intégrité physique au sein des articles 221 du Code pénal.

Il en résulte ensuite que tout homicide ou blessure causés par un conducteur n'est pas un homicide routier ou des blessures routières au sens du Code pénal, et ne relèvent pas du chapitre éponyme, ce qui n'est pas forcément d'une parfaite simplicité.

Enfin, et même si cette dernière remarque correspond à la volonté des auteurs du texte de rompre les liens entre homicide et atteintes

Actualité pénale

involontaires d'une part, et manquements routiers graves d'autre part, il en résulte que des comportements matériellement proches sont désormais traités à des endroits distincts du Code.

S'agissant des objectifs affichés, on peut douter que l'évolution opérée par la loi du 9 juillet 2025 conduira à une véritable prise de conscience, par les auteurs de ces comportements, de leur responsabilité : il serait surprenant que celles ou ceux qui se montrent suffisamment indifférents à la sécurité des autres pour méconnaître les règles de sécurité essentielles destinées à éviter les accidents routiers prennent soudainement conscience de la gravité de leurs actes au motif que l'infraction n'est plus expressément qualifiée d'involontaire. Soit le fait d'avoir tué ou blessé une autre personne est d'ores et déjà suffisant à réaliser la gravité de son comportement, soit, si tel n'est pas le cas, il paraît illusoire que l'intitulé de l'infraction permette une telle prise de conscience.

On peut en revanche penser que l'objectif de prise en compte du sentiment des victimes sera plus facilement atteint. La nouvelle qualification correspond d'ailleurs à une demande, fortement relayée à la suite de certains drames particulièrement médiatisés, de certains proches de victimes et de certaines associations de victimes.

Reste cependant que, techniquement, les infractions en cause continuent à être pensées comme des infractions involontaires. Les textes d'incrimination eux-mêmes sont clairs à cet égard, mentionnant respectivement, outre une référence à l'article 121-3 du Code pénal, « *la mort d'autrui sans intention de la donner* » et les blessures causées « *sans intention de nuire* ». Cette approche est, en

Actualité pénale

elle-même, cohérente : quel que soit le degré d'inconscience des auteurs de ces infractions, ils n'ont pas voulu le résultat de leur comportement. Elle est toutefois porteuse de conséquences importantes. On peut en effet penser que c'est, dans une large mesure, en raison de cette approche que les peines encourues n'ont pas été modifiées.

Pour mémoire, en effet, la classification tripartite des infractions (crime, délit, contravention) est fonction de la peine encourue. En ce qui concerne plus spécifiquement la distinction des crimes et des délits, ces derniers font encourir, au plus, une peine d'emprisonnement de dix ans. Au-delà, l'infraction devient un crime. Or, avant l'entrée en vigueur de loi du 9 juillet 2025, l'homicide involontaire commis par un conducteur avec deux circonstances aggravantes était déjà réprimé de dix ans d'emprisonnement : c'est dire que ce comportement ne pouvait être réprimé plus sévèrement, sauf à changer la nature de l'infraction. Pourquoi alors ne pas sauter le pas et acter qu'à un certain niveau d'indifférence à la sécurité des autres, le comportement de celui qui a causé une mort au volant devient un crime ? La modification aurait toutefois dérogé à un principe structurant de la distinction entre crimes et délits : ainsi qu'en dispose l'article 121-3 du Code pénal, si « *il n'y a point de crime ou de délit sans intention de le commettre* », la règle est absolue pour les crimes, mais admet des dérogations pour les délits. Dès lors que les nouvelles infractions demeurent envisagées sous l'angle d'infractions involontaires, aucune aggravation ne pouvait avoir lieu sans remettre en cause la logique d'ensemble de notre classification des infractions. Le reste en découle : si l'homicide commis avec deux circonstances prévues par l'article est puni de dix ans

Actualité pénale

d'emprisonnement, celui commis avec une seule circonstance doit être moins sévèrement réprimé. Et ainsi de suite.

La seule solution, pour opérer une modification qui ne soit pas seulement symbolique, aurait été de modifier radicalement la conception de ces infractions. Certes, dans les hypothèses considérées, la mort ou les blessures ne sont pas voulues. Pour autant, il ne s'agit pas de fautes simples, mais de la méconnaissance volontaire de règles de conduite édictées pour protéger la sécurité des personnes, de fautes délibérées ou traitées comme telles. Ce faisant, l'infraction présente bien un élément d'intentionnalité. Simplement, l'intention n'est pas tournée vers l'atteinte à autrui. C'est d'ailleurs cet élément qui rendait la qualification « *involontaire* » aussi difficile à supporter pour les victimes ou leurs proches (ce qui pourrait d'ailleurs conduire à se demander si, par cohérence, il ne faudrait pas retirer le qualificatif à tous les homicides et atteintes à l'intégrité corporelle résultant d'une violation manifestement délibérée d'une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement, y compris lorsque les faits ne présentent pas de lien avec la conduite d'un véhicule).

En certaines hypothèses, le législateur a cependant pu, en « décalant » l'objet de l'intention, qualifier d'infraction intentionnelle ce qui aurait pu être traité comme une infraction involontaire. Le principal exemple concerne l'incendie. On sait, en effet, que l'article 322-6 du Code pénal dispose que « *lorsqu'il s'agit de l'incendie de bois, forêts, landes, maquis, plantations ou reboisements d'autrui intervenu dans des conditions de nature à*

Actualité pénale

exposer les personnes à un dommage corporel ou à créer un dommage irréversible à l'environnement, les peines sont portées à quinze ans de réclusion criminelle et à 150 000 euros d'amende », et que l'article 322-10 du Code pénal dispose que « l'infraction définie à l'article 322-6 est punie de la réclusion criminelle à perpétuité et de 150 000 euros d'amende lorsqu'elle a entraîné la mort d'autrui ». Dans un cas comme dans l'autre, l'un des « résultats redoutés » est la mort d'autrui ou l'atteinte grave à l'intégrité physique. Alors même que l'auteur de l'infraction n'aurait pas souhaité parvenir à ce résultat, le législateur a cependant estimé que le comportement adopté est en lui-même tellement dangereux et destructeur qu'il convient de s'arrêter à la volonté de causer un incendie, permettant de caractériser une intention et de passer le seuil de la qualification criminelle.

Reste que la transposition aux homicides routiers aurait été difficile : l'incendie volontaire, particulièrement d'un bois ou d'une forêt, présente en soit une gravité suffisante pour que le comportement soit érigé en crime même lorsqu'aucune atteinte à la vie ou à l'intégrité physique n'est à déplorer, ce que traduit d'ailleurs l'article 322-6. Appliquée aux homicides routiers, la solution aurait été plus artificielle. En effet, à la différence de l'incendie volontaire, le caractère criminel de l'infraction ne paraît envisageable, s'agissant d'infractions routières, que lorsqu'une victime est effectivement à déplorer. Il semble dès lors excessivement artificiel de considérer que l'infraction est intentionnelle au seul motif que les manquements aux règles routières le sont, tant le lien avec la mort de la victime est alors important.

Actualité pénale

C'est dire que le renforcement de la lutte contre les homicides et blessures routières ne pouvait vraisemblablement pas passer par une aggravation des peines encourues, au moins en ce qui concerne les peines privatives de liberté.

II) Les améliorations substantielles

Les auteurs de la proposition de loi n'ont pas limité leur projet à une amélioration terminologique et symbolique, ce que révèle à nouveau la lecture de l'exposé des motifs. Si certaines modifications sont, pour l'heure, incertaines, d'autre, bien que ponctuelles, sont indiscutables et constituent des améliorations du droit existant méritant d'être approuvées.

Au titre des évolutions qui doivent encore être confirmées, l'exposé des motifs affirme : « *Les peines principales encourues par les auteurs d'homicide routiers ou de blessures routières restent les mêmes qu'avant le changement de qualification. Cependant, le nouveau régime d'infraction créé, qui se différencie désormais des homicides et des blessures involontaires relevant du seul champ accidentel, ne devrait pas laisser les magistrats indifférents dans leur appréciation de la faute pénale commise, ce qui pourrait entraîner un durcissement du prononcé des peines* ». Le conditionnel employé est bienvenu, l'évolution apparaissant incertaine : aujourd'hui comme hier, on peut penser que les magistrats sont conscients de la gravité du comportement de ceux qui, par leur méconnaissance des règles routières fondamentales, ont causé un décès ou blessé autrui. Elle mérite *a minima* d'être confirmée par la pratique.

Actualité pénale

Pour le reste, la loi apporte des modifications qui concernent à la fois les comportements réprimés et les peines encourues.

En ce qui concerne les comportements réprimés, ainsi que le prévoyaient antérieurement les articles 221-6-1, 222-19-1 et 222-20-1 du Code pénal, sont visées les atteintes commises alors que le conducteur méconnaissait les règles élémentaires de prudence imposées par le Code de la route : conduite sous l'empire d'un état alcoolique ou refus de se soumettre à un test destiné à établir cet état, conduite en ayant fait usage de stupéfiants ou refus de se soumettre à un test, conduite sans être titulaire du permis de conduire et dépassement important des limites de vitesse. Est également concernée, bien que ce comportement intervienne *a posteriori*, l'hypothèse dans laquelle « *le conducteur, sachant qu'il vient de causer ou d'occasionner un accident, ne s'est pas arrêté et a tenté ainsi d'échapper à la responsabilité pénale ou civile qu'il peut encourir* ».

