



LA RÉVOLUTION TECHNOLOGIQUE AU SERVICE DES ACTEURS DU CONTINUUM DE SÉCURITÉ ET DE JUSTICE



Perception des Français
et regards d'experts

Guillaume FARDE



Sécurité, Société, Justice

LE THINK TANK DES MÉTIERS DE LA SÉCURITÉ ET DE LA JUSTICE

Le Continuum Lab est un think tank initié par INTÉRIALE en mai 2021, aux côtés de six autres membres fondateurs. Lieu d'échange et de dialogue, il a pour ambition d'être force de propositions pour favoriser la qualité de vie au travail et l'exercice des métiers des agents publics et privés qui concourent à la sécurité intérieure ainsi que d'alimenter le débat public sur les sujets de société en lien avec les métiers de la sécurité et de la justice.

Le Continuum Lab regroupe l'ensemble des métiers liés au continuum de sécurité et de justice : police nationale, gendarmerie nationale, police municipale, sapeurs-pompiers, surveillants et responsables de l'administration pénitentiaire, préfets, entreprises de sécurité privée, responsables de collectivités territoriales, élus et acteurs de la justice.

Les organismes fondateurs et les membres
du conseil d'administration du Continuum Lab



Pilotage scientifique de l'étude

SciencesPo
CEVIPOF

MÉTHODOLOGIE

L'étude présentée dans cet ouvrage est destinée à comprendre et analyser les connaissances et l'opinion des Français sur les technologies de sécurité et leur impact dans la société. Elle s'appuie sur un sondage OpinionWay pour le Centre de recherches politiques de Sciences Po (Cevipof) et le Continuum Lab (groupe INTÉRIALE).

Celui-ci a été mené auprès d'un large échantillon composé de 3 438 personnes, représentatif de la population française âgée de 18 à 75 ans, constitué selon la méthode des quotas, au regard des critères de sexe, d'âge, de catégorie socioprofessionnelle, de catégorie d'agglomération et de région de résidence.

Les interviews ont été réalisées du 18 au 26 juin 2024, par questionnaire autoadministré en ligne sur le système *Computer assisted web interview* (CAWI).

SOMMAIRE

PRÉFACE	Page 4
INTRODUCTION	Page 8
I. LA CONNAISSANCE DES TECHNOLOGIES DE SÉCURITÉ	Page 19
II. LES CAS D'USAGE ET LES UTILISATEURS	Page 31
III. LES POLITIQUES PUBLIQUES DE SÉCURITÉ	Page 59
PAROLES D'EXPERT DE LA SÉCURITÉ CIVILE	Page 67
PAROLE D'EXPERTS DE LA SÉCURITÉ PUBLIQUE	Page 79
CONCLUSION	Page 88
ÉCLAIRAGE D'EXPERTS	Page 91
LES PROPOSITIONS DU CONTINUUM LAB	Page 101



Gilles BACHELIER

Président du Continuum Lab
et du groupe INTÉRIALE

Le Continuum Lab, proche du terrain et de ses besoins

Les Jeux olympiques et paralympiques de Paris 2024 ont rassemblé des millions de spectateurs. Cet événement mondial a été l'occasion de tester de nouvelles technologies de sécurité. Mais l'innovation ne doit pas se limiter à ces grands rendez-vous : elle est indispensable chaque jour pour tous les acteurs de la sécurité et de la justice.

Le Continuum Lab s'inscrit dans cette logique. C'est un lieu de confiance où les professionnels de la sécurité et de la justice peuvent se rencontrer, partager leurs expériences et imaginer des solutions ensemble.

En juillet 2024, juste avant les Jeux, nous avons mené avec OpinionWay et le Centre de recherches politiques de Sciences Po (Cevipof) une enquête sur la confiance des Français envers les technologies de sécurité. C'était la première étude de cette ampleur. Elle montre que les Français font confiance à ces technologies, à condition qu'elles soient utilisées par des acteurs publics et encadrées strictement.

Ces innovations ne remplacent pas l'humain. Au contraire, elles soutiennent le travail des femmes et des hommes sur le terrain. Elles rendent leurs missions plus efficaces, améliorent leurs conditions de travail et attirent de nouveaux professionnels. Par exemple, les centres de supervision urbaine comme le Centre de coordination opérationnelle de sécurité (CCOS) de la Préfecture de police de Paris facilitent les interpellations.

De même, la lutte contre la cybercriminalité progresse grâce à ces outils. L'innovation permet donc aux agents de se concentrer sur l'essentiel de leur métier, en les déchargeant des tâches répétitives et administratives.

Cet ouvrage ne se contente pas d'analyser les résultats de l'étude. Il s'appuie aussi sur les travaux d'un groupe réuni au Continuum Lab entre janvier et octobre 2025. Deux propositions en ressortent :

1. Assouplir le droit à l'expérimentation prévu par la Constitution, pour tester plus facilement de nouvelles solutions sur le terrain, tout en gardant un cadre clair et contrôlé ;

2. Créer un fonds de soutien aux collectivités, pour les aider à financer ces innovations, avec l'appui de financements européens, régionaux ou pilotés par le ministère de l'Intérieur et les préfetures.

Ces deux mesures offriraient aux acteurs locaux un meilleur cadre pour innover et les moyens d'investir dans les technologies nécessaires, au service de la sécurité et de la justice.

Enfin, je souhaite remercier toutes les personnalités qui ont accepté de témoigner dans cet ouvrage :

- Gérald Darmanin, ministre d'État, garde des Sceaux, ministre de la Justice ;
- François-Noël Buffet, ministre auprès du ministre de l'Intérieur ;
- Louis Laugier, directeur général de la police nationale ;
- Laurent Nuñez, préfet de police de Paris ;
- Marc Boget, directeur de l'Agence du numérique des forces de sécurité intérieure (Anfsi) ;
- Bruno Maestracci, contrôleur général de sapeurs-pompiers, directeur du Service départemental d'incendie et de secours de la Seine-et-Marne (77) ;
- Philippe Latombe, député de la Vendée (85) ;

- Jean-Paul Jeandon, maire de Cergy-Pontoise (95) et coprésident de la commission Prévention de la délinquance et sécurité de l'Association des maires de France (AMF).

Mes remerciements vont aussi à Olivier Renaudie, professeur de droit public à l'université Paris 1 Panthéon-Sorbonne et à Caroline Lequesne, maîtresse de conférences en droit public à l'université Côte d'Azur.

Gilles BACHELIER est fonctionnaire de police et mutualiste depuis plus de 30 ans. Il est diplômé de la Sorbonne et de l'École supérieure des sciences économiques et commerciales (Essec). Président D'INTÉRIALE depuis octobre 2018, il préside également le *think tank* Continuum Lab, fondé en 2021 aux côtés de six autres membres fondateurs. Administrateur de la Mutualité française depuis 2018, président de sa commission nationale de formation depuis 2020 et représentant à l'Union nationale des organismes d'assurance maladie complémentaire (Unocam), il a été réélu 1^{er} vice-président du Système fédéral de garantie jusqu'en 2027. Il est enfin membre associé de l'Association des hauts fonctionnaires de la police nationale.



Laurent MICHEL

Directeur du Continuum Lab et directeur des affaires publiques d'INTÉRIALE

« Une enquête qui dévoile une réelle et massive confiance des Français dans les technologies de sécurité. »

Les acteurs du continuum de sécurité – police nationale, gendarmerie nationale, police municipale et administration pénitentiaire, sans oublier la sécurité civile pour ne parler que des acteurs publics – recourent de plus en plus fréquemment à de nouvelles technologies. C'est le cas également, depuis quelques années, des entreprises de sécurité privée, dont certaines sont d'ailleurs essentiellement spécialisées dans ce domaine.

Nos forces de sécurité intérieure sont désormais confrontées à une véritable révolution : celle de l'utilisation des technologies de sécurité pour faire face aux nouvelles formes de criminalité et de délinquance, mais aussi pour garder une longueur d'avance sur la grande criminalité mondialisée.

Encore tout récemment, la résolution d'un enlèvement et d'une prise d'otages n'a pu trouver un dénouement rapide et

heureux que grâce à l'utilisation par nos services de police et de gendarmerie de technologies très pointues qui ont permis la détection et l'interpellation des auteurs. S'il fallait un symbole pour illustrer cette révolution des technologies de sécurité à laquelle sont confrontés nos services de sécurité intérieure, il se trouve dans la répartition des crédits de la Lopmi* votée le 24 janvier 2023 : près de la moitié du budget de cette loi est consacré à la « révolution numérique » du ministère de l'Intérieur et à la modernisation des moyens de lutte contre la cybercriminalité.

Le Continuum Lab a donc jugé primordial, au début des Jeux olympiques et paralympiques (JOP) 2024, de demander leur avis aux Français sur leur niveau de connaissance et d'acceptation de ces technologies, qui cache un véritable paradoxe. D'une part, ces technologies améliorent considérablement la sécurité et donc, la liberté d'aller et venir de nos concitoyens et des acteurs écono-

miques. Mais elles peuvent aussi, en dehors de contrôles appropriés, se révéler comme attentatoires à certaines de nos libertés.

Les résultats de cette enquête inédite en France dévoilent une réelle et massive confiance des Français dans ces technologies de sécurité. Ils indiquent également une forte demande de pédagogie et attente en matière d'information, notamment vis-à-vis de l'utilisation des technologies les plus innovantes. Enfin, dernier enseignement majeur de notre enquête : les Français sont enclins à faire confiance en priorité aux acteurs publics de la sécurité et de la justice dans l'utilisation de ces technologies.

* Loi d'orientation et de programmation du ministère de l'Intérieur.

Laurent MICHEL est directeur des affaires publiques d'INTÉRIALE et directeur du Continuum Lab dont il pilote l'équipe opérationnelle. Juriste de formation (titulaire d'une maîtrise de droit public et d'un diplôme d'études approfondies – DEA – de science politique à l'université Paris 2 Panthéon-Assas), il a exercé au cabinet du ministre de l'Intérieur, auprès de parlementaires et de présidents de conseils départementaux. Entré chez INTÉRIALE en 2011 comme directeur de cabinet du président, il y devient ensuite directeur des affaires publiques. Auditeur de la 27^e session nationale « Sécurité et Justice » de l'Institut national des hautes études de la sécurité et de la justice (INHESJ) en 2015-2016 et de la 3^e session « Citoyenneté et valeurs de la République » de l'Institut des hautes études du ministère de l'Intérieur (IHEMI) en 2024, il enseigne la communication d'influence et la gestion des crises au sein du master Manager des institutions et des affaires publiques – MIAP (Hautes études internationales et politiques – HEIP).



Guillaume FARDE

est docteur en sciences de gestion
et professeur affilié à l'École d'affaires publiques
de Sciences Po. Spécialiste des questions de sécurité
intérieure, il est l'auteur de plusieurs ouvrages,
dont *La lutte antiterroriste* (PUF, 2023)
coécrit avec Bernard Cazeneuve.
Associé fondateur du cabinet Fidelis et associés,
il dispose de près de 15 ans d'expérience
dans le conseil en sûreté.
Consultant police justice pour TF1 et LCI,
il est également chevalier
de l'ordre national du Mérite.

INTRODUCTION

En France, les technologies de sécurité constituent un objet ambivalent. Indispensables à l'efficacité des forces de l'ordre pour les uns, attentatoires aux libertés fondamentales pour les autres, le clivage est ancien. Déjà en 1995, la nature du suffixe (protection ou surveillance) appelé à qualifier la captation de vidéos sur la voie publique était fermement débattue avant que la loi d'orientation et de programmation pour la performance de la sécurité intérieure (Loppsi) de 2011 ne tranche définitivement la question.

Depuis, aucune grande loi relative aux technologies de sécurité n'a échappé aux tensions charriées par le couple libertés/sécurité ; ni la loi renseignement de 2015, ni celle de 2021, ni, encore moins, la loi Jeux olympiques (JO) de 2024 qui autorise l'expérimentation de l'analyse algorithmique des images captées dans l'espace public.

Dans ce contexte, l'enquête réalisée par le Continuum Lab, sous le patronage du Centre de recherches politiques de Sciences Po (Cevipof) et en partenariat avec OpinionWay, permet de porter un regard plus distancié sur les technologies de sécurité, loin des postures et des antagonismes idéologiques.

Entièrement tourné vers l'étude de l'opinion, ce travail de recherche livre

trois enseignements majeurs : le premier est celui du niveau de confiance élevé des Français dans les technologies de sécurité et ce, indépendamment des affinités partisans. Plus des deux tiers des Français approuvent ainsi la présence de caméras sur la voie publique (y compris le recours à des algorithmes !) quelles que soient leurs inclinations politiques ; les variations de niveau de confiance étant plus volontiers générationnelles.

Le deuxième enseignement est celui d'une corrélation croissante entre l'antériorité du déploiement d'une technologie de sécurité et le niveau de confiance dont elle est créditée : le temps aide à l'acceptation sociale et les controverses d'hier ne sont clairement plus celles d'aujourd'hui.

Pour autant, et c'est là le troisième enseignement majeur, jamais les Français ne donnent un blanc-seing : favorables aux technologies de sécurité par nature, ils n'en restent pas moins attachés à un contrôle de leur emploi – preuve, s'il en était besoin, que la distinction entre l'outil et son usage se fait naturellement et avec bon sens.

Voilà donc les principaux enseignements de ces travaux qui ne manqueront pas d'alimenter les travaux parlementaires à venir. ■



Gérald DARMANIN

Ministre d'État,
garde des Sceaux,
ministre de la Justice

Dans notre société traversée par l'incertitude, la sécurité n'est plus un simple besoin, elle devient une exigence partagée. Cette exigence, ce sont les citoyens Français, mais aussi celles et ceux qui l'assurent quotidiennement – policiers, gendarmes, magistrats – qui l'expriment de la manière la plus claire. Selon la dernière enquête du Continuum Lab, 87 % des Français déclarent que la vidéoprotection constitue pour eux un outil incontournable. Plus encore, la majorité d'entre eux souligne aujourd'hui combien ces technologies renforcent la chaîne de preuve et l'efficacité de l'action judiciaire, au bénéfice de toutes les victimes.

Que révèlent ces chiffres ? Avant tout une réalité trop souvent méconnue : la sécurité est une construction collective où la justice joue un rôle moteur. Si la vidéoprotection est plébiscitée, ce n'est pas par goût du contrôle, mais parce que chaque image peut permettre de dissiper un doute, de protéger une victime ou de confondre un auteur de violences. Le monde judiciaire, parfois décrit comme prudent vis-à-vis de la technologie,

s'approprie désormais ces outils, gage d'une adaptation intelligente aux nouveaux défis qui secouent notre société.

Tout au long de mes fonctions ministérielles, j'ai perçu combien il était urgent d'équiper notre stratégie de sécurité de nouveaux outils technologiques, conformément aux attentes exprimées par les professionnels du terrain et par les Français. Cette réalité a inspiré la démarche qui a permis d'obtenir, par la loi d'orientation et de programmation du ministère de l'Intérieur (Lopmi), le budget le plus ambitieux de l'histoire du ministère de l'Intérieur. Quinze milliards d'euros ont été mobilisés non seulement pour le renforcement des effectifs – 8 500 policiers et gendarmes supplémentaires – mais également pour l'investissement technologique, la formation, le renouvellement des équipements, et le soutien au continuum de sécurité.

Cette conviction a été portée concrètement, sur le terrain, avec l'introduction de la vidéoprotection algorithmique, dont l'efficacité fut éprouvée lors des Jeux olympiques et paralympiques. Ce dispositif est allé plus loin qu'une simple



La sécurité est une construction collective où la justice joue un rôle moteur.