Le texte des nouvelles infractions n'est toutefois pas un pur décalque des anciennes circonstances aggravantes de l'homicide ou des atteintes involontaires. Sont désormais également visés par les textes les cas dans lesquels le conducteur a contrevenu « *aux dispositions du code de la route réglementant l'usage du téléphone portable tenu en main ou le port à l'oreille d'un dispositif susceptible d'émettre du son* », n'a pas prêté assistance à une personne en danger (ici la victime de l'accident) et, s'agissant de l'homicide routier et des blessures routières ayant entraîné une incapacité totale de travail supérieure à trois mois, a refusé d'obtempérer à une sommation de s'arrêter.

Actualité pénale

Est également ajoutée l'hypothèse dans laquelle « *le conducteur a volontairement consommé, de façon détournée ou manifestement excessive, une ou plusieurs substances psychoactives figurant sur une liste dressée dans des conditions déterminées par décret en Conseil d'Etat* ». Le rapport du 23 janvier 2024 explicite le comportement envisagé, mentionnant pour exemple « *la consommation de protoxyde d'azote ou les cas de surconsommation de médicaments* » : l'idée est ici de réprimer ceux qui, tout en consommant des substances licites, l'ont fait dans des conditions rendant particulièrement dangereuse la conduite, sans pour autant s'abstenir de prendre le volant.

Enfin, alors que l'excès de vitesse pris en considération était de 50 km/h, le seuil a été ramené à 30 km/h.

La portée de certaines évolutions est à relativiser. Que ce soit avant ou après la réforme, la première circonstance envisagée est celle dans laquelle « *le conducteur a commis une violation manifestement délibérée d'une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement autre que celles mentionnées* » aux points suivants. Cette « disposition balai » permettait potentiellement déjà de recouvrir certains comportements désormais expressément visés, notamment l'interdiction d'user d'un téléphone au volant. Il faut toutefois constater que, sur d'autres aspects, l'évolution est réelle, et qu'elle présente dans tous les cas une vertu pédagogique certaine.

Le seul ajout qui pourra, nous semble-t-il, véritablement interroger, est celui du cas dans lequel « *le conducteur a contrevenu à l'article L. 236-1 du code de la route* ». On sait que cet article réprime, pour

Actualité pénale

l'exprimer clairement, la pratique des « *rodéos urbains* ». À nouveau, ce type de comportement entraine déjà certainement dans le champ des articles 221-6-1, 222-19-1 et 222-20-1 du Code pénal. La clarification pédagogique apparaît toutefois ici moins évidente. Déjà parce que le texte opère par renvoi, ce qui n'est jamais gage de lisibilité pour les justiciables. Surtout parce que l'article L. 236-1 du Code de la route incrimine « *le fait d'adopter, au moyen d'un véhicule terrestre à moteur, une conduite répétant de façon intentionnelle des manœuvres constituant des violations d'obligations particulières de sécurité ou de prudence prévues par les dispositions législatives et réglementaires du présent code dans des conditions qui compromettent la sécurité des usagers de la route* ». Au titre des circonstances permettant l'application des articles 221-18 et suivants du Code pénal, sont donc désormais envisagées à la fois le manquement délibéré à une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement, et le même comportement dans le cadre d'une « *conduite répétant de façon intentionnelle* » de telles manœuvres. La lecture combinée des articles 221-18 du Code pénal et L. 236-1 du Code de la route apparaît d'autant moins claire qu'au titre des circonstances aggravantes, l'article L. 236-1 mentionne la conduite sous l'empire d'un état alcoolique, en ayant fait usage de stupéfiants ou sans être titulaire du permis de conduire... qui constituent déjà des circonstances mentionnées par les articles 221-18 et suivants. Il nous semble que l'ajout de cette circonstance aurait pu être cohérent, si elle avait entraîné, par elle-même, une aggravation de la répression correspondant au dernier alinéa des articles 221-18 et suivants.

Actualité pénale

En ce qui concerne les peines, ainsi qu'il a été vu, les peines principales sont demeurées inchangées. Tel n'est en revanche pas le cas des peines complémentaires qui ont été partiellement revues. On peut notamment mentionner l'ajout, à l'article 221-21, I, 6° et 8°, de la possibilité de prononcer la confiscation ou l'immobilisation pour une durée maximale d'un an du véhicule utilisé pour commettre l'infraction, même lorsque ce dernier n'appartient pas au condamné, dès lors que « *le propriétaire du véhicule l'a laissé à la disposition du condamné en ayant connaissance du fait que ce dernier* » était en état d'ivresse manifeste, avait fait usage de stupéfiants ou de substances psychoactives ou n'était pas titulaire du permis de conduire. L'ajout est sans doute louable, en ce qu'il vise à responsabiliser ceux qui offrent la possibilité à des personnes n'étant pas en mesure de conduire de prendre la route. On peut cependant, une nouvelle fois, douter de la portée du mécanisme, l'article 131-21 alinéa 2 du Code pénal permettant la confiscation de l'outil de l'infraction dès lors que l'auteur de l'infraction en a la libre disposition, « *sous réserve des droits du propriétaire de bonne foi* ». Dans l'hypothèse nouvellement consacrée, la bonne foi du propriétaire s'opposant à la confiscation pouvait déjà être raisonnablement discutée.

Pour le reste, les nouvelles dispositions étendent l'application de diverses peines complémentaires et peines complémentaires obligatoires. Certaines évolutions sont assurément opportunes : d'une façon peu cohérente, alors que l'article 222-44, I 5° permettait d'ores et déjà la confiscation « *d'un ou plusieurs véhicules appartenant au condamné* » même lorsque ces derniers n'avaient pas servi à commettre l'infraction, en présence d'atteintes à l'intégrité

Actualité pénale

physique, tel n'était pas le cas en matière d'homicide involontaire (Code pénal, art. 221-8). Les solutions sont désormais unifiées, étendant la possibilité d'une telle confiscation en cas d'homicide routier.

D'autres, sans être nécessairement critiquables, présentent un intérêt moins évident. Sans se livrer ici à une énumération exhaustive, on pourra synthétiser les différentes évolutions réalisées par la loi. D'abord, les blessures et homicides routiers étant désormais traités de façon autonome, l'article 221-21 du Code pénal ne reprend pas certaines peines complémentaires ne présentant pas de lien avec ce type de comportement (comme l'interdiction, à titre définitif ou temporaire, de détenir un animal). Ensuite, la possibilité de prononcer l'interdiction de conduire un véhicule qui ne soit pas équipé d'un dispositif d'anti-démarrage par éthylotest électronique est étendue à l'ensemble des hypothèses d'homicide routier et de blessures routières. Enfin, les cas dans lesquels les peines complémentaires d'annulation du permis avec interdiction de le repasser pendant un certain temps, d'interdiction de conduire un véhicule qui ne soit pas équipé d'un dispositif d'anti-démarrage par éthylotest électronique ou de confiscation de véhicule sont obligatoires, sont étendus, à la fois quant aux hypothèses concernées et, pour les deux premières, dans leur durée.

Jérôme Millet

Un simple tableau transmis à la préfecture mais sans base légale constitue un traitement illicite

Note sous CE, 4 juillet 2025, n° 503717

Le Conseil d'État a rejeté un recours déposé par le ministre de l'Intérieur contre une décision du juge des référés du tribunal administratif de Nantes qui a suspendu une note de la direction interdépartementale de la police nationale de Loire-Atlantique instituant un traitement de données à caractère personnel sur des étrangers en situation régulière.

1. Le ministre de l'Intérieur, Bruno Retailleau, invitait les préfets, le directeur général de la police nationale, le directeur général de la gendarmerie nationale et le directeur général des étrangers en France, dans une circulaire INTK2428339J du 28 octobre 2024¹ relative au renforcement du pilotage de la politique migratoire², à « *un pilotage dynamique de [leurs] services [devant] déboucher sur des décisions administratives fermes* ». Se faisant précis, il demande aux préfets d'organiser « *sur la base des éléments qui [leur] sont communiqués par les services de police, la gendarmerie nationale, l'administration pénitentiaire, ainsi que par l'autorité judiciaire, la prise*

1. MINISTRE DE L'INTÉRIEUR. *Renforcement du pilotage de la politique migratoire* [en ligne]. *Legifrance.fr*. Disponible sur : <https://www.legifrance.gouv.fr/download/pdf/circ?id=45581>

2. JCP G, n° 45, 11 novembre 2024, act. 1321.

Police administrative

en compte efficace des éléments nouveaux communiqués qui peuvent avoir des conséquences sur la police du séjour ». C'est ainsi qu'il est demandé « à ce que les forces de sécurité intérieure portent régulièrement et rigoureusement à la connaissance des services des préfectures et sous-préfectures chargés des étrangers les éléments susceptibles de caractériser un risque pour l'ordre public, afin que puissent être engagées les procédures administratives appropriées ». L'objectif est clair : aux étrangers en situation régulière suspectés d'avoir commis des actes de délinquance et, à ce titre, placés en garde à vue, l'administration doit pouvoir retirer ou dégrader le titre de séjour ou opposer un refus de séjour, s'il s'avère qu'ils ont effectivement causé un trouble à l'ordre public. Dans les départements où l'immigration est considérable et la délinquance importante, notamment en Outre-mer (on pense naturellement à Mayotte ou à la Guyane), il y a là un véritable levier pour le préfet, responsable de l'ordre public.