Gérald DARMANIN est ministre d'État, garde des Sceaux, ministre de la Justice depuis 2024. Né en 1982 à Valenciennes et issu du gaulisme social, il a débuté son engagement auprès de Philippe Séguin, avant d'être élu à Tourcoing en 2008, puis de devenir député du Nord en 2012. Maire de Tourcoing (59) à partir de 2014, il a également exercé des mandats régionaux. Ministre des Comptes publics en 2017, il conduit la retenue à la source, supprime la taxe d'habitation, baisse l'impôt sur le revenu, maintient l'endettement public et diminue le déficit public. Nommé ministre de l'Intérieur en 2020, il fait adopter des lois majeures (séparatisme, loi d'orientation et de programmation du ministère de l'Intérieur – Lopmi, immigration) et soutient les forces de l'ordre. Réélu député en 2022 et 2024, il reste attaché à son ancrage local.



surveillance : il a permis, grâce à l'analyse automatisée en temps réel, d'anticiper et de signaler des situations à risque, tout en restant fidèle à nos principes juridiques et éthiques. L'efficacité de ce modèle a été unanimement reconnue, tant par les observateurs français qu'internationaux, qui l'ont salué comme un succès face à la menace terroriste. La réussite de nos Jeux en est l'une des plus belles illustrations.

Dans cet héritage, l'administration pénitentiaire prend toute sa place, avec le déploiement de caméras individuelles au bénéfice des surveillants, à l'instar de la police nationale. Elle explore également l'usage de la biométrie pour sécuriser les accès – empreintes digitales, reconnaissance veineuse, et demain peut-être reconnaissance faciale – qu'il s'agisse de contrôler l'identité des personnes détenues ou de protéger les zones les plus sensibles, comme les armureries.

Plus largement, la Justice, trop souvent reléguée au second plan du débat sécuritaire, est désormais replacée au cœur du dispositif : en 2026, nous mainten-

drons notre niveau annuel d'investissements dans nos technologies et dans le numérique. Cette modernisation s'accélère ainsi dans le monde carcéral, où une cinquantaine d'établissements sont désormais équipés de brouilleurs antidrones, capables de neutraliser les tentatives d'introduction de stupéfiants, d'armes ou de téléphones par voie aérienne. Car sans technologie efficace, il n'y aura pas d'avenir à nos nouvelles prisons de haute sécurité. Sans technologie efficace, l'État sera toujours moins bien armé que ceux qu'il combat.

Ce n'est donc pas seulement la sécurité publique que nous avons fait progresser, mais la confiance collective dans la capacité de l'État à innover, à protéger et à rendre justice. Le chemin n'est pas achevé, mais l'exigence demeure : faire de la sécurité et de la justice, ensemble, le socle d'une République forte, fidèle à ses valeurs et résolument tournée vers l'avenir. ■



François-Noël BUFFET

Ministre auprès du ministre d'État, ministre de l'Intérieur*

Face à des réseaux criminels de plus en plus structurés sur le sol français, à une menace terroriste qui perdure et à la prolifération des ingérences étrangères, les forces de sécurité intérieure continuent de consolider leur arsenal pour anticiper, devancer et prévenir le pire. Derrière la course-poursuite quotidienne contre l'insécurité se joue une course à l'innovation entre les réseaux criminels et les forces de l'ordre, dans laquelle l'État cherche à conserver un coup d'avance et à ne jamais se contenter de réagir, de poursuivre, de subir les délinquants ou les criminels.

Le mandat qui nous est donné par les Français est clair : lutter contre l'insécurité qui continue de parasiter le quotidien des honnêtes gens. Dans un contexte où le numérique permet aux criminels de faire prospérer des activités illicites en ligne avec des conséquences néfastes bien réelles, il est anachronique que les forces de l'ordre ne soient pas armées des moyens nécessaires à l'exercice de leur mandat. Pour répondre à ces attentes légitimes, dans le respect des libertés individuelles, mais aussi du devoir



Nous devons faire ce que la France fait de mieux : innover.

d'efficacité et d'efficience du service public, nous devons faire ce que la France fait de mieux : innover.

Depuis la loi d'orientation et de programmation relative à la sécurité du 21 janvier 1995, la vidéosurveillance a permis une meilleure remontée d'informations pour des interventions des forces de sécurité plus rapides, et donc plus efficaces. Elle constitue aujourd'hui un élément doublement dissuasif car en plus d'être contrôlés en direct par des opérateurs, les flux vidéos peuvent servir de preuve *a posteriori* ou participer à la résolution d'enquêtes.

Maire d'Oullins pendant vingt ans, je sais à quel point la vidéosurveillance a marqué un tournant pour la sécurité du quotidien : les villes qui ont fait le choix de s'équiper tôt sont aujourd'hui fières du service rendu à leurs habitants, et celles qui ne l'ont pas fait à l'époque s'équipent désormais. Malgré les réticences de certains responsables politiques, l'étude nous rappelle aujourd'hui que les Français sont clairvoyants : ils soutiennent à 87 % la vidéoprotection de l'espace public, et plus de 90 %

François-Noël BUFFET est ministre auprès du ministre d'État, ministre de l'Intérieur depuis décembre 2024, en charge des questions de sécurité du quotidien. Ancien ministre des Outre-mer dans le gouvernement de Michel Barnier, il a été maire d'Oullins (69) pendant vingt ans entre 1997 et 2017 et sénateur du Rhône de 2004 à 2024.

Avocat de formation, inscrit au barreau de Lyon, il a été membre titulaire élu par le Sénat à la formation de jugement de la Cour de justice de la République entre 2009 et 2019 et a présidé la commission des lois du Sénat de 2020 à 2024. En tant que président de l'agence d'urbanisme de Lyon et du Grand Lyon entre 2001 et 2004, puis comme conseiller de la métropole de Lyon entre 2004 et 2020, et enfin membre puis secrétaire de la délégation aux collectivités territoriales et à la décentralisation du Sénat, son engagement pour les territoires l'a conduit à œuvrer toute sa vie sur les sujets sécuritaires, juridiques et institutionnels qui l'accompagnent aujourd'hui au ministère de l'Intérieur.



d'entre eux prêtent une grande confiance à leurs services publics, plus que dans les sociétés privées, notamment étrangères : moins de 50 % des Français prêtent confiance aux Gafam – Google, Apple, Facebook, Amazon, Microsoft – pour l'exploitation d'images de vidéoprotection. Cette confiance, nous l'accueillons avec fierté et gravité car elle illustre le dévouement et l'exemplarité des agents qui composent le continuum de sécurité, et elle nous invite à être à la hauteur en répondant mieux encore aux situations à risque, en luttant contre la criminalité du quotidien et contre le sentiment d'impunité.

Dans ce contexte, les grands progrès enregistrés ces dernières années par les technologies d'intelligence artificielle et de reconnaissance algorithmique permettent de détecter plus efficacement le danger que l'œil humain : départs d'incendie, repérage d'armes, de corps tombés, de bagages oubliés, lutte contre les vols de vélos, les mouvements de foule inhabituels... Les cas d'usage sont nombreux et prometteurs, ils ne nécessitent pas d'avoir recours à la reconnaissance

faciale. Avec toute la mesure et la réflexion que les nouvelles technologies peuvent susciter, notre responsabilité est de mettre au service du public les outils de pointe nécessaires à sa sécurité tout en épargnant aux opérateurs du temps pour se concentrer sur le terrain, sur la protection, sur la prévention et sur l'aide aux populations.

Enfin, le sondage OpinionWay pour Cevipof/INTÉRIALE nous rappelle l'importance de la transparence pour conserver durablement la confiance que les Français placent dans leur police, leur gendarmerie, leurs sapeurs-pompiers, leurs douanes. Plus de la moitié des Français déclarent ne pas être assez informés sur l'utilisation des technologies de sécurité et un tiers expriment des inquiétudes légitimes sur l'utilisation des données personnelles. Or, la bonne information et la transparence sont les prérequis de la confiance, de l'adhésion, et par conséquent de la démocratie.

Aujourd'hui, de très nombreuses communes françaises bénéficient d'un réseau étendu de caméras de surveil-

lance mais les images ne peuvent pas toujours être exploitées à leur plein potentiel, faute de moyens humains, les reléguant en partie à des outils dissuasifs. Bien encadré, l'usage des nouvelles technologies telles que l'intelligence artificielle doit nous fournir un avantage considérable dans la protection des citoyens et libérer des ressources et des agents pour des actions plus locales et plus proches des populations. C'est notamment le souhait de nombreux maires et cette étude nous montre que les Français partagent ce constat. Dans cette optique, le ministère de l'Intérieur continue de travailler pour mettre la sécurité au service des Français et suivra les évolutions du secteur avec une grande attention. ■

* Intervention recueillie avant les remaniements ministériels d'octobre 2025.

I. LA CONNAISSANCE DES TECHNOLOGIES DE SÉCURITÉ

La connaissance des technologies de sécurité chez les Français apparaît globalement satisfaisante, puisque 62 % d'entre eux sont capables d'en citer spontanément au moins une. Parmi les technologies évoquées, ce sont logiquement les plus communément répandues qui prédominent dans les réponses données. Ainsi, la captation vidéo et les systèmes d'alarme représentent à eux seuls près de la moitié des mentions, ce qui témoigne de leur forte intégration dans la vie quotidienne des Français. En outre, la présence significative de technologies plus récentes et fortement liées au domaine numérique se révèle corrélée aux écarts générationnels observés parmi les répondants.

Dans le détail, lorsqu'on interroge les participants sur ce que leur évoquent spontanément ces technologies de sécurité, la vidéosurveillance émerge clairement comme la technologie la plus fréquemment citée, recueillant 27 % des réponses. Les systèmes d'alarme (15 %), les antivirus (10 %) et l'intelligence artificielle (6 %) apparaissent dans une moindre mesure. Ce résultat souligne le poids des dispositifs visuels déjà largement implantés dans l'espace public, mettant en lumière que la sécurité technologique est principalement perçue à travers le prisme visuel et de la captation d'images, davantage que par le traitement ou l'analyse des données. Cependant, la mention de l'intelligence artificielle indique une préoccupation croissante vis-à-vis de l'automatisation et de la surveillance algorithmique, particulièrement perceptible chez les jeunes générations, les

individus les plus diplômés ainsi que ceux familiers du numérique.

Toutefois, ce sont les usages attribués à ces technologies qui révèlent une polarisation notable des perceptions parmi la population. Ainsi, 27 % des termes cités spontanément reflètent une vision positive des technologies de sécurité. Les notions de « sûreté », de « sécurité » ou de « tranquillité » sont les plus fréquemment évoquées (11 %), suivies par celles de « confiance » et de « protection » (8 %), et enfin de « modernité » et de « futur » (4 %).

À l'inverse, 21 % des réponses traduisent une vision négative, exprimée par des craintes liées à la « surveillance », au « contrôle » ou à « l'espionnage » (11 %), ainsi qu'à la « cybercriminalité » et au « piratage » (6 %), ou encore au « danger » et à la « crainte » (4 %).

Ces résultats mettent clairement en évidence l'ambivalence qui caractérise encore la perception des technologies de sécurité au sein de la société française. Si ces dispositifs rassurent une partie de la population par leur promesse de protection et de modernité, ils suscitent simultanément des inquiétudes légitimes relatives aux risques d'intrusion, de contrôle excessif et d'atteinte potentielle

27 %

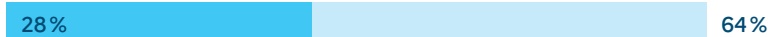
des technologies de sécurité citées spontanément reflètent une vision positive.

Concernant les technologies de sécurité, quels sont les trois premiers utilisateurs qui vous viennent à l'esprit ?

Plusieurs réponses possibles - Total supérieur à 100 %



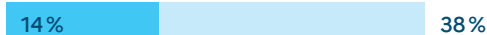
■ La police nationale et la gendarmerie nationale



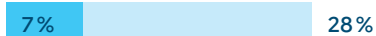
■ Les services de renseignement



■ Les entreprises de surveillance et de gardiennage



■ Les polices municipales



■ Les Gafam (Google, Apple, Facebook, Amazon, Microsoft)



■ Les douanes



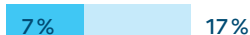
■ L'administration pénitentiaire / ministère de la Justice



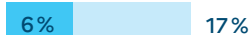
■ Les sapeurs-pompiers



■ Les particuliers



■ Les grandes entreprises



■ NSP



■ En premier
■ Au total

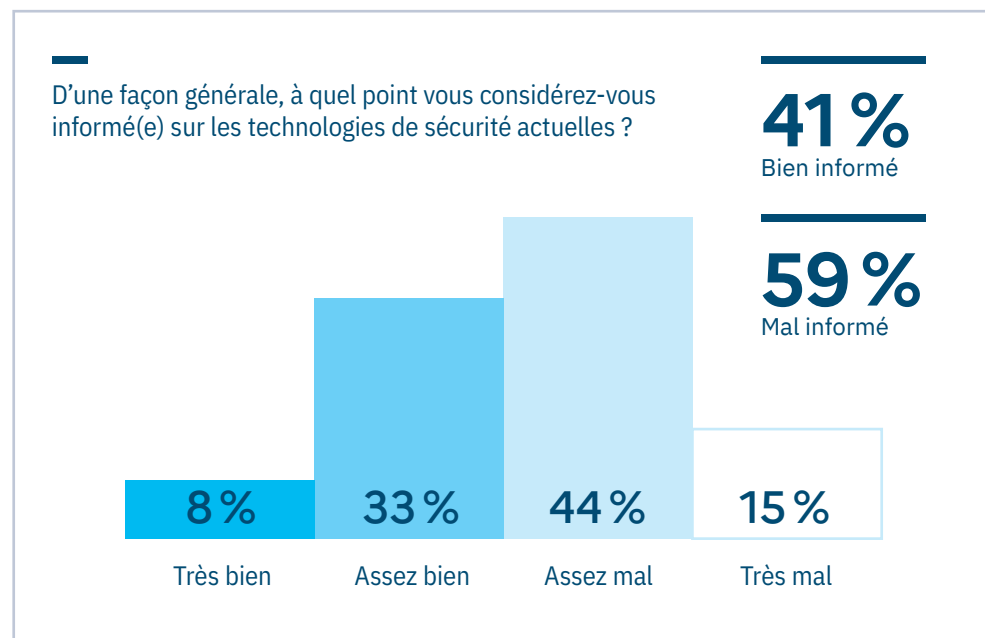
aux libertés individuelles. Cette ambivalence constitue un enjeu central dans les débats publics et les politiques futures relatives à la sécurité technologique.

Concernant le profil sociologique des répondants, ni le sexe ni la catégorie socioprofessionnelle ne semblent influencer significativement la manière dont les technologies de sécurité sont perçues. En revanche, un effet générationnel marqué se manifeste clairement. Ainsi, 39 % des jeunes âgés de 18 à 24 ans associent spontanément ces technologies à des connotations positives, contre seulement 19 % chez les 25-34 ans et 28 % chez les 50-64 ans. À l'inverse, 29 % des répondants âgés de 18 à 24 ans expriment une vision

négative, comparativement à seulement 12 % chez les 25-34 ans et 26 % chez les 50-64 ans.

Cette forte polarisation observée chez les plus jeunes révèle sans doute une familiarité accrue avec ces technologies, leur permettant une meilleure compréhension des mécanismes en jeu, tout en les rendant plus conscients des dérives potentielles.