2. La circulaire est animée du souci de « *la reprise du contrôle de notre immigration* », fort du constat de la sur-représentation des étrangers impliqués dans la délinquance : c'est ainsi qu'au 1^{er} janvier 2025, près de 23 % des 95 380 personnes écrouées³ sont étrangères⁴, que 18 % des mis en cause enregistrés par la police ou

3. La population écrouée se compose des personnes en détention provisoire (prévenues en attente de jugement ou mises en examen) et des personnes condamnées à une peine de prison ferme (détenues ou pas).

4. MINISTÈRE DE LA JUSTICE. Références Statistiques Justice - en continu [en ligne]. Site du ministère de la Justice, Edition 2025 - sommaire des fiches disponibles, 12 juin 2025, mis à jour le 9 septembre 2025. Disponible sur : <https://>

Police administrative

la gendarmerie en 2024 pour homicide sont étrangers, 20 % pour tentative d'homicide, 22 % pour vol avec armes, 30 % pour vol violent, 37 % pour cambriolage de logement, 39 % pour vol dans les véhicules et 22 % pour trafic de stupéfiants⁵, étant précisé, d'une part, que le Service statistique ministériel de la sécurité intérieure ne dispose pas, à ce jour, d'informations permettant d'établir quels mis en cause sont plurinationaux⁶ et, d'autre part, que l'INSEE estime la population étrangère vivant en France à 5,6 millions de personnes, soit 8,2 % de la population totale⁷, incluant les étrangers en situation irrégulière, estimés à 900 000 au regard du nombre des bénéficiaires de l'aide médicale d'État (AME)⁸.

www.justice.gouv.fr/documentation/etudes-et-statistiques/references-statistiques-justice-continuu

5. SERVICE STATISTIQUE MINISTÉRIEL DE LA SÉCURITÉ INTÉRIEURE. Insécurité et délinquance en 2024 : bilan statistique [en ligne]. *Site du ministère de l'Intérieur*, 10 juillet 2025, p. 17 : <https://www.interieur.gouv.fr/Interstats/Infractions-et-sentiment-d-insecurite/Homicides-et-tentatives-d-homicides/Insecurite-et-delinquance-en-2024-bilan-statistique-et-atlas-departemental>

6. Réponse à question parlementaire du ministre de l'intérieur, *JO Sénat*, 05 décembre 2024, p. 4727.

7. INSEE. L'essentiel sur... les immigrés et les étrangers [en ligne]. *Site de l'INSEE*, 22 mai 2025. Disponible sur : <https://www.insee.fr/fr/statistiques/3633212>

8. On estime que seule la moitié des étrangers en situation irrégulière demanderait l'AME (Cf. DELAHAYE, Vincent, sénateur. Rapport d'information n° 841 fait au nom de la commission des finances sur l'aide médicale d'État, juillet 2025, p. 62). Or, au 30 septembre 2024, 465 744 étrangers en situation irrégulière bénéficient de l'AME, soit une multiplication par plus de 2 entre 2011 et 2024 (*Ibid.*, p. 54) représentant un coût de 1,3 milliard d'euros par an pour la collectivité nationale, en hausse de 64 % en dix ans (*Ibid.*, p. 38).

Police administrative

3. C'est dans ce contexte que le directeur interdépartemental de la police nationale de Loire-Atlantique a établi une note de service, le 20 novembre 2024, adressée aux services de police placés sous son autorité, intitulée « *Information des préfectures sur les délits commis par les étrangers en situation régulière* ». Celle-ci demandait au service interdépartemental de la police aux frontières d'adresser une fois par semaine les fiches complétées à la préfecture. La note de service est accompagnée de la « fiche navette » à compléter, qui comporte les rubriques suivantes : l'identification du « *service émetteur* », la « *situation administrative de l'étranger* », notamment l'« *identité de la personne* », sa « *nationalité* », son « *adresse connue* », son numéro dans l'application de gestion des dossiers des ressortissants étrangers en France (AGDREF), le « *titre [de séjour] en [sa] possession* », l'« *exposé des faits judiciaires* », notamment la présence dans le traitement des antécédents judiciaires (TAJ), avec l'« *exposé des principaux faits* », la « *date du placement en garde à vue* », l'« *élément d'ordre public pour lequel la personne a été interpellée* », les éventuelles « *suites judiciaires (déferrement, comparution immédiate, écrou...)* », les « *articles du code pénal fondant la procédure en cours* », la liste des « *pièces jointes* », notamment la « *copie du titre [de séjour]* » et le procès-verbal de garde à vue. Au titre du « *suivi de la demande* », la « fiche navette » comporte une rubrique à compléter par la préfecture retraçant les « *conséquences de la décision sur le droit au séjour* » et les « *suites administratives relatives à l'étranger : éloignement, placement en [rétention]* ».

Police administrative

4. Le Syndicat de la magistrature, le Syndicat des avocats de France et la Ligue des droits de l'Homme ont contesté cette note, arguant qu'elle mettait en place un traitement de données à caractère personnel sans autorisation légale. Par une ordonnance du 4 avril 2025⁹, le juge des référés du tribunal administratif de Nantes, saisi sur le fondement de l'article L. 521-1 du Code de justice administrative, leur a donné raison. Il a, d'abord, estimé qu'en organisant de manière générale et impérative, pour sa zone de compétence, les modalités de transmission des informations sur les procédures pénales engagées à l'encontre des étrangers en situation régulière pour l'ensemble des services pouvant être destinés à en connaître, la note en litige présentait le caractère, non d'une mesure d'ordre intérieur qui n'aurait pu être valablement contestée, mais d'une décision faisant grief eu égard aux effets qu'elle est susceptible d'entraîner sur le droit au séjour des personnes concernées. Le juge des référés reconnaît, ensuite, que la note du directeur interdépartemental de la police nationale peut « *concerner un nombre important d'étrangers en situation régulière sur le territoire* » au point qu'elle « *excède les seules circonstances locales* », permettant ainsi à la Ligue des droits de l'Homme de se voir reconnaître qualité pour agir, en dépit de la généralité de l'objet de l'association. Le juge des référés, enfin, mobilise la loi « Informatique et libertés » du 6 janvier 1978 qui prévoit, à son article 31, que les traitements de données à caractère personnel mis en œuvre pour le compte de l'État et intéressant la sûreté de l'État,

9. TA Nantes, 4 avril 2025, n° 2504541.

Police administrative

la défense ou la sécurité publique, sont autorisés par arrêté du ministre compétent, pris après avis motivé de la Commission nationale de l'informatique et des libertés (CNIL). Le juge des référés du tribunal administratif de Nantes a suspendu la note au motif que « *le moyen tiré de ce que cette note instituait un traitement de données à caractère personnel non autorisé par un arrêté ministériel* ».

5. Le ministre de l'Intérieur conteste cette suspension et, à l'appui de son pourvoi en cassation, tente de convaincre le Conseil d'État que ce traitement se borne à mettre en œuvre les dispositions applicables à l'enquête administrative et au traitement des antécédents judiciaires (TAJ). Selon les dispositions du V de l'article L. 114-1 du Code de la sécurité intérieure, il peut être procédé à des enquêtes administratives, notamment pour le retrait, en application de l'article L. 432-4 du Code de l'entrée et du séjour des étrangers et du droit d'asile, d'un titre ou d'une autorisation de séjour à un étranger dont la présence en France constitue une menace ou une menace grave pour l'ordre public. Dans le cadre de ces enquêtes, les policiers et les gendarmes habilités ainsi que les personnels investis de missions de police administrative individuellement désignés et spécialement habilités, peuvent consulter sans autorisation du ministère public les données à caractère personnel figurant dans le TAJ se rapportant à des procédures judiciaires en cours ou closes. Lorsque des personnels investis de missions de police administrative constatent à cette occasion que l'identité de la personne concernée a été enregistrée dans le TAJ en tant que mise en cause, l'enquête administrative ne peut aboutir à un avis ou une décision

Police administrative

défavorables sans, notamment, la saisine préalable, pour complément d'information, des services de la police nationale ou des unités de la gendarmerie nationale compétents. Mais, dans sa décision du 4 juillet 2025¹⁰, le Conseil d'État a considéré la note de service du directeur interdépartemental de la police nationale comme mettant en place un traitement de données à caractère personnel des « *étrangers en situation régulière placés en garde à vue* » qui nécessitait une autorisation légale, en l'occurrence, un arrêté ministériel, en application de l'article 31 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

6. À certains égards, cette décision du Conseil d'État est à rapprocher de celle du tribunal administratif de Montreuil du 20 mai 2025¹¹. En l'espèce, le préfet de la Seine-Saint-Denis avait diffusé au sein de ses services, mais aussi au sein de services ne relevant pas de son autorité, un document intitulé « *Fiche réflexe / Le signalement des ESR TOP par la DTSP93 à la préfecture de la Seine-Saint-Denis* » leur imposant de signaler les étrangers en situation régulière placés en garde à vue, au moyen d'une fiche contenant les données personnelles des personnes étrangères concernées. Le document diffusé indiquait que les étrangers en situation régulière, interpellés et placés en garde à vue par ses destinataires, devaient être signalés aux services de la préfecture. Il organisait les modalités

¹⁰. CE 4 juillet 2025, n° 503717, *JCPA*, 15 juillet 2025 act. 339, *AJDA* 2025, p. 1313.

¹¹. TA Montreuil, ord., 20 mai 2025, n° 2506577, *Ligue des droits de l'Homme*. V. Cédric MEURANT, *JCPA* 2025, chron. 2218.