Par ailleurs, 80 % des répondants âgés de 18 à 24 ans sont capables de citer au moins une technologie de sécurité, contre seulement 47 % des 25-34 ans et 63 % des 65-75 ans, ce qui traduit sans surprise une culture numérique plus développée chez les jeunes générations.



59 %
des Français se disent mal informés
sur les technologies de sécurité.

Ainsi, la perception des technologies de sécurité demeure profondément ambivalente, particulièrement chez les jeunes adultes, ce qui nécessite de tenir compte de ces divergences générationnelles dans l'élaboration des politiques publiques et des stratégies de déploiement technologique.

Quant à la proximité partisane, elle ne semble pas s'imposer comme un marqueur extrêmement polarisant. Si les sympathisants de la majorité présidentielle sont les plus favorables aux technologies de sécurité (36 %), une inclination positive se retrouve dans des proportions similaires chez les partisans de La France insoumise (29 %) et du Rassemblement national (RN) (26 %).

La manière de percevoir les technologies de sécurité recoupe assez nettement la vision positive ou négative que portent les Français sur la vidéoprotection. Dans l'imaginaire collectif, la sécurité technologique est surtout associée à la surveillance visuelle et aux forces de l'ordre et renvoie naturellement aux technologies les plus anciennes et les plus facilement identifiables.

59 % des Français considèrent qu'ils sont mal informés au sujet des technologies de sécurité actuelles. Ce sentiment

concerne majoritairement les personnes âgées, avec 73 % des individus âgés de 65 à 75 ans se déclarant insuffisamment informés, comparativement à seulement 32 % des jeunes adultes âgés de 25 à 34 ans. Ce constat concerne également les catégories socioprofessionnelles les moins favorisées, souvent moins familières des sources d'information généralistes ou rencontrant des difficultés d'accès aux outils numériques et aux supports médiatiques modernes.

À l'inverse, une proportion non négligeable, soit 41 % de la population française, estime être bien informée sur ces sujets. Parmi cette catégorie, on retrouve majoritairement des hommes (45 % contre seulement 36 % chez les femmes) ainsi que les jeunes adultes âgés de 25 à 34 ans, soulignant ainsi un clivage important en fonction de critères générationnels. Toutefois, les 18-24 ans expriment un besoin croissant et manifeste d'obtenir une information de meilleure qualité et davantage accessible.

D'autre part, les technologies de sécurité évoquent souvent, dans l'esprit du grand public, les usages spécifiques qui en sont faits par les forces de l'ordre. Le niveau de connaissance et d'information varie fortement selon le type précis de dispositif concerné. De fait, chez une part

significative de la population, la compréhension générale des technologies utilisées fréquemment par la police et la gendarmerie, notamment les systèmes biométriques, les drones, la lecture automatisée des plaques d'immatriculation et les caméras piétons, est bonne.

En revanche, d'autres technologies plus complexes ou plus récentes demeurent largement méconnues. Ainsi, les logiciels de traitement des données de masse ou les systèmes de vidéoprotection intelligente sont considérés comme particulièrement opaques par 59 % des Français, ce qui illustre un déficit d'information sur ces sujets essentiels.

Plus précisément, la compréhension et l'information concernant l'utilisation spécifique des données biométriques par les forces de sécurité ne concernent positivement que 46 % des répondants. Ce chiffre est encore plus bas concernant l'intelligence artificielle, avec seulement 41 % des Français s'estimant suffisamment informés à son propos.

Ces données soulignent d'ailleurs la tendance selon laquelle la compréhension de ces technologies diminue avec l'âge : seules 29 % des personnes âgées de 65 à 75 ans s'estiment bien informées, tandis que ce chiffre atteint 64 % chez les jeunes adultes âgés de 25 à 34 ans, reflétant ainsi une disparité générationnelle importante en termes de culture numérique.

Malgré ces disparités d'information, une majorité notable de Français, soit 71 %, déclare chercher activement des rensei-

gnements sur ces technologies. Les médias traditionnels restent le moyen privilégié d'accès à l'information pour près de la moitié d'entre eux (45 %), suivis par le bouche à oreille (27 %) et les réseaux sociaux (25 %), ces derniers étant particulièrement prisés par les jeunes générations.

Les profils sociologiques les plus curieux en matière de technologies de sécurité sont principalement les jeunes (81 % contre 67 % des plus âgés), les catégories socioprofessionnelles supérieures ainsi que les sympathisants politiques de gauche. Ces mêmes groupes montrent parallèlement une conscience accrue des risques associés à ces technologies, notamment en ce qui concerne leur impact sur les libertés individuelles.

En définitive, bien que les Français disposent globalement d'une bonne connaissance générale des technologies de sécurité, il subsiste des disparités importantes selon les générations, les niveaux d'éducation et les catégories socioprofessionnelles.

L'enjeu de la sensibilisation et de l'éducation autour des technologies les plus récentes et complexes s'avère donc crucial. Car la méconnaissance ou la compréhension limitée de ces outils alimente fréquemment des perceptions biaisées, une acceptation passive voire une hostilité manifeste avec le risque d'empêcher la conduite d'un débat public éclairé et la mise en place d'une régulation adaptées à ces matériels et systèmes dans une société en constante évolution technologique. ■



Olivier RENAUDIE

Secrétaire général
de l'Association française
de droit de la sécurité
et de la défense (AFDSD)
et président du comité
scientifique du Continuum Lab

La sécurité est en proie à de multiples transformations contemporaines. Parmi celles-ci, on peut en citer deux. La première transformation tient à l'affirmation de la sécurité comme un service public. Sur le plan juridique, cela s'est traduit par deux éléments majeurs. D'une part, la reconnaissance d'un droit à la sécurité par la loi du 21 janvier 1995 : « La sécurité est un droit fondamental et l'une des conditions d'exercice des libertés individuelles et collectives »¹. D'autre part, la globalisation des réponses à l'insécurité, incarnée par un concept, celui de continuum de sécurité, selon lequel la sécurité n'est pas seulement l'affaire de l'État, mais doit être coproduite de manière coordonnée et efficace par tous les acteurs susceptibles d'y contribuer. La seconde transformation concerne l'apparition des technologies comme outils permettant d'assurer la sécurité au quotidien. Longtemps, le recours aux technologies en matière de sécurité s'est limité aux caméras de vidéoprotection installées pour assurer la surveillance des voies publiques. Aujourd'hui, c'est un véritable marché numérique qui est à la disposition de l'État, des communes et des entre-

prises : vidéoprotection « intelligente », algorithmes, détection de mouvements de foule, plateformes dites d'hypervision, *open* et *big data*, drones, reconnaissance faciale, agents de police connectés, police prédictive, etc. De ce point de vue, les Jeux olympiques de Paris ont pu être perçus comme une vitrine des instruments numériques dédiés à la sécurité et un puissant vecteur de promotion des *safe cities*². Reste que le développement de l'usage de ces différentes technologies pose un certain nombre de questions. Certaines sont relatives à la protection de la vie privée et à l'exercice d'un certain nombre de libertés, individuelles et collectives. D'autres concernent les modalités de mise en œuvre et de contrôle de celles-ci par les autorités publiques, nationales et locales.

Ces questions sont au cœur de l'étude intitulée « Les Français et les technologies de sécurité » réalisée par OpinionWay pour le Cevipof et la mutuelle INTÉRIALE. Avant d'évoquer le contenu de cette étude, il n'est pas inutile d'insister sur deux éléments d'ordre méthodologique. Le premier élément tient au calendrier : l'étude a été réalisée à la fin

”

La connaissance des technologies de sécurité apparaît largement perfectible.

Olivier RENAUDIE est agrégé des facultés de droit et professeur de droit public à l'École de droit de la Sorbonne. Il est membre de deux centres de recherche : l'Institut des sciences juridiques et philosophiques de la Sorbonne et le Centre d'études et de recherches en science administrative.

Il est par ailleurs directeur du master 2 Contentieux public, directeur de l'École doctorale de droit public et référent « Défense et sécurité » de l'université Paris 1 Panthéon-Sorbonne.

Il est également directeur du Groupement de recherche sur l'administration locale en Europe (GrALE), groupement d'intérêt scientifique (GIS) réunissant une trentaine de partenaires publics et privés. Spécialiste reconnu, il a publié de nombreux ouvrages et articles dans le domaine de la police et de la sécurité.

Depuis juillet 2020, il est membre du collège en charge de la déontologie et de la sécurité auprès du Défenseur des droits et, depuis janvier 2022, du Comité d'éthique de la police municipale de Paris.





du mois de juin 2024, soit juste avant les Jeux olympiques de Paris, c'est-à-dire à un moment où les Français avaient été particulièrement sensibilisés aux technologies de sécurité utilisées, voire expérimentées, à cette occasion³. Le second élément tient à l'échantillon de personnes interrogées. Loin d'être négligeable, celui-ci représente 3 438 personnes, âgées de 18 à 75 ans, choisies selon la méthode des quotas pour représenter la population française.

Il ne faut pas s'en cacher, les résultats de cette étude sont absolument décapants. Trois enseignements d'ordre général nous paraissent pouvoir en être tirés. D'abord, ils donnent à voir une population ayant plutôt confiance dans les technologies pour contribuer de manière efficace à la sécurité sur la voie publique. Ensuite, ces résultats témoignent d'un renouvellement de l'opposition classique (et souvent stérile) entre sécurité et libertés : pour une majorité de Français, les technologies peuvent renforcer à la fois leur sécurité et l'exercice de leurs libertés.

Enfin, et c'est peut-être la surprise majeure de cette étude, les Français ne se positionnent pas à l'égard des technologies de sécurité en fonction de

considérations politiques et idéologiques, mais apparaissent davantage enclins au pragmatisme et à l'adaptation.

Au-delà de ces enseignements d'ordre général, trois points méritent attention. Le premier point tient à l'état de l'opinion sur la question de l'usage d'outils technologiques en temps réel, notamment de la géolocalisation : les Français y sont majoritairement favorables en matière de prévention d'actes terroristes, d'arrestation d'auteurs de crimes et délits et de secours à personne⁴. Le deuxième point est relatif à la confiance de la population à l'égard de ceux qui utilisent les technologies de sécurité dans l'exercice de leurs missions. Si celle-ci n'est pas absolue, les chiffres de l'étude sont éclairants : ils montrent que, très majoritairement, les Français font confiance aux forces de sécurité pour utiliser à bon escient la vidéoprotection ou les données biométriques dans le cadre de leur action⁵. Le troisième, et dernier, point concerne la connaissance des technologies de sécurité par les Français. Si désormais, la vidéoprotection fait partie de notre vie quotidienne, c'est loin d'être le cas de nombreuses autres technologies de sécurité, par exemple le cryptage ou l'intelligence artificielle, qui demeurent mal connues⁶.

La connaissance des technologies de sécurité apparaît ainsi largement perfectible. Dès lors, il est nécessaire de contribuer à cette appréhension afin de comprendre ce que leur usage signifie, mais également pour contribuer à renforcer la confiance qu'elles peuvent inspirer. De ce point de vue, la présente étude se présente certainement autant comme un point d'arrivée, que comme un point de départ. ■

¹ Art. L 111-1 du Code de la sécurité intérieure.

² Voir Maximilien Lanna, *Villes, numérique et sécurité*, Mare et Martin, 2025.

³ Voir en ce sens la loi du 19 mai 2023 relative aux Jeux olympiques et paralympiques de 2024 et portant diverses autres dispositions.

⁴ Voir p. 37.

⁵ Voir p. 57.

⁶ Voir p. 23.

II. LES CAS D'USAGE ET LES UTILISATEURS

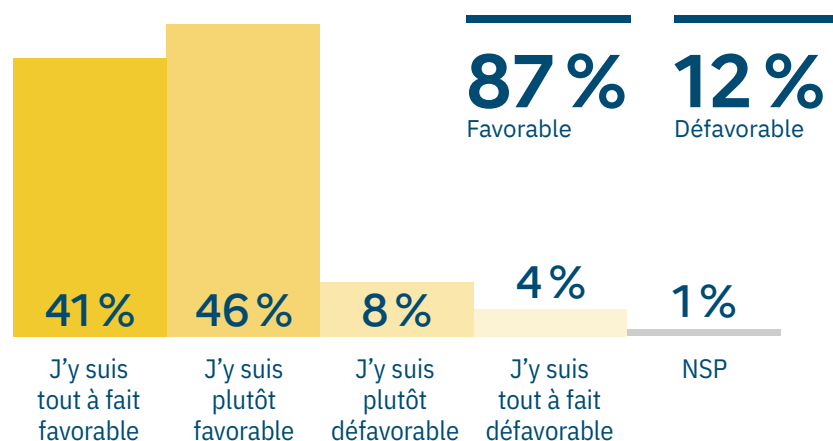
La couverture vidéo de l'espace public

Si l'adhésion de la population aux technologies de sécurité dépend significativement du type d'outil employé, il apparaît toutefois qu'un large consensus existe autour de la présence de caméras de vidéoprotection dans l'espace public. 87 % des Français s'y déclarent favorables, dont 41 % « tout à fait favorables », tandis que l'opposition ferme, qualifiée de « tout à fait défavorable », reste très marginale à hauteur de seulement 4 %. Les femmes manifestent une adhésion encore supérieure à celle des hommes (90 % contre 85 %),

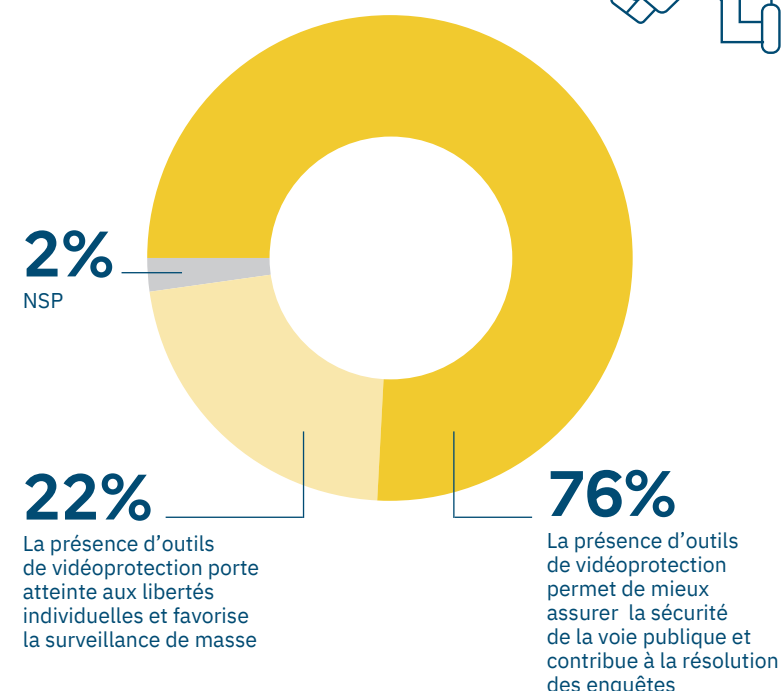
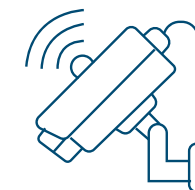
un phénomène probablement lié à une perception plus directe des bénéfices en matière de sécurité personnelle. De manière générale, cette adhésion massive à la vidéoprotection transcende largement les critères sociodémographiques classiques, incluant genres, âges et catégories sociales et témoigne ainsi d'un soutien transversal dans la société française.

Toutefois, les affinités politiques jouent un rôle significatif dans l'intensité de cette adhésion. Les sympathisants de

Quelle est votre opinion relative à la présence de caméras de vidéoprotection dans l'espace public ?