Police administrative

de ce signalement au moyen d'un support intitulé « *rapport administratif* » comprenant des éléments d'identité de la personne concernée, une description des faits lui étant imputés et constitutifs d'une infraction, ainsi que les suites judiciaires données. Il précisait que ce rapport devait être accompagné, lors de sa transmission, d'un rapport d'identification dactyloscopique et des pièces d'identité et titre de séjour de l'intéressé. Il prévoyait, enfin, que le bureau du séjour de l'arrondissement de Bobigny de la direction des étrangers de la préfecture soit chargé de centraliser les signalements. Le syndicat de la magistrature avait pu dénoncer « *une administration parallèle des personnes étrangères, fondée sur la suspicion généralisée et le contournement des garanties les plus élémentaires* »¹². Mais ce n'est pas sur le fondement d'une prétendue création de fichier non autorisé que le juge administratif suspend la note du préfet mais sur le moyen tiré de l'incompétence du préfet de la Seine-Saint-Denis pour prendre des mesures d'organisation et de fonctionnement des services de la direction territoriale de la sécurité de proximité de la Seine-Saint-Denis qui ne relèvent pas de son autorité. En effet, depuis 2009, ces services sont placés sous l'autorité du préfet de police¹³.

¹². SYNDICAT DE LA MAGISTRATURE. Fichage des étranger.e.s en situation régulière : après Nantes, Montreuil suspend à son tour. Jusqu'où ira la politique de Retailleau ? [en ligne] *Site du Syndicat de la magistrature*, 23 mai 2025. Disponible sur : <https://www.syndicat-magistrature.fr/notre-action/communiqués-de-presse/fichage-des-%C3%A9trangeres-en-situation-r%C3%A9gul%C3%A8re-apr%C3%A8s-nantes-montreuil-suspend-%C3%A0-son-tour-jusqu'o%C3%B9-ira-la-politique-de-retailleau/>

¹³. Article 1^{er} du décret n° 2009-898 du 24 juillet 2009 relatif à la compétence territoriale de certaines directions et de certains services de la préfecture de police :

Police administrative

7. Au final, nous formulerons une double remarque : d'une part, à la suite de la suspension en urgence décidée par le Conseil d'État, le tribunal administratif de Nantes devra se prononcer, dans les prochains mois, sur le fond quant à la légalité de la note de service. D'autre part, et surtout, le Conseil d'État ne condamne pas définitivement l'initiative de la police nationale, comme l'y invitait le rapporteur public, Frédéric Puigserver, dans ses conclusions¹⁴ mais semble conditionner la légalité de la démarche du directeur interdépartemental de la police nationale à l'édiction d'un arrêté ministériel. Dès lors, compte tenu de la part prise des étrangers même en situation régulière à la délinquance (près de 23 % des 95 380 personnes écrouées¹⁵ sont étrangères), de la saturation des établissements pénitentiaires et de l'intérêt qu'il y a à lutter contre la récidive en éloignant vers leurs pays d'origine ceux qui troublent l'ordre public, il n'est pas impossible qu'un arrêté ministériel organisant la transmission de données entre services de police interpellateurs et services de la préfecture soit à l'étude au ministère de l'Intérieur.

« La direction de la préfecture de police chargée des missions de sécurité et de paix publiques est compétente à Paris et dans les départements des Hauts-de-Seine, de la Seine-Saint-Denis et du Val-de-Marne ainsi que, dans les secteurs définis par arrêté du ministre de l'intérieur, sur les emprises des aéroports de Paris-Charles de Gaulle, du Bourget et de Paris-Orly ».

¹⁴. CONSEIL D'ÉTAT. Conclusions du rapporteur public, N° 503717, *Ministre d'Etat, ministre de l'intérieur c/ syndicat de la magistrature, du syndicat des avocats de France et la Ligue des droits de l'homme*, 10ème et 9ème chambres réunies. Disponible sur : <https://share.google/PnCf8lyzMgMUCrYx3>

¹⁵. Cf. note 3.

Florence NICOUD

Le cas des rodéos urbains motorisés en question : lorsque le maire supplée à l'impéritie publique

À l'heure où la sécurité des transports terrestres fait souvent la une des médias et l'objet de récentes législations¹, le phénomène des rodéos urbains motorisés ou « cross bitume » bat son plein, mettant directement en danger les habitants, et plus globalement déstabilisant l'ordre public dans nos villes par l'effet de nuisances sonores. Ce type d'activité, consiste, selon la loi de 2018² visant à en éradiquer le phénomène, à « *adopter, au moyen d'un véhicule terrestre à moteur, une conduite répétant de façon intentionnelle des manœuvres constituant des violations d'obligations particulières de sécurité ou de prudence prévues par les dispositions législatives et réglementaires du code [de la route] dans des conditions qui compromettent la sécurité des usagers de la route ou qui troublent la tranquillité publique* »³. L'activité se déroule généralement au moyen

¹. Voir notamment notre note sur les apports des loi Savary et Tabarot : NICOUD, Françoise. *Quand la sûreté des transports ferroviaire passe à la vitesse supérieure : Bilan de la sûreté ferroviaire dans le cadre des récentes lois visant à renforcer les prérogatives de police des services de sécurité internes de la SNCF et RATP*. *La Veille juridique*, CRGN, mars 2025 n° 130, p. 50-65. Disponible sur : <https://www.calameo.com/read/0027192920d24c54389dc?page=50>

². Loi n° 2018-701 du 3 août 2018 renforçant la lutte contre les rodéos urbains, JO, n° 0179 du 5 août.

³. Art. L. 236-1 du Code de la route.

Droit des collectivités territoriales et de la sécurité privée

de scooters, de motos, voire de voitures⁴, directement sur la voie publique et quelquefois sur des champs agricoles. Aussi, nombre de maires de communes, petites ou grandes métropoles ont maille à partir aujourd'hui avec ce nouveau fléau, suivi la plupart du temps de refus d'obtempérer, voyant le nombre de victimes s'égrener sur les trottoirs et rues de nos cités. Qu'on se souvienne, pour les cas les plus récents et dramatiques par exemple, de la petite Kamyliya en août 2024 à Vallauris, mortellement percutée par un chauffard en moto à un passage piéton, du sapeur-pompier d'Evian-les-Bains en mai 2025 traîné sur plusieurs mètres par l'auteur des faits avant que ce dernier ne crache sur sa victime une fois son forfait accompli. Le terme de rodéos urbains devient alors inapproprié, on le remplacerait bien volontiers par le terme de rodéos sauvages.

Dans les zones périurbaines souvent encore agricoles, les rodéos motorisés se développent dans un certain nombre de villes moyennes comme Saint Quentin ou Charleville-Mézières, voyant les champs agricoles abîmés par l'action de ces nouveaux délinquants en deux-roues. Un certain nombre de communes comme celles du Havre ou de Valence ont même créé, afin d'endiguer ce phénomène, des unités spécialisées dédiées à la lutte contre ce fléau manifestement difficile à éradiquer. Face à cela, il était attendu que le droit de la sécurité intérieure s'empare de ce questionnement majeur relatif à la sécurité urbaine. Très souvent, les termes d'impunité des auteurs d'infraction, de négligence de l'État, voire

⁴. C'était effectivement le cas lors du rodéo motorisé d'Evian de mai 2025 ayant rassemblé quelque 500 voitures et 3 000 personnes.

Droit des collectivités territoriales et de la sécurité privée

même d'absence de prise en compte du problème par les décideurs publics, sont relevés dans les rapports ou synthèses relatifs à ce sujet. Face à ce phénomène en pleine recrudescence ces derniers mois, il a même pu être invoqué que « *lorsque des tiers se retrouvent percutés par les auteurs de rodéos, comme ce fut le cas le 5 août 2022 à Pontoise et le 8 juin 2022 à Rennes, alors la doctrine de l'intervention différée des FSI trouve ses limites* »⁵. En effet, et contrairement à la politique pénale du Royaume-Uni par exemple, privilégiant le contact direct avec les auteurs de troubles (technique dite du « choc tactique » se manifestant par la percussion volontaire de l'auteur du rodéo), la France préconise avant tout le non-contact et le développement d'une politique raisonnée de prévention.

Si l'effet de course-poursuite entre policiers et conducteurs comporte en effet un certain nombre de risques et de limites, pour autant l'heure est au questionnement quant à un éventuel changement de paradigme. Le ministre de l'Intérieur, M. Retailleau, indiquait dernièrement « *qu'une nouvelle instruction pour généraliser les poursuites sur les rodéos serait prise dans quelques jours* ». Il sera donc demandé aux policiers et gendarmes partout sur le territoire de prendre en chasse ces véhicules⁶, isolant le cas

5. MURBACH-VIBERT, Mathias. Lutte contre les rodéos : une occasion manquée par la LOPMI. *AJDA*, 2023, p. 146.

6. Rodéos urbains : Face à l'hyperviolence, Bruno Retailleau appelle « à une révolution pénale » [en ligne] [3'33"]. *YouTube*, juin 2023. Disponible sur : <https://www.youtube.com/watch?v=cqeyF69aplo>

Droit des collectivités territoriales et de la sécurité privée

particulier de la zone du ressort du préfet de police de Paris pour laquelle la poursuite physique avec le véhicule est la règle. Alors, comment appréhender et mettre fin à ce fléau urbain, s'étendant même jusqu'aux campagnes ? Quelles mesures ont été prises jusque-là et comment améliorer le droit déjà existant en ce domaine ? Afin d'y répondre, trois principaux points seront analysés, tout d'abord le constat d'un fléau urbain qui n'a en réalité rien de nouveau (I), puis une loi de 2018 semblant atterrir à son but (II) et, enfin, une jurisprudence hésitante ayant du mal à déterminer la part de responsabilité administrative des décideurs locaux et nationaux (III).

I) Un fléau sociétal préexistant

Les chiffres parlent d'eux-mêmes et semblent faire de cette pratique un nouveau fléau urbain. Loin d'être éradiqués, les rodéos urbains augmentent sensiblement d'année en année, attestant d'une certaine forme d'incapacité publique à vouloir ou pouvoir les juguler. Ainsi, en 2017, selon les données du ministère de l'Intérieur, un total de 8 700 rodéos a été enregistré par la police nationale, dans des zones urbaines, et particulièrement dans les quartiers prioritaires de la politique de la ville. *« Initialement circonscrit aux quartiers dits sensibles, ce phénomène tend à se développer largement en périphérie des centres urbains et parfois même dans les campagnes. Sur cette même année, la gendarmerie nationale a recensé 6 614 interventions contre 5 335 en 2016, soit une*

Droit des collectivités territoriales et de la sécurité privée

*augmentation de 19,3 % en un an ! »⁷ Le début de l'année 2018 connaît une nouvelle fois une hausse sensible des interventions de la gendarmerie pour des faits de rodéos (+ 19,8 %)⁸. Plus largement, en 2025, au premier semestre de l'année, « *quelque 40.200 signalements numériques ont déjà été enregistrés par la Direction nationale de la sécurité publique sur la plateforme Masecurité.fr. Soit une moyenne de 220 par jour, en augmentation de 164 % rapport à la même période de l'année précédente* »⁹.*

Bien que, ces deux dernières années, le phénomène des rodéos urbains motorisés ait connu une certaine recrudescence dans les villes comme dans les zones périurbaines, le fléau ne date pas d'hier mais semble aller de pair avec les émeutes des banlieues que connaît la France depuis maintenant trente ans. En effet, le phénomène est en réalité bien antérieur à l'année 2018. Pour preuve, à chaque embrasement de cités, le rodéo urbain est très souvent à l'origine d'un accident, impliquant scooters, petites motos, motocross souvent trafiqués, causant la mort de jeunes délinquants et déclenchant par la suite des jours et des nuits d'émeutes. Ce fut le cas, pour ne citer que quelques exemples, à Vaulx- en-Velin en octobre 1990 et à Villier-le-Bel en novembre 2007. Plus récemment et dès l'année 2012 à Marseille, de nombreux riverains de certains

7. Rapport AN n°995 du 30 mai 2018 par N. Pouzyreff sur la proposition de loi renforçant la lutte contre les rodéos urbains, p. 7.

8. *Ibid.*

9. CORNEVIN, Christophe. Rodéos urbains : la France en proie à une fièvre de violence mécanique. *Le Figaro*, 10 juillet 2025.

Droit des collectivités territoriales et de la sécurité privée

quartiers de la ville menacés par les trafics en tous genres et la grande criminalité, n'hésitent plus à porter plainte contre la plaie des incessants rodéos urbains s'y déroulant (pourtant considérés comme de petites incivilités). Une affaire emblématique jugée par le TA Marseille en 2020¹⁰ fait d'ailleurs de multiples signalements de riverains agacés et mis en danger par les rodéos sauvages de quartiers du XV^e arrondissement : « *La requérante, et d'autres personnes, ont alerté à de multiples reprises les services de l'Etat : lettres du 16 mars 2012 et du 27 mai 2016 ; pétition transmise à l'été 2017 par le collectif de résidents "Vivre au Verduron" ; nouveaux courriers en octobre 2017, janvier 2018 et août 2018 ; saisine du procureur de la République le 19 mars 2018* »¹¹. Cette affaire, emblématique d'un problème de société récurrent, se soldera par un jugement en demi-teinte (cf. *infra* III^e partie), signe qu'il était temps qu'une législation dédiée soit adoptée afin d'éradiquer ce phénomène. Là encore, le législateur a tardé à intervenir malgré un fléau se développant dès les émeutes de 2007. Cela aboutissant à une réponse législative relativement inefficace.

II) Une législation relativement inefficace

Quasiment dix années se sont écoulées entre le développement des premiers rodéos urbains ayant abouti à un embrasement de certains

¹⁰. TA Marseille, 6 juillet 2020, req n°1800819.

¹¹. TRAVARD, Jérôme. Condamnation de l'Etat pour les rodéos urbains : beaucoup de bruit...pour pas grand-chose. *AJDA*, 2020, p. 2514.

Droit des collectivités territoriales et de la sécurité privée

quartiers touchés par l'insécurité, notamment dans la banlieue parisienne, et l'adoption de la première législation dans ce domaine. Si cette première législation relative aux conditions de commercialisation et d'utilisation de certains engins motorisés¹², d'initiative parlementaire, avait déjà renforcé le cadre juridique applicable aux mini-motos, la situation devenant plus que préoccupante, une nouvelle réaction législative s'imposait. Désormais, la législation de 2018¹³ tant attendue fait de cette activité particulièrement dangereuse tant pour l'auteur que pour les riverains et les forces de l'ordre, un délit passible d'un an d'emprisonnement et de 15 000 euros d'amende, complété d'un certain nombre de circonstances aggravantes comme l'absence de permis, la consommation de stupéfiants et d'alcool ou encore la commission des faits en réunion¹⁴. Une gamme de peines complémentaires est également à disposition des magistrats, comme la suspension du permis pendant trois ans maximum ou la confiscation du véhicule. La loi de 2022¹⁵ viendra aussi compléter l'éventail législatif préexistant en doublant les pénalités encourues

¹². Loi n° 2008-491 du 26 mai 2008 relative aux conditions de commercialisation et d'utilisation de certains engins motorisés, *JO*, n° 0122 du 27 mai 2008.

¹³. Loi n° 2018-701 du 3 août 2018 renforçant la lutte contre les rodéos urbains, *op.cit.* note 2.

¹⁴. La diffusion et la promotion d'image de rodéos urbains sur les réseaux sociaux est réprimée au même niveau que l'apologie du terrorisme, cf. art. L. 236-2 3° du Code de la route.

¹⁵. Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, *JO*, n° 0020, 25 janvier.

Droit des collectivités territoriales et de la sécurité privée

lorsque le rodéo se poursuit par l'infraction du refus d'obtempérer et en mettant en place un cumul de peines entre les deux infractions¹⁶. Puis, à la faveur du vote de la Loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur (LOPMI) en 2023¹⁷, le législateur, face à un phénomène urbain semblant s'enraciner dans les quartiers dits sensibles des banlieues françaises, envisage de durcir la réponse pénale. Par cette modification législative, il s'agissait alors, en cas de rodéos exposant autrui à un risque de mort ou d'infirmité permanente, de prononcer une peine allant jusqu'à cinq ans d'emprisonnement et 75 000 euros d'amende. Néanmoins la nouvelle loi prévoyant le renforcement de l'incrimination au Code de la route ne passera pas le barrage du contrôle du Conseil constitutionnel, ce dernier y voyant la présence d'un cavalier législatif¹⁸. Pour certains, il ne fait alors guère de doute que cette tentative de renforcement de l'incrimination pénale sonnait comme « *un aveu d'impuissance de la part des autorités* »¹⁹, d'autant plus que les forces de l'ordre restaient soumises à une note interne de la direction générale de la police datant de 1999²⁰,

16. Cela revenant à dire que l'auteur d'un rodéo aggravé et d'un refus d'obtempérer peut aujourd'hui encourir jusqu'à 7 ans d'emprisonnement hors récidive.

17. Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur, JO, n° 0021, 25 janvier.

18. Cons. const. 19 janvier 2023, n° 2022-846 DC.

19. TRAVARD, Jérôme, *op. cit.* note 11.

20. Cité par Mme Eutache-Brinio dans une interview à Public Sénat. Voir : Rodéos motorisés : « La loi existe, il suffit de la faire appliquer » [en ligne]. *Public Sénat*, 9 août 2022. Disponible sur : <https://www.publicsenat.fr/actualites/non-classe/rodeos-motorises-la-loi-existe-il-suffit-de-la-faire-appliquer-217994>

Droit des collectivités territoriales et de la sécurité privée

renouvelée par une instruction de commandement du directeur central de la sécurité publique en date du 18 août 2020²¹, leur assignant de ne pas aller au contact de l'auteur du rodéo ou, à tout le moins, de ne s'engager dans une course poursuite que lorsque cette dernière s'avère proportionnée au risque encouru. En France, l'hésitation est grande à vouloir utiliser la technique bien connue Outre-Manche du *Tactical contact* britannique, alors même que le rapport d'information relatif à l'impact de la loi de 2018 souligne expressément que « *la direction centrale de la sécurité publique a indiqué [...] que le nombre de rodéos motorisés a "drastiquement baissé" depuis l'entrée en vigueur de cette méthode, qui a été plébiscitée par plusieurs des policiers auditionnés par la mission d'évaluation* »²². De plus, la réponse strictement judiciaire au problème des rodéos semblait se heurter à un manque de formation de certaines polices municipales dans la rédaction des procès-verbaux, systématiquement rejetés par les magistrats et se soldant par une relative absence de poursuite pénale.

Si la loi de 2018 semblait avoir achoppé à son but car trop dépendante de poursuites judiciaires qui n'eurent finalement pas assez lieu²³ ou d'actions policières trop restrictives, restait alors la

²¹. Rapport d'information AN n° 4434, Mme Pouzyreff et M. Reda, sur l'évaluation de l'impact de la loi du 3 août 2018 renforçant la lutte contre les rodéos motorisés, p. 38.