À propos de la présence de caméras de vidéoprotection dans l'espace public, de laquelle de ces opinions vous sentez-vous le plus proche ?



droite se montrent nettement plus attachés à la vidéoprotection que leurs homologues de gauche. Plus précisément, la vidéoprotection recueille un soutien très élevé au sein de la majorité présidentielle (96 %), de Reconquête (93 %), du Rassemblement national (93 %) et des Républicains-LR (99 %). À gauche, l'adhésion reste importante mais diminue sensiblement chez les Français les plus à gauche : on relève ainsi des taux d'approbation de 82 %

chez les sympathisants du Parti socialiste (PS), de 81 % chez ceux d'Europe écolo-logie-Les verts (EELV), et de 77 % chez ceux des LFI, ces derniers étant d'ailleurs surreprésentés parmi les personnes défavorables (23 % contre seulement 1 % chez LR).

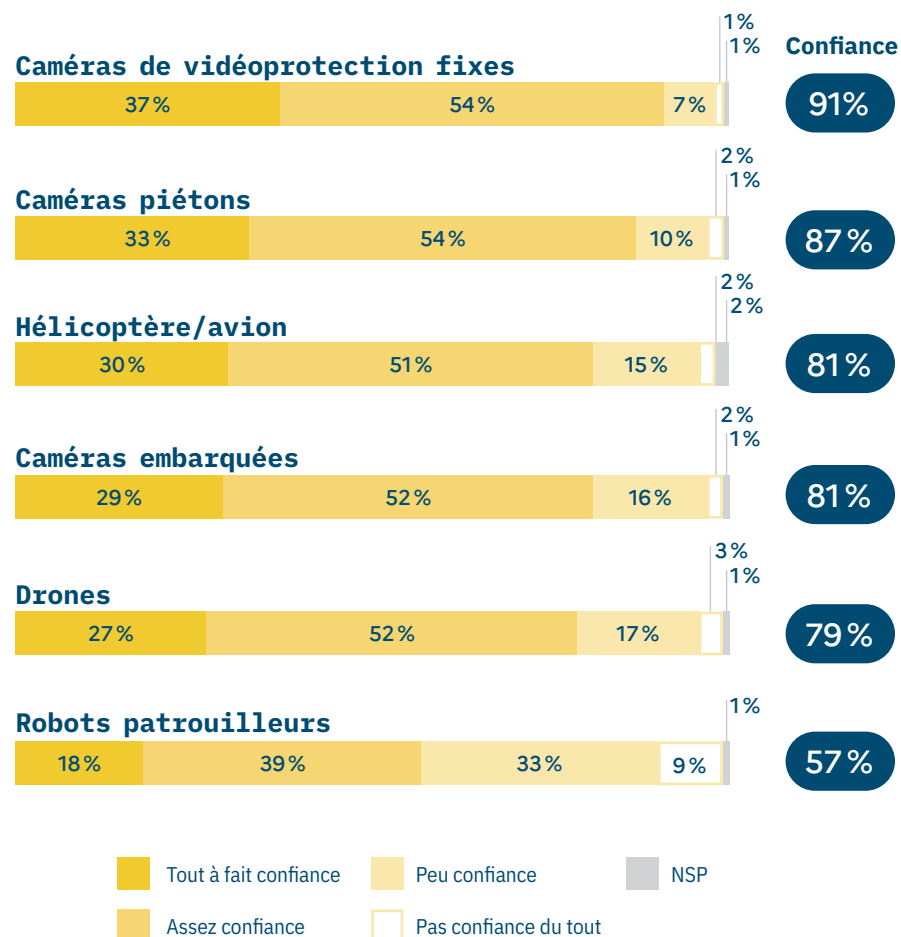
Cette large adhésion à la vidéoprotection s'explique principalement par les bénéfices qui lui sont associés, notamment pour le renforcement de la sécurité de

59 %

des Français sont favorables
aux caméras de vidéoprotection
dans l'espace public.

Avez-vous confiance dans les outils de captation d'images suivants pour assurer la sécurité sur la voie publique ?

Question posée uniquement aux personnes favorables à la présence de caméras
de vidéoprotection dans l'espace public, soit 87% de l'échantillon.



la voie publique et, plus encore, pour sa contribution déterminante à la résolution des enquêtes criminelles, un avis partagé par 76 % des Français. En revanche, une minorité non négligeable de Français (22 %) estime que ces dispositifs portent atteinte aux libertés individuelles et facilitent la surveillance de masse, révélant ainsi la persistance – même amoindrie – du traditionnel clivage entre la sécurité collective et la préservation des libertés individuelles.

Les femmes apparaissent une nouvelle fois plus enclines que les hommes à souligner les avantages de la vidéoprotection (79 % contre 73 %), un phénomène particulièrement marqué chez les personnes âgées (84 % des 65-75 ans). Paradoxalement, si les jeunes adultes âgés de 25 à 34 ans expriment une certaine réserve à l'égard de ces dispositifs (seulement 67 % d'approbation), la génération encore plus jeune (18-24 ans) témoigne d'une adhésion plus forte, 76 % partageant l'idée que la vidéoprotection constitue davantage une protection qu'une menace pour les libertés individuelles.

L'influence des convictions politiques est ici encore très nette, avec une différence marquée selon les partis : ainsi, 92 % des sympathisants LR estiment que la vidéoprotection protège avant tout la sécurité publique, contre seulement 62 % chez les sympathisants LFI, soit un écart significatif de près de 30 points.

Enfin, le degré de confiance envers la captation d'images en temps réel varie

également selon le type précis de technologie employé, l'usage envisagé et les acteurs exploitant ces données. Ainsi, 91 % des Français expriment leur confiance envers les caméras de vidéoprotection fixes, 87 % envers les caméras piétons portées par les forces de sécurité, tandis que seulement 57 % manifestent cette même confiance à l'égard des robots patrouilleurs. Ce résultat révèle clairement que les technologies éprouvées et bien établies sont mieux acceptées que les dispositifs émergents, perçus comme futuristes, et potentiellement moins maîtrisés et encadrés.

En conclusion, si la vidéoprotection bénéficie d'une large adhésion sociale, il est indispensable d'intégrer les nuances liées aux profils socio-démographiques et aux convictions politiques. L'introduction de nouvelles technologies doit donc s'accompagner d'une réflexion approfondie sur leur acceptabilité sociale, les garanties apportées en matière de libertés individuelles, et la nécessaire transparence dans leur déploiement et leur usage.

L'adhésion aux technologies d'analyse en temps réel dépend fortement de leur finalité, notamment lorsqu'elle est associée à des enjeux sécuritaires vitaux. Ainsi, 96 % des Français soutiennent leur utilisation pour combattre la criminalité, prévenir les actes terroristes ou assister les personnes en danger. En revanche, ils manifestent une très légère réticence lorsqu'il s'agit d'utiliser ces outils à des fins jugées punitives, telles que la verbalisation routière ou la

96 %

des sondés sont favorables
à l'analyse en temps réel pour
prévenir le terrorisme et arrêter
des auteurs de crimes et délits.

sanction des incivilités, avec une adhésion oscillant entre 80 % et 88 %. Cette retenue doit toutefois être relativisée puisque l'adhésion demeure très majoritaire, indépendamment du sexe, de l'âge ou de la proximité partisane.

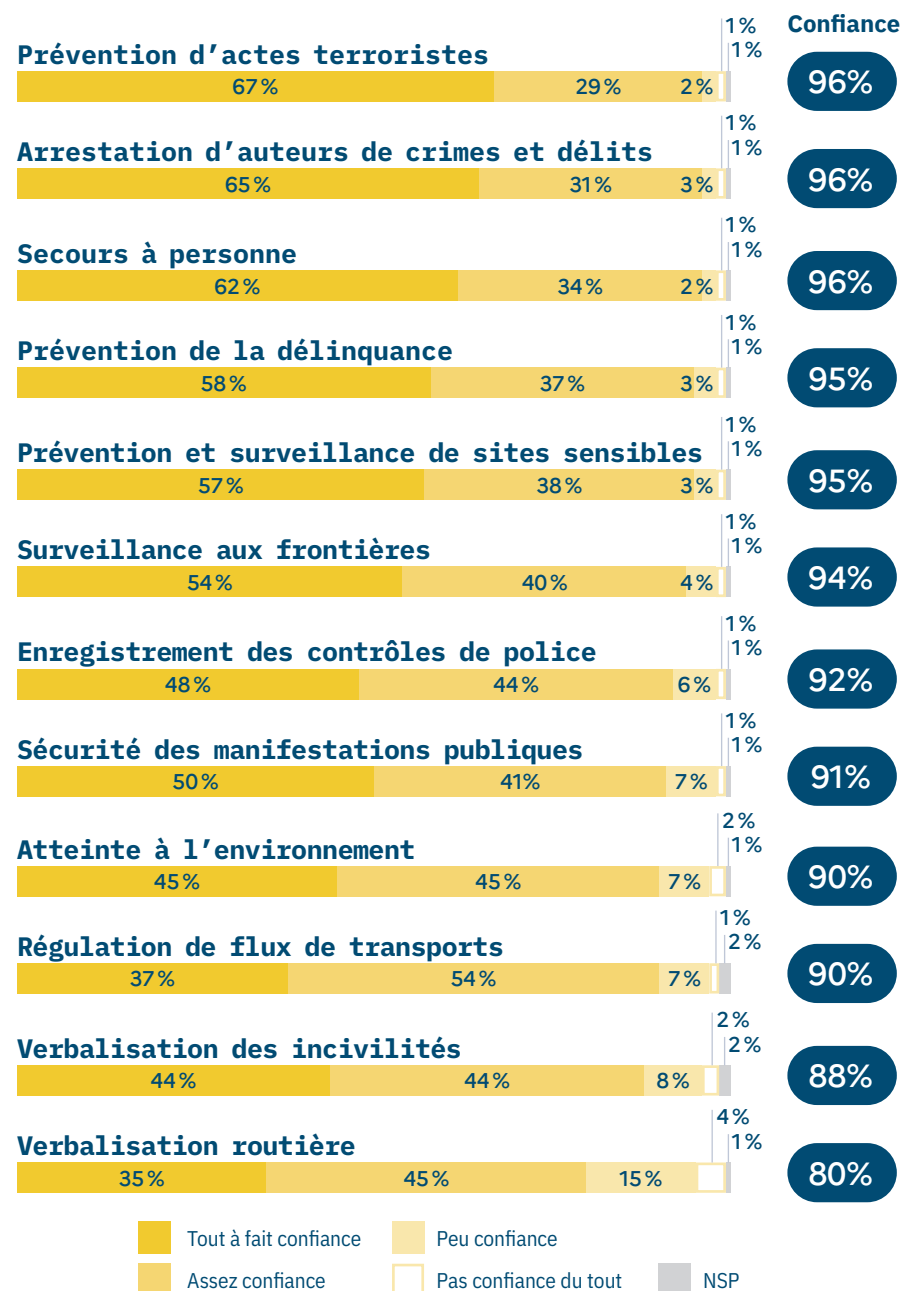
Concernant les acteurs impliqués dans la gestion des technologies de sécurité, la confiance de la population est presque unanime envers les services publics et les forces de l'ordre, en particulier les pompiers (94 %), la police et la gendarmerie (91 %) et les douanes (90 %). À l'inverse, les acteurs privés tels que les Gafam suscitent une méfiance significative, avec seulement 45 % de confiance. Cette divergence révèle une perception des dispositifs de vidéo-protection comme devant essentiellement relever d'une compétence publique destinée à l'intérêt général, alimentant ainsi une défiance envers les acteurs commerciaux, notamment étrangers.

Cependant, cette méfiance pourrait évoluer avec les générations car seuls 30 % des 65-75 ans font confiance aux Gafam contre 42 % des 18-24 ans. À l'inverse, la confiance envers les forces de l'ordre diminue avec l'âge : 97 % des 65-75 ans font confiance à la police et à la gendarmerie contre 86 % des 18-24 ans, avec une différence encore plus marquée vis-à-vis des services de

renseignement (89 % chez les 65-75 ans contre 72 % chez les 18-24 ans). Cette divergence générationnelle recoupe également les affinités politiques, les sympathisants de LFI, généralement plus jeunes, accordant moins de confiance à la police (77 % contre 91 % en moyenne), tandis que les sympathisants du RN manifestent une confiance supérieure à la moyenne, y compris envers les Gafam.

Quant à l'amélioration de l'efficacité des équipements de vidéoprotection dans l'espace public, les Français proposent plusieurs axes prioritaires : une densification des caméras, notamment dans les zones sensibles ou insuffisamment couvertes, ainsi que l'amélioration technique des dispositifs via une meilleure résolution des images, des angles de vue ajustables et l'intégration de l'intelligence artificielle. Ils préconisent aussi une meilleure gestion des données, notamment en prolongeant leur conservation. Par ailleurs, certains suggèrent de mieux protéger les équipements en les rendant soit plus discrets, soit, au contraire, plus visibles dans une démarche de transparence accrue. Enfin, l'importance de renforcer le rôle humain est également soulignée, en particulier chez les personnes âgées, tandis que les jeunes privilégient davantage le développement technologique des équipements.

Êtes-vous favorable à l'utilisation, en temps réel, d'outils d'analyse d'images, de sons, de mouvements et de géolocalisation, dans les cas suivants ?





94 % font confiance
aux sapeurs-pompiers pour
capter/exploiter des images ;
**PIC DE CONFIANCE DANS
UN ACTEUR DE PROXIMITÉ.**

Parmi les 12 % de Français défavorables à la vidéoprotection, deux types de critiques émergent clairement. D'une part, une critique conceptuelle axée sur les risques pour les libertés individuelles et la vie privée, particulièrement forte chez les catégories socioprofessionnelles défavorisées et les inactifs (respectivement 18 % et 23 % contre 9 % chez les CSP+). Certains évoquent même un risque de dérive totalitaire, une inquiétude surtout exprimée par les CSP+ et les sympathisants LFI (22 % contre 14 % en moyenne).

D'autre part, une critique pragmatique concerne l'efficacité limitée perçue des équipements, jugés insuffisamment dissuasifs face à la délinquance quotidienne ou peu suivis d'actions concrètes de la part des autorités. Ces critiques proviennent majoritairement d'hommes appartenant aux générations les plus jeunes et les plus âgées, plutôt qu'aux générations intermédiaires.

En conclusion, comprendre la perception des Français sur la vidéoprotection revêt une importance cruciale car elle influence fortement leur attitude globale envers les technologies de sécurité. Majoritairement plébiscité dans toutes les couches sociales, notamment pour son efficacité contre la criminalité, ce dispositif suscite néanmoins des réserves quand il touche à des usages perçus comme punitifs ou intrusifs. Enfin, la confiance reste largement accordée aux autorités publiques tandis que les acteurs privés et les technologies émergentes sont envisagés avec une méfiance relative, illustrant clairement l'importance d'une approche équilibrée entre sécurité publique et respect des libertés individuelles.

Avez-vous confiance dans les acteurs suivants pour capter et exploiter des images enregistrées sur la voie publique ?

Question posée uniquement aux personnes favorables à la présence de caméras de vidéoprotection dans l'espace public, soit 87 % de l'échantillon.