²². *Ibid.*, p. 36.

²³. La circulaire du 3 septembre 2018 relative à la loi n° 2018-701 du 3 août 2018 renforçant la lutte contre les rodéos motorisés (NOR : JUSD1823902C) de Nathalie Belloubet demandait d'ailleurs d'appliquer une répression pénale forte à l'égard des

Droit des collectivités territoriales et de la sécurité privée

possibilité d'engager la responsabilité administrative des décideurs publics que sont les préfets et les maires. Là encore, il a pu être relevé que « *la responsabilité administrative n'est qu'un maigre palliatif à l'inaction administrative, qui est la conséquence d'une véritable impuissance publique* »²⁴.

III) Une jurisprudence administrative en demi-teinte

Puisqu'en droit public la jurisprudence administrative est très souvent la bouche qui dit le droit, voire qui est à l'origine de jurisprudences créatrices de règles de droit, la décision du juge administratif du TA Marseille de 2020²⁵ était très attendue dans ce domaine. En effet, à la suite de nombreuses plaintes d'habitants d'un quartier de Marseille considérant que les mesures prises par les autorités administratives s'avéraient totalement inefficaces et insuffisantes à restaurer la tranquillité publique dans des lieux concernés par le déroulement régulier de rodéos motorisés, les requérants tentent d'engager la responsabilité administrative du maire ou du préfet des Bouches-du-Rhône. Il a pu être rapporté que

auteurs mais uniquement lorsqu'il s'agit des « *cas plus graves, notamment en cas de rodéos motorisés commis de nuit, par plusieurs personnes utilisant des véhicules de grande cylindrée, les poursuites pourront être exercées selon la procédure de comparution immédiate. La confiscation des véhicules utilisés, une fois prise une mesure d'immobilisation, pourra utilement être requise par les magistrats du ministère public* ».

²⁴. TRAVARD, Jérôme, *op. cit.* note 11.

²⁵. *Op.cit.* note 10.

Droit des collectivités territoriales et de la sécurité privée

le jugement était intéressant à plus d'un titre. « *Il est le premier rendu en France par les juridictions administratives sur la question des rodéos urbains et a de ce fait eu les honneurs de la presse nationale (Le Monde, 20 août 2020) et locale (Marsactu.fr, 17 août 2020)* »²⁶. En effet, il s'agissait, d'une part, de savoir qui du maire ou du préfet était responsable du point de vue administratif de cette impéritie publique à agir pour mettre un terme au fléau et, d'autre part, sur quel fondement juridique l'entité administrative pouvait être condamnée. En effet, une hésitation s'installa rapidement entre la possible responsabilité du maire pour absence de mesures prises face aux réguliers troubles de voisinage ou celle du préfet pour carence de mesures visant à faire assurer l'ordre et la tranquillité publique. Afin d'y apporter une réponse, une précision s'imposait préalablement. En effet, dans les villes à police étatisée (et c'est bien le cas pour Marseille), c'est le Préfet qui est principalement compétent pour assurer l'ordre public et prendre les mesures visant à réprimer les atteintes à la tranquillité publique. Le maire ne dispose alors plus que d'une compétence dans le cas des troubles de voisinage. Ainsi, les requérants comptaient bien sur cette compétence résiduelle pour engager la responsabilité administrative du maire sur ce fondement, les rodéos étant à l'origine de troubles de voisinage incessants. Pour autant, le TA de Marseille ne l'entendra pas de cette oreille, considérant qu'il manque le lien de proximité entre le lieu d'habitation des riverains et les auteurs de l'activité nuisible. Ainsi, comme le relève le juge à

²⁶. TRAVARD, Jérôme, *op.cit.* note 11.

Droit des collectivités territoriales et de la sécurité privée

propos des nuisances sonores, elles ne constituent pas des bruits de voisinage, dans la mesure où ces nuisances « *n'ont pas pour origine l'activité des personnes résidant à proximité du domicile de la requérante* »²⁷. Comme il a pu être noté par la doctrine, « *la requérante en effet possède sa résidence à environ 300 mètres des axes empruntés par les pratiquants de rodéos, et les auteurs de ces rodéos utilisent de manière illégale les voies publiques. Les dispositions du CGCT renvoient à des dommages permanents, réguliers, liés à une activité en proximité avec les résidences des riverains, ou accidentels* »²⁸. Faute d'avoir pu démontrer le lien de proximité nécessaire à la qualification du trouble de voisinage, le maire ne voit donc pas sa responsabilité administrative engagée pour défaut de mesures visant à mettre un terme à ce trouble. Ne restait alors qu'à se rabattre sur l'entité préfectorale et préciser le fondement et la nature de sa responsabilité administrative. C'est ce que fit le tribunal puisque, faute de mesures adéquates prises pour mettre un terme aux nuisances, la carence entraîne la responsabilité administrative du Préfet, pour faute simple. Ainsi, « *les mesures entreprises par le préfet de police des Bouches-du-Rhône afin de mettre fin aux rodéos motorisés responsables d'atteintes à la tranquillité publique ne peuvent être considérées comme suffisantes eu égard à l'ampleur et à persistance de ce phénomène. Si l'interpellation des conducteurs des engins présente un danger pour*

²⁷. TA Marseille, 6 juill. 2020, *Mme L c/ Cne de Marseille*, req n°1800819.

²⁸. PAULIAT, Hélène. Rodéos urbains motorisés : la responsabilité de l'Etat engagée pour faute. *JCP A*, n° 35, août 2020, 2231.

Droit des collectivités territoriales et de la sécurité privée

ces personnes, pour les agents de police ainsi que pour les autres usagers, cette circonstance n'exonère pas les services compétents de leur obligation de prendre des mesures appropriées pour assurer un niveau raisonnable de tranquillité publique »²⁹. Le jugement en profite pour confirmer l'abandon de la faute lourde en matière d'insuffisance et d'inadaptation des mesures de police. À l'inverse pourtant, un arrêt récent de la cour administrative d'appel de Lyon d'avril 2024³⁰, pour des mêmes faits reprochés de carence du Préfet dans le rétablissement de la tranquillité publique troublée par divers agissements, dont des rodéos urbains motorisés en plein centre de la ville de Lyon, semble ne pas poursuivre la logique du jugement de Marseille. En effet, deux points mis en exergue par la cour et aux conclusions contraires de son rapporteur public aboutissent à un rejet de la responsabilité administrative pour faute du Préfet du Rhône. D'une part, le juge estime que, s'agissant d'agissements entrant dans le cadre de la police judiciaire, la compétence du juge administratif doit être partiellement rejetée. D'autre part, concernant une éventuelle responsabilité administrative du Préfet, celle-ci est rejetée, car ce dernier aurait mobilisé les moyens et actions nécessaires ne pouvant aboutir en l'espèce à aucune carence fautive.

Au contraire, conscients de cet état de déficience publique à agir contre ce fléau, certains maires, dont ceux de Valence ou de Compiègne, ont décidé de réagir et d'appliquer une sorte de

²⁹. Jugement TA Marseille, 6 juillet 2020.

³⁰. CAA Lyon, 22 avril 2024, req n° 22LY00245.

Droit des collectivités territoriales et de la sécurité privée

méthode communale innovante s'inscrivant directement dans le *continuum* de sécurité. Si le volet judiciaire et pénal contenu à la loi de 2018 est appliqué, il est aussi relayé immédiatement, par exemple à Valence, par des arrêtés municipaux autorisant systématiquement l'enlèvement des véhicules, voire leur saisie et leur destruction, avec une amende en cas de dégradation du domaine public. Des équipes de policiers municipaux directement affectées à la problématique travaillent de concert avec la police nationale en utilisant le plus possible la vidéoprotection et désormais les drones, pour l'identification sur un travail de long terme des auteurs de ces actes, dans le but de mener des actions préventives sur le terrain. Les résultats semblent être là, car la ville de Valence connaît une baisse drastique du nombre de rodéos et, par conséquent, du nombre de plaintes de ses habitants³¹.

Au-delà, le ministre de l'Intérieur, Bruno Retailleau, appelle de ses vœux ce changement de paradigme avec en perspective l'application d'une nouvelle doctrine d'action en généralisant les poursuites directement au contact des auteurs de rodéos urbains tant pour la police que pour la gendarmerie. Gageons également que la loi de juillet 2025 relative à l'homicide routier³² puisse

³¹. Par exemple, les signalements sont passés de 550 en 2021 à 7 en 2025. Voir : VILLE DE VALENCE. Rodéos urbains et runs sauvages : à Valence, 150 motos détruites, la sécurité retrouvée grâce à une politique d'actions volontariste et des dispositifs innovants [en ligne]. *Communiqué de presse*, 19 juin 2025. Disponible sur : https://www.valence.fr/app/uploads/2025/07/2025-06-19_ValenceCPRodeosUrbains.pdf

³². Loi n° 2025-622 du 9 juillet 2025 créant l'homicide routier et visant à lutter

Droit des collectivités territoriales et de la sécurité privée

permettre d'avoir un effet positif sur l'éradication ou, tout du moins, une baisse du nombre de ces fléaux urbains, car le cas des rodéos est explicitement intégré dans cette loi comme circonstance aggravante permettant de caractériser l'infraction d'homicide routier (au même titre que le refus d'obtempérer ou encore la consommation de drogue, d'alcool ou la conduite sans permis). Puisque l'arsenal législatif est désormais complet, il ne reste plus qu'à mobiliser les moyens afin d'accroître la prévention, le contrôle et la répression, comme l'ont déjà fait certains maires.

contre la violence routière, *JO*, n° 0159, 10 juillet 2025. Voir également, *supra*, la rubrique « Actualité pénale » consacrée à cette Loi, p. 62.

Actualité institutionnelle européenne

Pierre BERTHELET

L'Europe de la sécurité intérieure

Synthèse législative et institutionnelle (printemps - été 2025)

C'est encore un agenda très dense. Les agences dites « JAI » (Justice et Affaires intérieures) ont publié chacune un ou plusieurs rapports : Eurojust (rapport d'activité), Europol (sur l'état de la menace terroriste – TE-SAT – ou sur l'état de la cybercriminalité – iOCTA) et Frontex (Analyse annuelle de risque). En parallèle, le Conseil de l'Union européenne (UE) a approuvé une série de conclusions lors de sa dernière réunion en format « Justice et affaires intérieures » tenue au mois de juin 2025. Quant à la Commission européenne, elle a aussi présenté plusieurs textes qui méritent l'attention : bilan d'étape du déploiement du Pacte sur la migration et l'asile, bilan annuel Schengen, bilan en matière de protection civile européenne et communication sur l'interception des communications. Tous ces documents seront présentés de manière organisée autour de cinq pôles, à savoir les frontières Schengen (1), le trafic de drogue et d'armes (2), la lutte antiterroriste (3), la coopération policière et judiciaire (4) et le *continuum* de sécurité (5), cela afin de couvrir la protection civile et la gestion des menaces dans le domaine nucléaire, radiologique, biologique, chimique et explosif (NRBC-E ou CBRN-E).

Actualité institutionnelle européenne

I) Frontières Schengen : flux et faiblesses

Le récent rapport annuel de Frontex, publié le 3 juin 2025, concernant l'évaluation des risques (*Annual Risk Analysis - ARA*)¹ sur la pression migratoire actuelle et future met en évidence le fait que **les flux migratoires ne devraient pas diminuer**. Ils pourraient d'ailleurs augmenter en raison de l'instabilité politique dans les régions périphériques de l'UE, voire au-delà, associée à une tentative d'utilisation de la migration par des États hostiles tels que la Russie et la Biélorussie. Un élément aggravant de la situation est la croissance de la criminalité transnationale, en particulier dans la région des Balkans occidentaux. Selon les informations fournies par Frontex, les voies migratoires reliant la Méditerranée occidentale et l'Afrique de l'Ouest demeurent les principaux points d'accès à l'UE, en raison des défis économiques, des conflits et de la présence de réseaux de criminalité organisée. La Méditerranée occidentale demeure un axe crucial pour le trafic de stupéfiants, en particulier de haschisch et de cannabis, de l'Afrique du Nord vers l'Espagne. La voie terrestre reliant l'Afrique de l'Ouest aux îles Canaries est, quant à elle, un itinéraire clé pour atteindre l'Espagne continentale.

Face à cette situation, les travaux concernant le Pacte sur la migration et l'asile progressent à bon train. Un rapport de la Commission, présenté le 6 juin 2025, dressant un état de la situation

¹. FRONTEX. *Annual Risk Analysis 2025/2026*, Luxembourg: Publications Office of the European Union, mai 2025.

Actualité institutionnelle européenne

à mi-parcours², souligne les avancées significatives, notamment en ce qui concerne le système Eurodac (qui est un système d'information à grande échelle contenant les empreintes digitales, notamment des demandeurs d'asile et des immigrants illégaux) ou les mécanismes de retour. Pour mémoire, les dispositions législatives du Pacte sont devenues effectives le 11 juin 2024 et entreront en vigueur à partir de la mi-2026. En juin 2024, la Commission a approuvé le plan conjoint pour sa mise en œuvre. Ce plan, détaillant les principales missions et étapes de cette phase de transition, est actuellement en cours de mise en œuvre et le rapport intermédiaire fait état de son application.

Reste que le rapport intermédiaire met en évidence des défis à relever, par exemple la nécessité de disposer d'infrastructures pour la procédure de tri aux frontières entre les demandeurs d'asile éligibles à une protection et les autres qui doivent être expulsés rapidement.

Selon ce rapport, les États membres doivent également corriger les inefficacités internes actuelles, tels un manque de coordination entre les autorités et l'existence de procédures excessivement complexes, pour assurer une procédure efficace de retour aux frontières telle que nouvellement créée dans le cadre du Pacte.

Dans le même sens, le rapport annuel sur la situation de l'espace Schengen, présenté par la Commission le 24 avril 2025, pointe le

². COMMISSION EUROPÉENNE. *State of play on the implementation of the Pact on Migration and Asylum* (COM(2025) 319 Final).

Actualité institutionnelle européenne

fait que de nombreuses lacunes subsistent dans plusieurs pays de l'espace Schengen, même des années après la réalisation de leurs évaluations, et bon nombre de ces lacunes portent sur des aspects essentiels du cadre Schengen³. En effet, l'ensemble des pays membres de l'espace Schengen ont initié des démarches internes de réexamen de leurs stratégies. Cependant, des manques importants demeurent dans la planification des ressources humaines, la coordination entre les institutions et les mécanismes financiers. De telles lacunes affectent particulièrement les contrôles aux frontières. Les évaluations Schengen révèlent que presque la moitié des États membres de l'espace Schengen rencontrent des déficiences en termes de ressources humaines, de formation, de mise en œuvre des procédures de contrôle aux frontières, ainsi que des problèmes techniques impactant le bon fonctionnement des équipements informatiques, notamment lors de l'utilisation du Système d'information Schengen. Selon le rapport, la persistance de ces déficiences représente une vulnérabilité majeure en matière de sécurité pour l'espace Schengen. Fait aggravant, **la France fait partie**, aux côtés de la Grèce et la Hongrie, **des trois pays membres de l'espace Schengen qui continuent à présenter des lacunes significatives** dans l'application des normes Schengen.

³. COMMISSION EUROPÉENNE. *Rapport 2025 sur la situation dans l'espace Schengen*. COM(2025) 185 final.

Actualité institutionnelle européenne

II) Trafic de drogue et d'armes : une priorité pour la sécurité intérieure européenne

La question des drogues est non seulement à l'agenda politique français, mais aussi européen. Observant le fait que les substances illicites, notamment les drogues de synthèse et les nouvelles substances psychoactives (NSP), ont des conséquences dévastatrices en Europe, le Conseil de l'Union européenne a adopté le 12 juin 2025, des conclusions exhortant les États membres à intensifier leurs efforts pour lutter contre ce problème⁴. Il sollicite la Commission européenne pour qu'elle envisage une révision du cadre juridique relatif aux précurseurs de drogues et aux NSP. En ce qui concerne les agences européennes, notamment Europol et l'Agence de l'Union européenne sur les drogues (EUDA), celles-ci sont également mises à contribution. Le Conseil recommande aux États membres de renforcer la surveillance de la prescription des médicaments opioïdes autorisés afin de prévenir toute forme de détournement. De plus, il encourage les États membres à intensifier leurs actions pour surveiller, geler et saisir les produits du crime, notamment les cryptomonnaies, issus du trafic de drogues de synthèse, de NSP et de pré-précurseurs.

Le trafic d'armes, en particulier l'usage d'armes 3D et de feux d'artifices, constitue également une priorité politique en matière de

⁴. CONSEIL DE L'UE. Conclusions sur le pacte visant à lutter contre les menaces liées aux nouvelles drogues de synthèse et aux nouvelles substances psychoactives dans l'Union européenne, doc. du Conseil n° 10265/25 du 13 juin 2025.

Actualité institutionnelle européenne

sécurité intérieure. Devant la menace que constitue la propagation des armes à feu au sein de l'UE, les ministres de l'Intérieur du Conseil ont approuvé des conclusions le 12 juin 2025, visant à renforcer le cadre législatif⁵. Plus exactement, ils préconisent d'examiner la pertinence d'amender la législation de l'UE pour opérer une modification de la classification des articles pyrotechniques. Ils entendent par ailleurs améliorer l'intégration des données dans le pôle « armes à feu » d'Europol. Cette démarche viserait à établir un référentiel européen unifié et à prévenir la duplication des systèmes. De surcroît, ils recommandent aux États membres d'améliorer leur collaboration tant entre eux qu'avec les pays extérieurs à l'UE, l'élaboration d'une stratégie à long terme pour combattre le trafic d'armes avec l'Ukraine ainsi que l'optimisation du système d'information Schengen.

III) Terrorisme : rajeunissement des auteurs et usage des technologies innovantes

Le rapport de 2025 sur la situation et les tendances du terrorisme dans l'UE (EU TE-SAT) met en lumière les évolutions majeures et les tendances clés de la menace terroriste au sein de l'UE en 2024⁶. Au

⁵. CONSEIL DE L'UE. Conclusions sur la lutte contre le trafic d'armes et les menaces découlant des armes à feu et des articles pyrotechniques, doc. du Conseil n° 9907/25 du 12 juin 2025.

⁶. EUROPOL. *EU Terrorism Situation & Trend Report (EU TE-SAT) - Reviewing the terrorism phenomenon*, juin 2025.

Actualité institutionnelle européenne

cours de cette année, 58 actes terroristes ont été répertoriés dans l'UE ; **24 sont attribués au terrorisme djihadiste, ce chiffre marquant une hausse notable** par rapport aux 14 attentats recensés en 2023. La majorité de ces actes ont été commis par des individus agissant seuls (20 sur 24). Sur les 58 attentats répertoriés, la majorité d'entre eux se sont déroulées en Italie (20) et en France (14).