	Sexe	Âge	Statut		
			CSP+	CSP-	Inactif
	% Confiance				
Pompiers	94%	18 à 24 ans : 95% 25 à 34 ans : 90% 35 à 49 ans : 93% 50 à 64 ans : 96% 65 à 75 ans : 99%	93%	93%	96%
Police nationale/gendarmerie nationale	91%	86%	89%	90%	93%
Douanes	90%	84%	88%	88%	92%
Services de renseignement	86%	72%	87%	85%	85%
Polices municipales	83%	78%	80%	82%	86%
Entreprises de sécurité privée	64%	62%	67%	66%	61%
Gafam (Google, Apple, Facebook, Amazon, Microsoft)	45%	42%	50%	46%	36%



Laurent NUÑEZ

Préfet de police de Paris*

La préfecture de police étant, à l'origine, un laboratoire de certaines innovations technologiques, il m'a semblé naturel de rebondir sur l'enquête diligentée par le Continuum Lab au sujet de la perception par les Français des technologies de sécurité innovante.

Le terme « technologies de sécurité » est très englobant et l'enquête fait apparaître que le grand public y rattache des technologies très différentes.

Pour bien comprendre l'usage des technologies de sécurité innovantes et leur nécessité au sein de la préfecture de police, il convient de rappeler les caractéristiques des missions de sécurité exercées par celle-ci.

La préfecture de police assure la sécurisation de l'ensemble du territoire formé par Paris intra-muros, les trois départements de la petite couronne (Hauts-de-Seine, Seine-Saint-Denis et Val-de-Marne) et les aéroports (Orly, Roissy, Le Bourget). Cette zone de responsabilité recense aujourd'hui près de 7 millions d'habitants et se caractérise par une très forte densité urbaine. Elle se démarque



*Les technologies innovantes
sont un tremplin pour faire
mieux, pour faire plus.*

également par des niveaux de fréquentation très élevés avec près de 37 millions de touristes pour le Grand Paris en 2023. La compétence du préfet de police s'étend également aux transports ferroviaires de toute l'Île-de-France. Enfin, en tant que préfet de zone, le préfet de police est compétent en situation de crise, dès lors que celle-ci dépasse le cadre d'un département.

Dans l'agglomération parisienne, on comptabilise plus de 10 000 manifestations et événements publics sécurisés par la préfecture de police chaque année, et environ 300 000 interventions policières (violences, vols, délits).

Dans ce contexte unique en France de volumes et de typologie de missions, le recours à des technologies de sécurité innovantes est un véritable levier d'efficacité qui a conduit la préfecture de police à asseoir sa stratégie dans un livre blanc du numérique. La préfecture de police mène ainsi de grands projets numériques à la pointe des dernières innovations technologiques :

- le plan de vidéoprotection pour Paris (PVPP) avec 5 000 caméras déployées à Paris et en petite couronne ;



Laurent NUÑEZ est né le 19 février 1964 à Bourges. Il est haut fonctionnaire, préfet de police de Paris depuis le 21 juillet 2022. Juriste de formation, il est titulaire d'une maîtrise de droit public, d'un diplôme d'études supérieures spécialisées (DESS) de gestion des collectivités locales et diplômé de l'École nationale des impôts. Il a été préfet de police des Bouches-du-Rhône et directeur de cabinet du préfet de police de Paris (2012–2015). Ancien directeur général de la sécurité intérieure (DGSI) de 2017 à 2018, il devient secrétaire d'État auprès du ministre de l'Intérieur jusqu'en 2020. Ensuite, il est nommé coordonnateur national du renseignement et de la lutte contre le terrorisme avant de devenir préfet de police de Paris en juillet 2022.



- l'expérimentation, dans le cadre des Jeux olympiques et paralympiques (JOP) 2024, de la vidéoprotection augmentée, avec l'équipement de caméras dédiées avec un logiciel d'intelligence artificielle (IA) ;
- des salles de commandement à la pointe de la technologie pour piloter l'ensemble des opérations, avec des murs d'images, et de la cartographie numérique ;
- une flotte de drones acquise pour sécuriser les grands rassemblements ou des opérations à risques ;
- un dispositif de lutte antidrone pour garantir la sûreté aérienne dans une zone urbaine dense.

Toutes ces technologies sont déployées dans un cadre réglementaire strictement respecté. L'information du public se fait *via* le site de la préfecture de police, prefecturedepolice.interieur.gouv.fr, qui recense par exemple l'ensemble des caméras déployées ou encore les autorisations accordées pour les vols de drones. Cette information est complétée par de l'information *ad hoc*, propre à la technologie utilisée : par exemple, à la fin de l'année 2025, la préfecture de police va déployer de nouveaux panon-

ceaux concernant la vidéoprotection pour encore mieux informer le public de la présence de caméras sur la voie publique. Il est fondamental de pouvoir répondre aux attentes de transparence des citoyens, afin de susciter une confiance pérenne.

Je note à cet égard qu'en matière de vidéoprotection – technologie que la préfecture de police utilise au quotidien, devenue indispensable au travail de voie publique comme judiciaire – l'enquête du Continuum Lab fait apparaître une opinion très nettement positive : l'usage de la vidéoprotection sur la voie publique recueille en effet 87 % d'opinions favorables.

Concernant l'IA, dont l'enquête révèle que les Français la perçoivent favorablement (54 %), la préfecture de police a pris une part active à l'expérimentation pendant les JOP. Notre retour d'expérience est positif. J'appelle donc de mes vœux l'adoption prochaine d'un cadre législatif pour pouvoir reprendre cette expérimentation. En effet, l'IA, dans ce cadre, est une aide formidable à la décision. Elle permet d'indiquer au policier quelle caméra regarder, et de détecter

des événements potentiels qui échapperaient à l'attention humaine. Mais il est important de préciser qu'il ne s'agit que d'une assistance : une levée de doute doit systématiquement être réalisée par un policier, qui ensuite traite l'événement de la même manière que s'il avait été détecté par un œil humain.

Les événements prédéterminés les plus pertinents pour la préfecture de police concernent :

- la densité de foule : anticipation de regroupements trop importants de personnes ;
- la présence d'un objet ou d'une personne dans un endroit interdit ;
- la circulation à contresens.

L'IA a également une utilité au-delà de la vidéoprotection en temps réel. Elle peut être utilisée pour de la transmission automatique (*speech to text*) : la préfecture de police expérimente cette technologie dans le cadre des auditions de mineurs exposés à des violences intra-familiales.

L'IA pourra à l'avenir également être employée, lorsque le cadre législatif le permettra, à des fins de rapprochement judiciaire : la technologie permet aujourd'hui de traiter des données hétérogènes et de les recouper (par exemple, issues d'un téléphone et des réseaux sociaux).

Il est indispensable, pour une institution comme la préfecture de police, d'exploiter les solutions existantes et d'anticiper celles à venir. Les technologies innovantes sont un tremplin pour faire mieux, pour faire plus, le décrochage en la matière n'est pas un risque que le secteur public peut prendre. ■

* Intervention recueillie avant les remaniements ministériels d'octobre 2025.

Au moment où nous mettons l'ouvrage sous presse, Laurent Nuñez a été nommé ministre de l'Intérieur.



Jean-Paul JEANDON

Membre du comité directeur de l'Association des maires de France (AMF), coprésident de la commission Prévention de la délinquance et sécurité

Interroger l'opinion sur les technologies de sécurité dans le contexte si singulier de la préparation de notre pays aux Jeux olympiques et paralympiques (JOP) de 2024 représentait un triple intérêt. D'abord sur la mesure de l'acceptabilité sociale des dispositifs nouveaux qui ont été expérimentés dans le cadre de la loi JOP du 19 mai 2023. Ensuite, pour anticiper et prendre en compte les réactions du public face à leur déploiement massif et visible. Enfin, pour éclairer les décideurs sur les attentes et les craintes des citoyens, afin d'ajuster les politiques de déploiement, de régulation et de communication sur ces technologies.

L'étude a fait ressortir une acceptation majoritaire de la vidéoprotection (87 % favorables), une acceptation moindre pour l'intelligence artificielle – IA – (65 %), un fort niveau de confiance dans les acteurs publics (91 à 94 % pour la vidéoprotection par les forces publiques), mais aussi un attachement au contrôle et à la régulation de ces technologies pour préserver les libertés individuelles.

L'étude souligne également que la confiance des citoyens dans l'usage des

technologies de sécurité est plus forte quand leur gestion est assurée par des acteurs publics (police nationale, gendarmerie nationale, sapeurs-pompiers, polices municipales) plutôt que par des entreprises privées ou des Gafam – Google, Apple, Facebook, Amazon, et Microsoft.

Les maires, en tant qu'autorité de proximité, sont des acteurs clés pour l'acceptabilité sociale, la mise en œuvre et la régulation de ces dispositifs innovants.

Leurs polices municipales bénéficient d'un niveau de confiance élevé (64 % pour la vidéoprotection, 76 % pour l'IA, 73 % pour les données biométriques), ce qui légitime leur rôle dans le continuum de sécurité.

Les usages acceptés de l'IA et de la vidéoprotection concernent en priorité la prévention du terrorisme, la lutte contre la criminalité, la gestion des secours et la surveillance de sites sensibles.

Les Français attendent des maires qu'ils soient moteurs dans l'expérimentation, la régulation et la pédagogie autour de ces technologies. L'étude montre que

”

Les maires ne peuvent qu'être sensibles au besoin de sécurité que la population exprime.

Jean-Paul JEANDON est un homme politique français né en 1958 à Paris. Économiste de formation, il a travaillé comme chercheur et expert à la Commission européenne, puis a occupé diverses fonctions de direction dans le secteur des télécommunications chez Orange. Il devient maire de Cergy (95) en 2013, puis président de la Communauté d'agglomération de Cergy-Pontoise en 2020. Engagé pour la transition écologique et la cohésion sociale, il occupe aussi des responsabilités nationales, notamment comme coprésident de la commission Prévention de la délinquance et sécurité à l'Association des maires de France (AMF) et vice-président de France urbaine.



les citoyens souhaitent un contrôle démocratique local sur l'usage des outils de sécurité.

Cependant, pour renforcer la sécurité, les Français privilégient d'abord l'augmentation des effectifs de police/gendarmerie (36 %), puis le recrutement de spécialistes en cybersécurité (24 %), et enfin l'investissement dans les nouvelles technologies (18 %). Cela montre que les technologies innovantes sont vues comme un complément, non un substitut, à l'action humaine et à la présence sur le terrain.

Avant même la fin de l'expérimentation liée aux JOP (mars 2025), 63 % des Français se disent favorables à la généralisation de l'IA dans la vidéoprotection.

Les usages de l'IA les plus acceptés sont la détection de départs de feu, l'identification d'auteurs de crimes/délits, la détection d'armes et la vidéo-verbalisation.

Du point de vue des maires, ces derniers ne peuvent qu'être sensibles au besoin de sécurité que la population exprime. Ce besoin a été illustré par une autre étude Ifop pour le Centre de réflexion sur la sécurité intérieure (CRSI) « Les maires et l'insécurité » en mars 2025.

Pour l'ensemble des maires, la perception de sécurité est vue comme un enjeu prioritaire (48 %).

Le deuxième résultat faisant le lien avec l'objet de cette tribune est le souhait, à 74 %, de simplification des procédures administratives pour faciliter l'installation de caméras de surveillance. L'étude d'OpinionWay fait d'ailleurs remonter, parmi les pistes d'amélioration, la nécessité de faciliter l'implantation des équipements, d'optimiser leur implantation et de couvrir de nouvelles zones.

La simplification des procédures (dépôt de dossier, délais de réponse, articulation avec les services de l'État) est donc un enjeu pour accélérer le déploiement, notamment dans les communes moyennes et rurales.

Les centres de supervision urbaine (CSU), gérés par les mairies, assurent la surveillance quotidienne, la prévention, la gestion des incivilités. Elles jouent un rôle clé dans la coordination locale, la gestion en temps réel des images et l'alerte des forces de sécurité intérieure (FSI). Celles-ci, police nationale et gendarmerie nationale, interviennent sur les faits graves, la criminalité, le terrorisme. Les policiers municipaux et les CSU peuvent être en appui. Les préfectures

assurent la coordination générale de la sécurité, notamment lors d'événements majeurs ou de crises *via* les centres opérationnels départementaux – COD – (organes de gestion de crise) pouvant s'articuler avec les postes de commandements communaux (PCC).

La plus-value partenariale repose sur le partage d'informations, la mutualisation des moyens techniques (caméras, logiciels d'analyse) et la capacité à agir rapidement dans une logique d'action complémentaire supervisée par les outils technologiques.

Dans l'étude, les répondants souhaitent d'ailleurs davantage d'agents derrière les écrans (CSU), une meilleure exploitation des données et une interconnexion accrue entre acteurs (forces nationales, municipales, CSU).

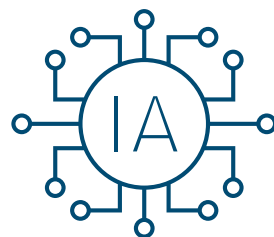
L'efficacité de la vidéoprotection est jugée optimale quand elle s'appuie sur une chaîne complète : captation (CSU), analyse (logiciels, IA), intervention (police nationale, gendarmerie nationale et polices municipales).

Dans cet écosystème partenarial, l'association des maires de France est très attachée au principe de libre administration des communes, principe qui

s'applique aux usages des technologies de sécurité innovantes. Au moment du bilan post JOP 2024, il est nécessaire d'accompagner les communes volontaires pour qu'un usage coproduit disposant de financements pérennes puisse démontrer sa plus-value dans les politiques de sécurité territoriales.

Pour ce qui est de l'acceptabilité sociale, elle dépendra de la transparence, de la pédagogie et du contrôle démocratique local, autant que de l'efficacité technique des dispositifs.

L'enjeu principal réside dans la recherche d'un juste équilibre entre la sécurité et le respect des libertés fondamentales. ■



L'intelligence artificielle et l'analyse automatisée

Concernant l'utilisation de l'intelligence artificielle (IA) par les forces de l'ordre, 65 % des Français adhèrent davantage à l'idée que cette technologie contribue à améliorer leur efficacité opérationnelle et, *in fine*, à garantir la sécurité publique. À l'opposé, 33 % perçoivent cette utilisation comme une menace potentielle pour les libertés individuelles, exprimant ainsi une inquiétude notable. Cette adhésion majoritaire reste toutefois moindre comparée au consensus observé autour de la vidéoprotection, soulignant une certaine prudence de la population face aux outils technologiques complexes et automatisés.

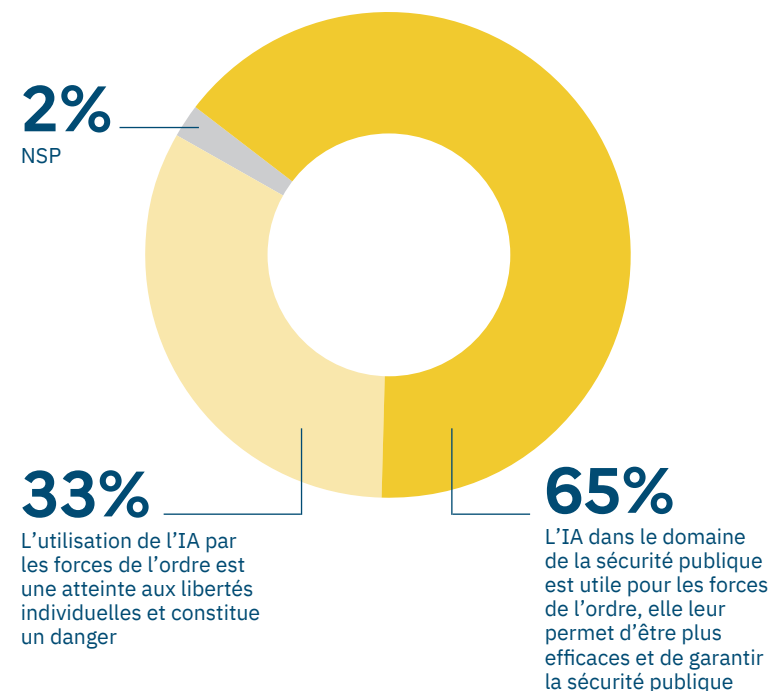
De façon quelque peu contre-intuitive, c'est la génération des 65-75 ans qui affiche le soutien le plus élevé à l'égard de l'intelligence artificielle utilisée par les forces de sécurité (73 % contre une moyenne générale de 65 %). À l'inverse, la génération des 25-34 ans se révèle la plus réticente, avec 38 % exprimant une défiance, contre 33 % en moyenne. Les divergences d'opinions apparaissent aussi en fonction de l'affiliation partisane selon un découpage plus classique : environ 80 % des sympathisants de la majorité présidentielle et des Républicains sont favorables à l'usage de l'IA

par les forces de l'ordre, alors que cette proportion tombe à 44 % chez les partisans de La France insoumise.

Lorsqu'on évalue sur une échelle de 1 à 10 la confiance en la fiabilité de l'IA dans l'analyse de données en temps réel à des fins de sécurité, la note moyenne obtenue est de 6,1. Plus précisément, 60 % des répondants attribuent une note supérieure à 6, tandis que près de 20 % expriment une réserve notable avec des notes inférieures à 5. Cette distribution reflète une perception globalement positive mais prudente de cette technologie émergente.

Face à l'essor de l'intelligence artificielle, 54 % des Français favorables à son usage estiment nécessaire une réglementation qui accorde toutefois une marge suffisante d'action aux forces de sécurité. Cette opinion est particulièrement présente chez les sympathisants de la majorité présidentielle (62 %), des LR (66 %), de Reconquête (77 %) et du RN (53 %). À l'opposé, 45 % prônent un encadrement législatif strict afin de protéger efficacement les libertés individuelles, position privilégiée notamment par les plus jeunes (51 %) et les sympathisants de gauche (PS à 62 %, EELV à 60 %, LFI à 58 %).

À propos de l'utilisation de l'intelligence artificielle (IA) par les forces de sécurité intérieure (police nationale, gendarmerie nationale, services de renseignement), de laquelle de ces opinions vous sentez-vous le plus proche ?

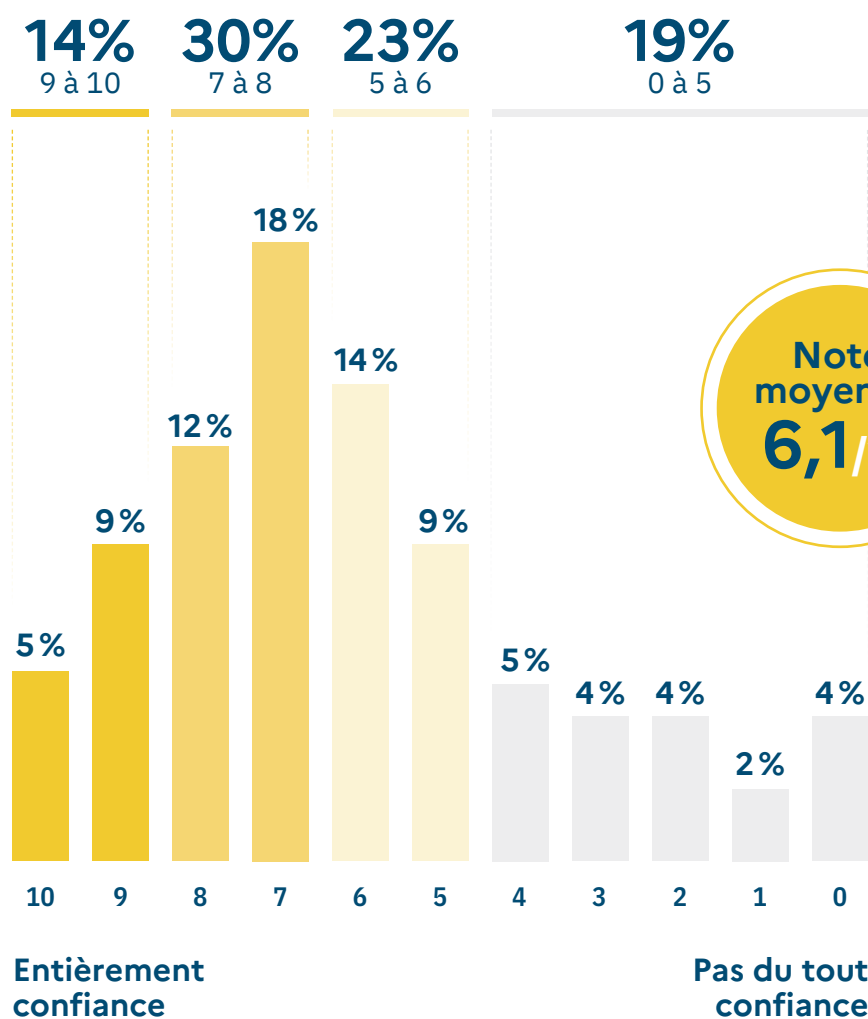


La perception de l'utilité des outils d'analyse automatisée varie selon le type de technologie concernée. Ainsi, parmi les Français favorables à l'IA, environ 85 % jugent essentiels ou utiles les dispositifs tels que les caméras fixes et embarquées ainsi que l'exploitation des données collectées *via* ces équipements. Par ailleurs, 78 % considèrent l'analyse des contenus diffusés sur les réseaux sociaux comme un levier stratégique indispen-

sable pour anticiper des menaces potentielles et enrichir les enquêtes traditionnelles. Toutefois, seuls 61 % des répondants attribuent une utilité élevée aux robots patrouilleurs, révélant ainsi une certaine méfiance vis-à-vis des systèmes autonomes.

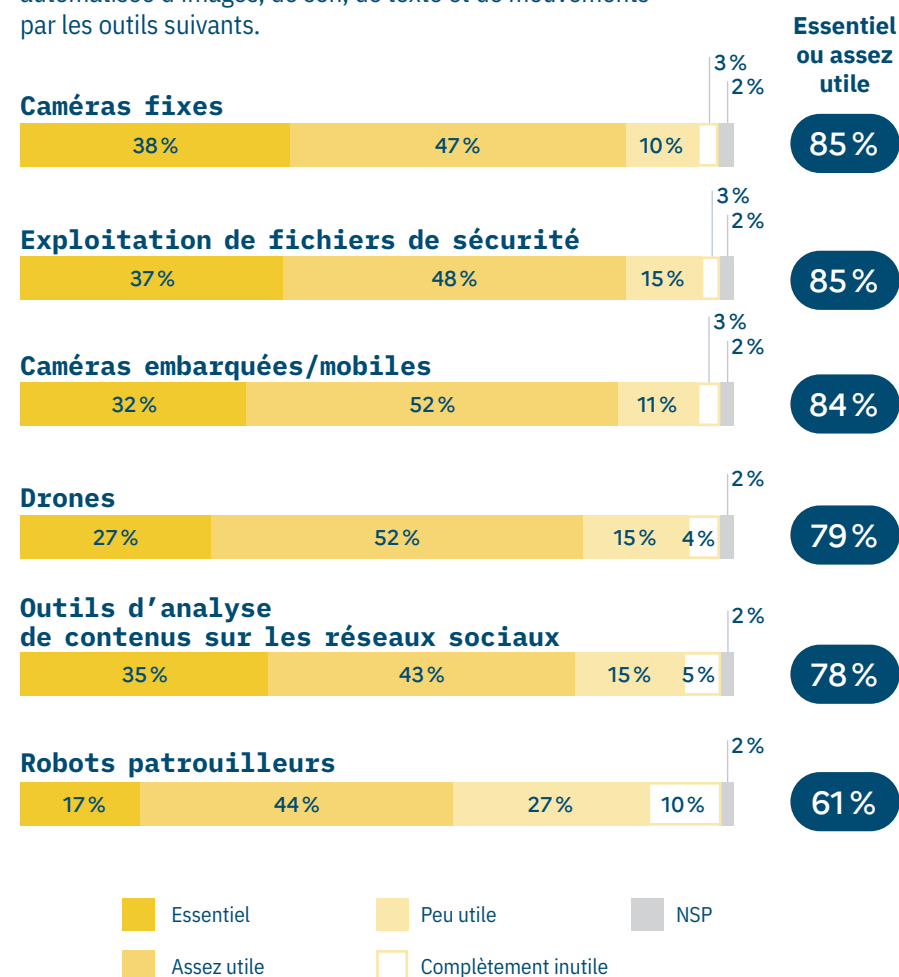
Sur le plan générationnel, les jeunes adultes âgés de 25 à 34 ans affichent un enthousiasme marqué et supérieur à la

Où classeriez-vous, sur cette échelle, votre niveau de confiance en la fiabilité de l'intelligence artificielle pour effectuer un travail d'analyse de données en temps réel (images, son, mouvements, etc.) à des fins de sécurité publique ?



LES 65-75 ANS AFFICHENT LE SOUTIEN LE PLUS ÉLEVÉ à l'égard de l'intelligence artificielle utilisée par les forces de sécurité.

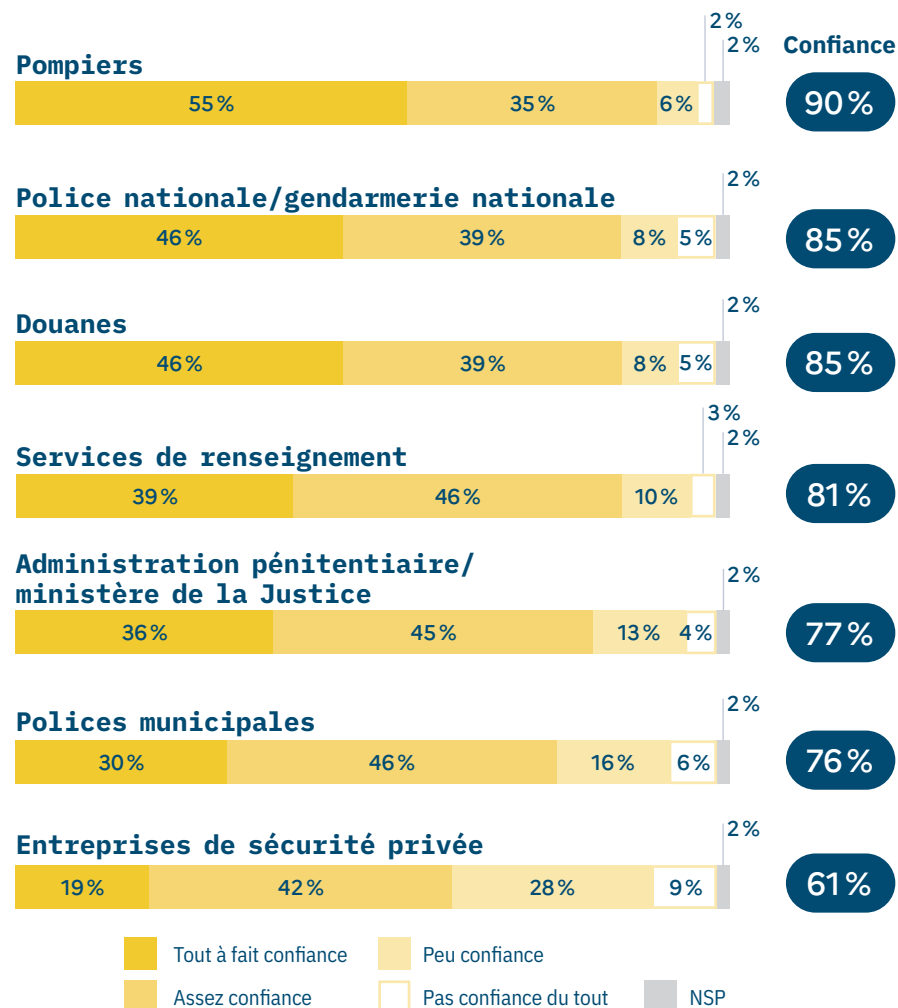
Évaluez le niveau d'utilité pour la sécurité publique de l'analyse automatisée d'images, de son, de texte et de mouvements par les outils suivants.



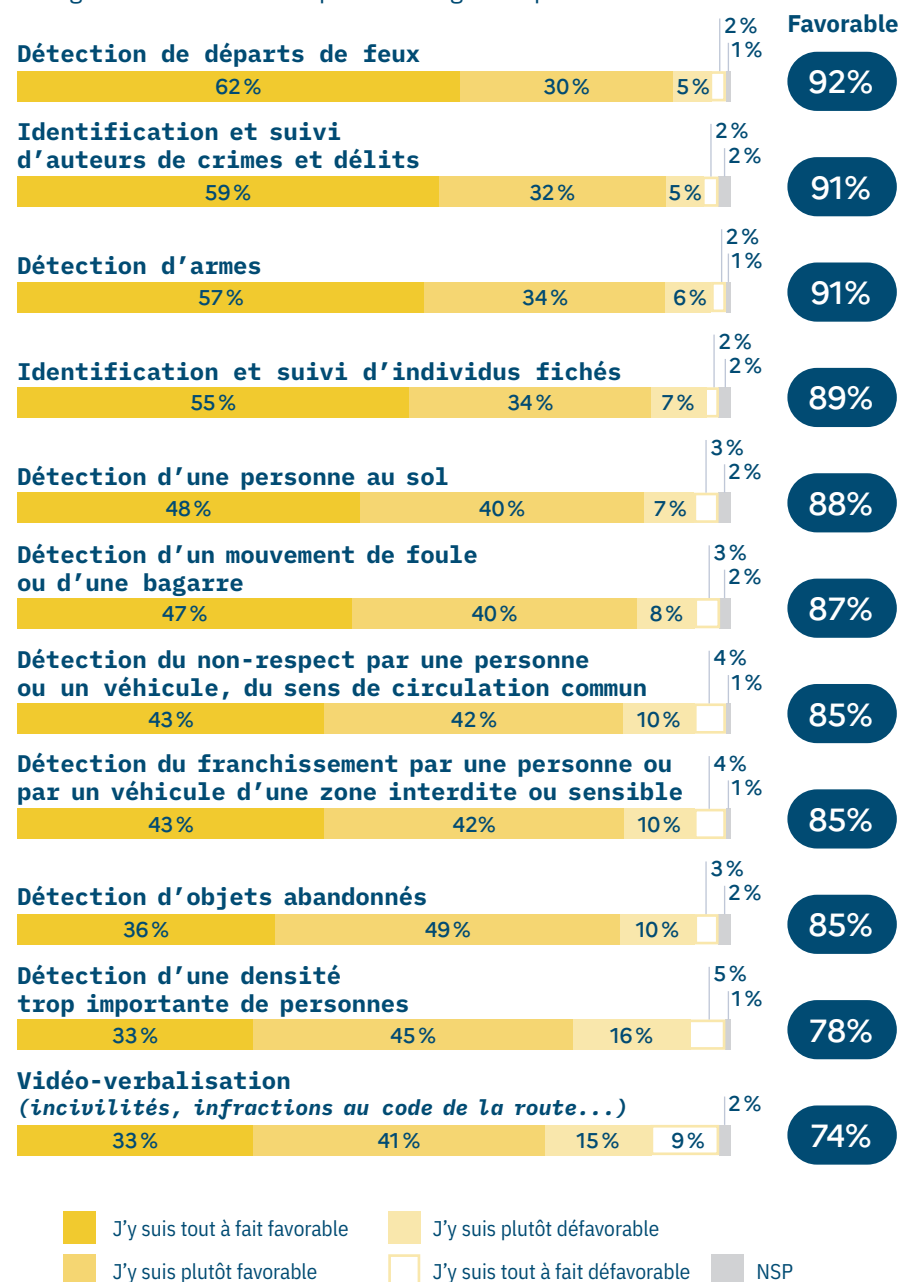
90%

font confiance aux pompiers
pour utiliser les outils d'analyse
en temps réel.