Au total, 449 individus ont été appréhendés. Il s'agit d'un chiffre en hausse par rapport à 2023 (426) et 2022 (380). La majorité des interpellations ont été effectuées en Espagne (90) et en France (69).

Fait notable, la personne la plus jeune à avoir été arrêtée était âgée de 12 ans et était inculpée pour son adhésion à une idéologie d'extrême droite. De manière plus générale, Europol observe que **l'engagement de mineurs représente une tendance préoccupante**. En effet, parmi les 449 suspects appréhendés en 2024, 133 se situaient dans la tranche d'âge de 12 à 20 ans.

Une autre problématique importante soulevée porte sur **l'utilisation des technologies innovantes, en premier lieu l'intelligence artificielle**, qui offrent de nouvelles opportunités en termes de recrutement, de propagande, de méthodes opérationnelles et d'instruments de financement. Europol indique que les technologies de pointe modifient le panorama des risques, remettant en question les approches traditionnelles des services de lutte contre le terrorisme. Autre fait remarquable, Europol note l'entrelacement de plus en plus étroit entre les sphères numériques et physiques de la vie des individus. Cette interconnexion conduit inévitablement à une transition de la radicalisation en ligne vers des

Actualité institutionnelle européenne

actes de violence dans la réalité matérielle.

IV) Intensification de la coopération policière et judiciaire

Le dernier rapport annuel d'activité d'Eurojust révèle des chiffres qui méritent l'attention : 13 000 dossiers traités, 1 200 suspects appréhendés et 1 milliard d'euros saisis⁷. De plus, 20 milliards d'euros de drogue l'ont été. Qui plus est, les enquêtes ont impliqué plus de trois fois plus de victimes par rapport à l'année précédente, sans compter le fait d'une augmentation de 25 % des équipes communes d'enquête. En tout et pour tout, la charge de travail de l'agence de coopération judiciaire a augmenté de plus de 60 % en cinq ans. D'autres aspects méritent d'être soulignés dans ce récent rapport d'activité, notamment le traitement prépondérant des affaires liées au trafic de drogue et à la criminalité financière par Eurojust. De plus, la cybercriminalité constitue l'un des cinq principaux domaines de criminalité traités par cette agence.

EMPACT est pour sa part un vaste projet de coopération policière de l'UE en expansion, et les conclusions adoptées par le Conseil de l'UE le 13 juin 2025, en définissent les orientations stratégiques⁸.

Pour mémoire, EMPACT est un cadre opérationnel permanent de l'UE pour lutter contre la grande criminalité organisée. La stratégie

⁷. EUROJUST. *Consolidated Annual Activity Report 2024*, 3 juillet 2025.

⁸. CONSEIL DE L'UE. Conclusions sur le renforcement de l'EMPACT et sur les priorités de l'UE en matière de criminalité pour le prochain cycle de l'EMPACT 2026-2029, doc. du Conseil n° 9397/25 du 13 juin 2025.

Actualité institutionnelle européenne

européenne de sécurité intérieure souligne que le prochain cycle d'EMPACT, à savoir celui pour la période 2026-2029, offre une opportunité pour consolider davantage ce cadre, en rationalisant les actions et en renforçant les engagements des États membres. Les conclusions se divisent en deux parties, la première se concentrant sur l'amélioration d'EMPACT. Le constat dressé dans les conclusions est que le manque de ressources financières allouées à l'EMPACT actuellement constitue un obstacle majeur entravant sa croissance et son expansion. Les aspects fondamentaux concernent donc un financement durable. Ils portent également sur une communication améliorée ayant trait au projet ainsi que sur une participation élargie, notamment envers les pays partenaires de l'UE. Quant à la deuxième partie, elle concerne l'établissement des priorités de l'UE en matière de criminalité pour la période 2026-2029. Une de ces priorités se distingue particulièrement des autres, à savoir celle portant sur **les réseaux criminels et délinquants les plus dangereux**⁹. Il s'agit dès lors de concentrer les efforts sur la collecte de renseignements sur les réseaux et les individus concernés, ainsi que sur la cartographie d'Europol.

Le numérique est un défi pour les services répressifs et de renseignement, en matière de lutte non seulement contre le terrorisme, mais aussi contre la criminalité. Les communications chiffrées offrent une protection aux criminels contre toute

⁹. Voir, à ce propos, le rapport d'Europol dénommé « *Decoding the EU's most threatening criminal networks* », du 5 avril 2024.

Actualité institutionnelle européenne

interception par ces services. Fait aggravant, les solutions proposées par les entreprises privées sont souvent onéreuses et ne correspondent pas toujours aux exigences de ces services devant gérer un grand volume de données sans toujours disposer des ressources adéquates pour le faire. Dans un tel contexte, la Commission a publié, le 24 juin 2025, une communication détaillant les actions à entreprendre¹⁰, telles que **l'élaboration d'une législation européenne sur la rétention des communications à des fins policières, le recours à l'intelligence artificielle pour l'analyse des mégadonnées, l'utilisation de la cryptographie post-quantique** pour contourner le chiffrement, ainsi que le renforcement des capacités d'Europol dans le domaine de la criminalistique numérique.

La Commission propose d'améliorer l'efficacité des demandes transfrontalières d'interception légale, d'une part, en renforçant si nécessaire, la décision d'enquête européenne d'ici 2027 et, d'autre part, en déployant un arsenal juridique à l'encontre des fournisseurs de services de communication qui se montrent récalcitrants. De surcroît, elle apportera son soutien à la recherche et au développement de nouvelles capacités de déchiffrement afin de garantir qu'Europol dispose des équipements nécessaires après 2030 pour assister les États membres, au vu des récentes avancées technologiques et des recherches de pointe dans ce domaine.

¹⁰. COM(2025) 349 final.

Actualité institutionnelle européenne

5. *Continuum de sécurité*: de gestion des menaces NRBC-E à celle des feux de forêts

Pour ce qui est de la protection civile, la Commission européenne a présenté un rapport qui dresse un bilan des progrès dans ce domaine. Il met l'accent sur les avancées réalisées en termes de capacités de réaction dans le domaine de la protection civile européenne et propose plusieurs recommandations, telles que l'élaboration d'indicateurs de performance et le renforcement du partenariat public-privé.

Il indique, en outre, que la diversité des risques et des menaces auxquels l'Europe est confrontée nécessite une adaptation constante des outils du Mécanisme de protection civile de l'Union européenne (MPCU) pour faire face à des situations imprévues, en fournissant une assistance aux États membres et participants. La Réserve européenne de protection civile est considérée comme l'un des éléments essentiels de la capacité de réaction du MPCU, symbolisant l'engagement des États membres à manifester leur solidarité en cas de catastrophe. En général, les déploiements de la réserve constituent environ 25% des capacités déployées lors des activations du MPCU.

Bien que de nombreuses avancées aient été constatées, ce rapport souligne également divers manques, notamment en matière de capacités de soutien spécialisé, en particulier dans le domaine NRBC (nucléaire, radiologique, biologique et chimique), ou dans le domaine de l'expertise médicale spécialisée.

En outre, **les capacités de lutte aérienne contre les incendies de**

Actualité institutionnelle européenne

forêt restent insuffisamment prises en compte en ce qui concerne les capacités répertoriées de la Réserve européenne de protection civile, avec une absence totale de modules basés sur l'utilisation d'hélicoptères.

Par ailleurs, les grands rassemblements tels que les Jeux Olympiques de Paris 2024 ont souligné l'importance de garantir la sécurité. Diverses menaces pèsent sur les événements de grande envergure, dont certaines comportent des risques dans les domaines NRBC-E (ou CBRN-E). C'est le cas de l'explosion d'un engin explosif improvisé lors d'un festival. Dans ce contexte, les ministres de l'Intérieur du Conseil ont approuvé, le 12 juin 2025, des conclusions visant à améliorer la recherche et le développement technologiques, ainsi que les compétences requises pour élaborer des plans et des procédures de réponse aux incidents CBRN-E¹¹. Il est envisagé de mettre en place une plateforme européenne dédiée aux échanges d'expérience. Ces conclusions traitent de divers aspects tels que l'amélioration de la coordination ou l'élaboration de lignes directrices. La formation est néanmoins la principale priorité. Le Conseil recommande aux États membres de développer un programme de formation CBRN-E en prenant en considération celles déjà disponibles, comme le projet Melody, qui est un programme européen de formation CBRN harmonisé pour les premiers intervenants et le personnel médical.

¹¹. CONSEIL DE L'UE. Conclusions sur la lutte contre les risques chimiques, biologiques, radiologiques, nucléaires et explosifs (CBRN-E) lors d'événements de masse, en particulier d'événements sportifs de masse, doc. du Conseil n° 9908/25 du 12 juin 2025.

Rédacteurs

- **Le Général d'armée (2S) Marc Watin-Augouard** est ancien directeur du CRGN et fondateur du FIC (Forum InCyber)
- **Nathan Allix** est magistrat, docteur en droit privé
- **Marc-Antoine Granger** est maître de conférences HDR en droit public à l'Université Côte d'Azur, 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'AFDSD
- **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
- **Florence Nicoud** est Professeur de droit public à l'Université Côte d'Azur, membre du CERDACFF, de l'AFDSD et co-directrice du Master II Sécurité Intérieure
- **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.