Avez-vous confiance dans les acteurs suivants pour utiliser
des outils d'analyse en temps réel, d'images, de sons, de texte
et de mouvements ?



Êtes-vous favorable à l'utilisation d'outils d'analyse, en temps réel,
d'images, de sons, de texte et de mouvements, par la police nationale
et la gendarmerie nationale pour les usages ci-après ?





moyenne envers toutes ces technologies. À l'inverse, la tranche des 18-24 ans exprime une légère réserve, tandis que les 65-75 ans privilégient nettement des dispositifs éprouvés comme les caméras et la gestion des données associées (91 % contre 85 % en moyenne).

Les affinités politiques influencent également la perception des technologies concernées : les sympathisants de la majorité présidentielle, des LR et du RN soutiennent massivement ces dispositifs. Les sympathisants de gauche, notamment de LFI, affichent un scepticisme relatif, avec par exemple 77 % d'approbation des caméras fixes (contre 85 % en moyenne) et 65 % pour les drones (contre 79 % en moyenne).

En termes de confiance envers les acteurs utilisant l'IA, un écart significatif apparaît entre les institutions publiques et privées. Ainsi, 90 % des Français accordent leur confiance aux pompiers, 85 % aux forces de police, de gendarmerie et aux douanes, et 81 % aux services de renseignement. Cette confiance chute à 61 % pour les entreprises de sécurité privée, ce qui révèle

une préférence marquée pour les acteurs étatiques, perçus comme plus légitimes.

Enfin, concernant les usages spécifiques de l'IA par les forces de l'ordre, les Français affichent une acceptation très élevée (environ 90 %) pour les applications destinées à prévenir ou réprimer des actes graves tels que la détection de départs d'incendies, l'identification de criminels ou d'individus fichés, et la détection d'armes. L'adhésion est légèrement moins forte (74 à 78 %) pour des usages touchant au quotidien des citoyens, tels que la verbalisation d'incivilités ou le contrôle routier automatisé.

En conclusion, bien que l'intelligence artificielle soit globalement perçue comme un atout précieux pour la sécurité publique, les Français témoignent d'une prudence marquée face à ses applications, notamment en raison de leur complexité et de leur automatisation accrue. Cette réserve se traduit par une exigence nette de transparence et d'un cadre légal clair, conciliant efficacité opérationnelle des forces de l'ordre et respect rigoureux des libertés individuelles. ■

Les données biométriques et la reconnaissance faciale

L'utilisation des données biométriques, au même titre que les autres technologies de sécurité, bénéficie d'un large soutien auprès de la population française, particulièrement lorsqu'elle demeure sous le contrôle strict de l'administration. Ainsi, plus de 80 % des Français considèrent que la police nationale, la gendarmerie nationale et les douanes sont légitimes pour exploiter les empreintes digitales, la reconnaissance faciale ou encore l'ADN. Ce niveau de confiance élevé s'étend également aux services de renseignement, approuvés par 79 % des répondants, ainsi qu'à l'administration pénitentiaire avec 76 % d'adhésion et aux polices municipales, bénéficiant d'un soutien à hauteur de 73 %. Cette forte confiance accordée spontanément aux institutions publiques peut s'expliquer par la perception de leurs missions – consubstantielles au principe d'intérêt général – ainsi que par le cadre réglementairement très strict de leur exercice.

À l'inverse, les entreprises privées, notamment les géants technologiques du secteur numérique (Gafam), suscitent une défiance nettement plus marquée : entre 40 % et 47 % seulement des Français leur accordent leur confiance en matière d'usage des données biométriques. Cette méfiance envers les acteurs privés traduit des préoccupations relatives aux risques liés à l'exploitation commerciale des données personnelles et aux éventuelles fuites de données sensibles. Toutefois, cette distinction tranchée entre acteurs publics et privés pourrait, là encore, progressivement s'atténuer avec les évolutions générationnelles. En effet, la génération des 18-24 ans exprime une confiance sensiblement supérieure envers les Gafam, avec 43 % d'approbation, contre seulement 20 % chez les 65-75 ans, ce qui révèle un écart générationnel significatif de 23 points.

En outre, si les hommes et les femmes accordent une confiance similaire aux forces de sécurité publique, les femmes en manifestent davantage envers les acteurs privés. Ainsi, 58 % des femmes se fient aux entreprises privées de sécurité, contre seulement 47 % des hommes. De même, le statut socioprofessionnel influence nettement cette confiance, les

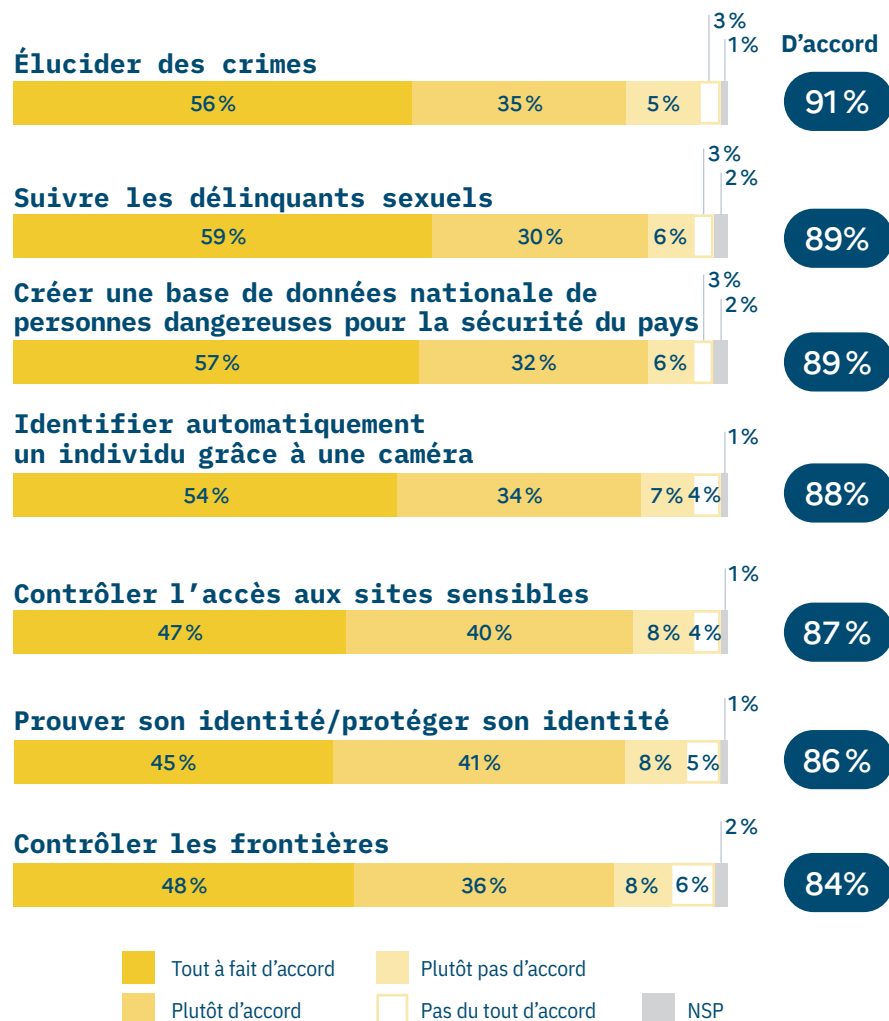
76 %

font confiance à l'administration
pénitentiaire pour exploiter
les données biométriques.

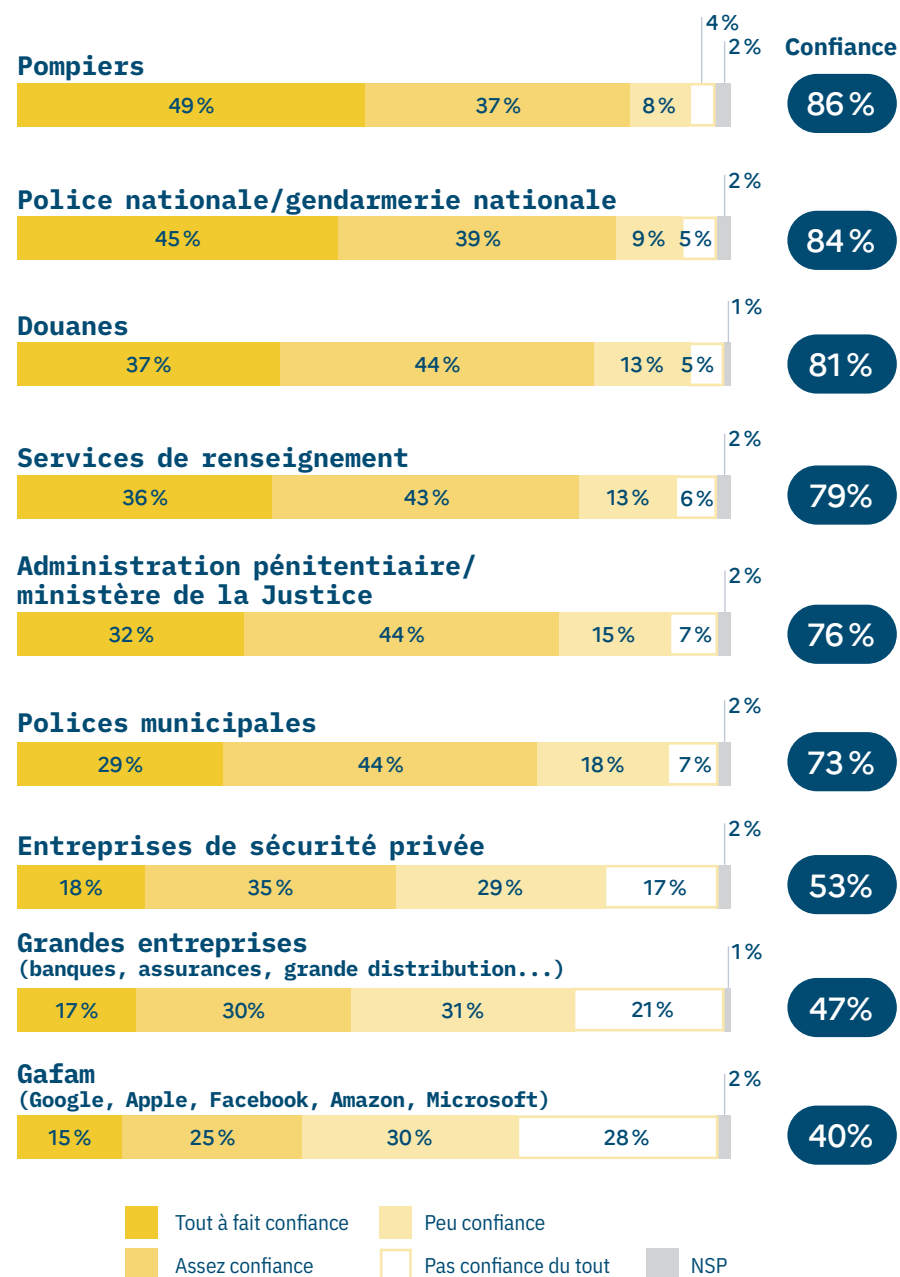
73 %

accordent leur confiance
aux polices municipales
pour détenir/exploiter
des données biométriques.

Êtes-vous d'accord avec l'utilisation de vos données
biométriques pour les usages ci-après ?



Avez-vous confiance dans les acteurs suivants pour posséder
et exploiter une partie de vos données biométriques ?



91 %

sont d'accord pour utiliser
les données biométriques
afin d'élucider des crimes.

inactifs étant plus sceptiques envers les acteurs privés (31 % seulement accordent leur confiance aux Gafam), comparativement aux CSP+ (43 %) et aux CSP- (44 %).

Concernant les objectifs spécifiques associés à l'usage des données biométriques, les Français montrent une très large adhésion dès lors qu'il s'agit d'assurer la sécurité collective. Ainsi, 91 % approuvent l'exploitation de ces données à des fins d'élucidation des crimes. Cette approbation reste extrêmement élevée à hauteur de 89 % pour le suivi des délinquants sexuels et la création de bases de données visant les individus considérés comme dangereux pour la sécurité nationale. Les autres finalités, telles que l'identification automatique *via* des caméras, le contrôle d'accès aux sites sensibles, la preuve d'identité ou

encore la surveillance des frontières, recueillent également un large soutien, oscillant entre 84 % et 88 % d'adhésion.

En conclusion, l'utilisation des données biométriques recueille une forte approbation lorsqu'elle est encadrée par l'administration, perçue comme légitime et digne de confiance. Cette confiance s'amoindrit nettement lorsqu'il s'agit d'acteurs privés, en particulier les grandes entreprises technologiques, ce qui traduit une méfiance persistante envers leur potentiel usage commercial ou intrusif. Les Français soutiennent massivement une utilisation strictement régulée et limitée à des fins sécuritaires clairement définies, illustrant une préoccupation constante pour la préservation des libertés individuelles face à des technologies particulièrement sensibles. ■

III. LES POLITIQUES PUBLIQUES DE SÉCURITÉ

36 %

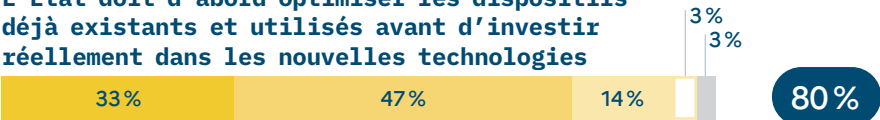
placent l'augmentation
des effectifs comme priorité
numéro un en matière
d'investissement.

Pensez-vous que l'État doive aller plus loin en matière de technologies de sécurité en expérimentant et en investissant davantage ou qu'il doive, au contraire, se contenter de ce qui existe déjà sur le marché pour renforcer la sécurité publique ?

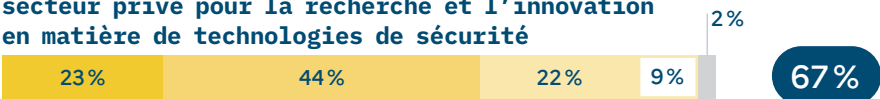
L'État doit investir dans la recherche de nouvelles formes de technologies afin d'améliorer les dispositifs de sécurité publique



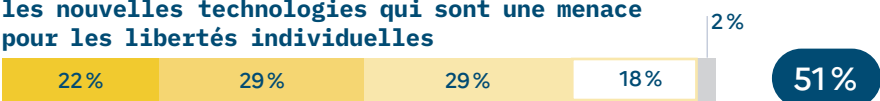
L'État doit d'abord optimiser les dispositifs déjà existants et utilisés avant d'investir réellement dans les nouvelles technologies



L'État devrait davantage s'appuyer sur le secteur privé pour la recherche et l'innovation en matière de technologies de sécurité



L'État ne doit pas investir dans les nouvelles technologies qui sont une menace pour les libertés individuelles



Oui, tout à fait Non, plutôt pas
Oui, plutôt Non, pas du tout NSP

Classez par ordre de priorité, selon vous, ces investissements pour garantir la sécurité publique.

Opinion sur la vidéoprotection	Défavorable	Favorable				
	31%	37%	28%	10%	10%	17%
Proximité partisane	Aucune préférence	40%	23%	17%	10%	9%
	RN	42%	18%	20%	9%	10%
	Reconquête	39%	17%	25%	8%	11%
	LR	37%	19%	22%	16%	6%
	Majorité présidentielle	29%	28%	24%	12%	7%
	EELV	32%	27%	18%	14%	9%
	PS	34%	26%	15%	13%	12%
	PCF	29%	27%	18%	14%	12%
	LFI	27%	30%	14%	15%	13%
% En premier		36%	24%	18%	11%	10%
Augmenter le nombre de policiers et gendarmes sur la voie publique						
Recruter des spécialistes des nouvelles formes de risque (cybercriminalité, cybersécurité, etc.)						
Investir dans des technologies de détection du risque en temps réel						
Investir dans des technologies d'aide à l'enquête						
Investir dans les équipements ordinaires (véhicules, locaux, armement, tenues)						

85 %

veulent que l'État
investisse davantage
dans les technologies.

67 %

sont favorables à davantage
d'implication du privé.

Nous savons ainsi que les Français affichent un soutien clair dans les différentes technologies de sécurité, mais qu'en est-il plus largement des politiques publiques de sécurité ? Quels investissements jugent-ils prioritaires ? Les Français manifestent globalement une confiance significative envers les technologies de sécurité, tout en restant profondément attachés à une présence humaine accrue des forces de l'ordre sur le terrain. Cette préférence est illustrée par le fait que 36 % des répondants considèrent l'augmentation du nombre de policiers et de gendarmes dans l'espace public comme la mesure prioritaire à mettre en œuvre en termes de politiques publiques de sécurité. Cette opinion est particulièrement répandue chez les générations les plus âgées, avec 43 % des 50-64 ans et 40 % des 65-75 ans la plaçant en tête, contre seulement 26 % des 25-34 ans. Cette priorité est également marquée chez les électeurs de droite, notamment parmi les sympathisants des LR (37 %), de Reconquête (39 %) et du RN (42 %), dépassant ainsi la moyenne générale de 36 %.

En deuxième position, 24 % des Français privilégient le recrutement de spécialistes des nouveaux risques tels que la cybercriminalité et la cybersécurité. Cette priorité est davantage exprimée par les

femmes (26 % contre 21 % chez les hommes), ainsi que par les sympathisants de gauche, notamment ceux de LFI (30 % contre seulement 18 % chez les électeurs du RN). Ce sujet est également jugé crucial par les générations extrêmes, les plus jeunes (18-24 ans) et les plus âgées (65-75 ans), avec 27 % d'entre elles y étant sensibles, contrairement aux générations intermédiaires (35-49 ans), où seulement 20 % y accordent une importance particulière.

Les investissements dans les technologies de détection en temps réel occupent la troisième position avec 18 %, suivis par les outils d'aide à l'enquête en quatrième place (11 %). En cinquième position viennent les investissements ordinaires tels que les véhicules, locaux et armements (10 %). Enfin, les questions du renforcement du lien entre les forces de l'ordre et la justice ainsi que l'amélioration des conditions de travail des forces de sécurité recueillent chacune 3 % des réponses, illustrant leur importance secondaire.

De manière générale, bien que les technologies de sécurité soient largement soutenues par la population française, ces dernières restent considérées comme moins urgentes que le renforcement humain, tant par l'augmentation des effectifs que par l'amélioration des

compétences face aux nouveaux défis sécuritaires. Cette distinction varie sensiblement selon les affiliations politiques, les électeurs de droite privilégiant une présence accrue et visible sur le terrain, tandis que les électeurs de gauche insistent davantage sur l'amélioration de l'expertise face aux nouveaux risques.

Concernant la confiance dans les technologies de sécurité, le niveau moyen est évalué à 6,9 sur 10. Plus précisément, 57 % des répondants attribuent une note égale ou supérieure à 7, dont 17 % attribuent des notes très élevées (9 ou 10). À l'inverse, seuls 9 % expriment une défiance claire, avec des notes inférieures à 5. Le niveau de confiance le plus élevé se retrouve parmi les 25-34 ans, avec une moyenne de 7,2 sur 10. Les clivages les plus importants apparaissent selon les affiliations politiques : les sympathisants du Parti communiste français (PCF) (7,9), du RN (7,6), de la majorité présidentielle et des LR (7,4) montrent une confiance particulièrement forte, alors que ceux de LFI et EELV expriment davantage de réserves avec une moyenne de 6,4 sur 10.

La perception positive des technologies de sécurité semble fortement liée à l'acceptation de la vidéoprotection : parmi les répondants ayant un haut

niveau de confiance (notes de 9 ou 10), seuls 1 % est opposé aux caméras, contre 39 % d'opposition parmi ceux affichant une confiance très faible (notes de 0 à 4). Cette corrélation révèle le rôle central de la vidéoprotection comme point de référence dans l'évaluation générale des technologies sécuritaires.

Par ailleurs, une large majorité de 85 % des répondants souhaite que l'État intensifie ses investissements dans la recherche technologique sécuritaire, une opinion particulièrement soutenue par les sympathisants de la majorité présidentielle (94 %) et des LR (93 %). En parallèle, 67 % des Français se disent favorables à une plus forte implication du secteur privé dans la recherche et l'innovation sécuritaire, malgré une moindre confiance dans sa capacité à gérer directement les données personnelles. Ces résultats indiquent clairement une préférence pour un modèle de coopération entre les secteurs public et privé, où l'État conserverait un rôle prépondérant et régulateur.

Toutefois, une majorité significative (80 %) estime prioritaire d'optimiser les dispositifs existants avant d'introduire de nouvelles technologies, traduisant une approche pragmatique privilégiant les outils éprouvés. Par ailleurs, 51 % des répondants expriment leur inquiétude quant à la menace potentielle que représentent les nouvelles technologies pour les libertés individuelles. Cette inquiétude est particulièrement vive chez les sympathisants du PCF (87 %), de LFI (65 %), ainsi que chez les jeunes adultes de 25-34 ans (71 %).

80 %

estiment prioritaire d'optimiser
l'existant avant de financer
de nouveaux outils.

63 %

souhaitent généraliser
après les Jeux olympiques
et paralympiques de Paris
l'expérimentation en cours.

En dépit de cette ambivalence, 63 % des Français croient en la possibilité de concilier sécurité renforcée et respect des libertés individuelles, contre 22 % qui en doutent et 15 % d'indécis. Ce soutien est plus marqué chez les générations âgées (66 % des 50-64 ans), les CSP+ (66 %), ainsi que chez les électeurs du RN (76 %), des LR (80 %) et de la majorité présidentielle (82 %). Les sympathisants de LFI, en revanche, sont notablement plus sceptiques, avec 41 % estimant impossible cette conciliation.

Le déploiement de la vidéosurveillance algorithmique (VSA) lors des Jeux olympiques et paralympiques de Paris en 2024, autorisé par la loi du 19 mai 2023, a ouvert la voie à des expérimentations élargies. Face aux résultats positifs, une prolongation jusqu'en septembre 2027

est envisagée en vue des Jeux olympiques d'hiver de 2030, événement qui se déroulera en France. Un projet de loi de mai 2025 vise ainsi à étendre cette technologie aux manifestations publiques majeures. Selon l'étude, 63 % des Français soutiennent cette généralisation, principalement les électeurs LR (82 %), de la majorité présidentielle (78 %) et du RN (76 %), alors que 21 % y sont opposés, notamment les sympathisants de LFI (38 %) et d'EELV (28 %).

En conclusion, si les Français approuvent largement le recours aux technologies sécuritaires avancées, ils restent attentifs à la protection des libertés individuelles, appelant à une régulation stricte garantissant un équilibre entre efficacité sécuritaire et respect des droits fondamentaux. ■

Paroles d'expert de la sécurité civile

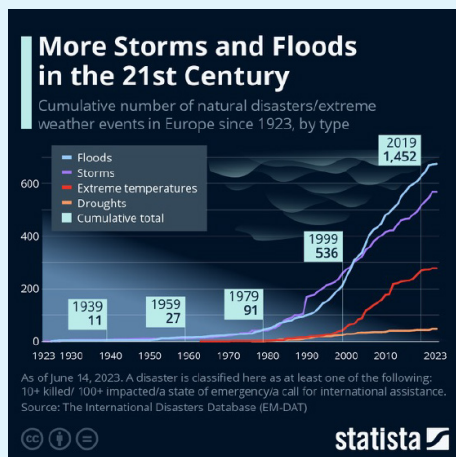
Participation de l'ANDSIS*
aux technologies de sécurité innovantes

* Association nationale des directeurs et directeurs-adjoints
des services départementaux d'incendie et de secours.



Bruno MAESTRACCI

Membre du bureau de l'ANDSIS



Vers une transformation numérique des services de secours

À l'échelle de notre planète, deux évolutions notables sont constatées en matière de risques naturels.

La première concerne l'augmentation de la fréquence d'occurrence mise parfaitement en lumière par la source fiable Statista, utilisées par les entreprises, les universités, les gouvernements et les médias du monde entier.

La seconde évolution est liée au niveau d'intensité de ces crises (incendies de forêt, sécheresses, canicules), conjuguée à des contraintes de ressources.

Ainsi, en France, la sécurité civile est active 365 jours par an, 24 heures sur 24, bien que ne représentant des coûts qu'à hauteur de 0,2 % du produit intérieur brut (PIB).

Ces deux caractéristiques conjuguées poussent, dans le monde entier, les services de secours à innover et à s'adapter.



En France, la sécurité civile est active 365 jours par an, 24 heures sur 24.

L'intelligence artificielle (IA) – notamment via l'apprentissage automatique, l'analyse d'images, la modélisation prédictive ou les systèmes embarqués – apparaît comme un levier majeur pour améliorer la détection, l'aide à la décision et l'efficacité opérationnelle dans les interventions des sapeurs-pompiers.

En 2024, les pertes économiques totales ont atteint environ 318 milliards de dollars étatsuniens, dont 137 milliards étaient assurés. Le protection gap (c'est-à-dire la part non assurée) reste donc de 181 milliards de dollars étatsuniens, soit 57 % des pertes totales. Selon Swiss Re (rapport Sigma de janvier 2025), les pertes mondiales assurées dues aux catastrophes naturelles, ont connu une croissance annuelle moyenne de 5 à 7 %. Le même rapport précise que les événements climatiques secondaires (inondations, feux de forêts, orages convectifs) en constituent une part croissante.

En France comme ailleurs, plusieurs initiatives se dessinent : des dispositifs de surveillance environnementale, des robots autonomes, des outils d'aide à la décision en temps réel, des systèmes

Bruno MAESTRACCI est contrôleur général de sapeurs-pompiers. Il dirige le service départemental d'incendie et de secours (Sdis) de Seine-et-Marne (77). Il a été chef du détachement français à Yogyakarta (Indonésie), qui sera frappé par un tremblement de terre en 2006. Il a aussi été chef de la mission européenne pour le tremblement de terre d'Haïti en 2021. Il est membre du bureau national de l'Association des directeurs et directeurs départementaux adjoints des services d'incendie et de secours (ANDSIS).



de localisation ou de *monitoring* des équipiers.

Pour les sapeurs-pompiers français, l'enjeu est double puisqu'il s'agit d'accroître la sécurité des populations tout en préservant les intervenants en opération, et dans un contexte budgétaire de plus en plus restreint, sans agence de développement ni financements de l'État dédiés.

Nous examinerons d'abord les réalisations et perspectives françaises, puis les développements marquants à l'international, avant de discuter des défis et orientations possibles.

Le développement en France

1. Détection précoce des incendies : le projet Pyronear en forêt de Fontainebleau

L'un des exemples les plus médiatisés de l'IA appliquée aux pompiers en France est le projet **Pyronear**, déployé dans la forêt de Fontainebleau¹ (Seine-et-Marne).

- Des caméras fixées en hauteur (sur des pylônes ou châteaux d'eau) prennent une image toutes les 30 secondes. Ces images sont traitées localement par un micro-ordinateur embarqué, équipé d'un modèle d'IA pour détecter des fumées (ou les indices d'un début d'incendie).

- Dès qu'une anomalie est détectée, un signal est envoyé aux sapeurs-pompiers, qui peuvent zoomer sur l'image pour confirmer ou infirmer l'alerte.
- L'approche est dite « sobre en énergie » et *open source*, ce qui permet des expérimentations à bas coût et une plus grande transparence².
- L'objectif est de détecter le plus tôt possible un départ de feu pour limiter la mobilisation, la consommation d'eau, et le risque de propagation.

Ce type d'initiative illustre la tendance à rapprocher l'IA au plus près du terrain, dans des architectures embarquées ou distribuées, plutôt que *via* des supercalculateurs seuls.

Il faut noter que le CAL Fire, *California Department of Forestry and Fire Protection* (agence responsable de la gestion des incendies de forêt dans l'État de Californie), dispose de 17 000 caméras de surveillance, sans recours systématique à l'IA.

2. Caméras intelligentes dans les territoires

D'autres services départementaux d'incendie et de secours (Sdis) explorent des systèmes analogues.

- Ces dispositifs de détection précoce connectés aux centres de traitement de l'alerte sont déjà mis en œuvre dans des départements comme les

Landes (40) ou la Sarthe (72) et plusieurs autres projets sont en cours de développement.

- Le Sdis 37 (Indre-et-Loire) a installé une douzaine de caméras sur des châteaux d'eau, connectées par fibre optique, pour surveiller les zones à risque sur 360°. Le coût total (infrastructures notamment) est estimé à 1,8 million d'euros³.
- Ces systèmes peuvent repérer, non seulement les feux en zone naturelle, mais aussi des véhicules en feu ou des bâtiments.
- Une difficulté mentionnée est la réutilisation des données existantes pour rendre l'IA plus « frugale » (moins gourmande en ressources, tirant parti des capteurs déjà déployés).

3. Robotique : Colossus et Shark robotics

En France, la robotique est un domaine en avance, notamment grâce à l'entreprise **Shark robotics**, qui conçoit des robots destinés à intervenir dans des zones dangereuses, avec des capacités de reconnaissance et d'action.

- Colossus⁴ est un robot téléopéré capable de monter des escaliers, équipé d'une caméra thermique, d'un canon à eau, de chenilles, etc. Il peut être utilisé pour des missions de reconnaissance ou d'attaque dans des environnements trop dangereux pour les pompiers. Il a notamment été

employé lors de l'incendie de Notre-Dame de Paris en 2019.

- Le recours à des robots permet de limiter l'exposition humaine, mais se heurte à des contraintes telles que la robustesse, la communication en milieu hostile (fumée, rupture de réseau) et la coordination avec les équipes humaines.

4. Recherche, IA embarquée et systèmes de surveillance

Outre les systèmes de détection, des initiatives plus prospectives se développent dans la recherche.

Le portail numérique des ressources de la sécurité civile de l'École nationale supérieure des officiers de sapeurs-pompiers, **PNRS-ENSOSP**⁵, traite des enjeux de l'IA dans la gestion des crises, et notamment de la modélisation des feux de forêt, de la prédiction, et de l'aide à la décision opérationnelle.

Par ailleurs, des outils plus généralistes sont explorés, comme **Open rescue**⁶, un système basé sur des drones visant à automatiser la recherche de personnes disparues, utilisé dans des exercices par le Sdis 74 (Haute-Savoie).

L'idée est que l'IA ne s'applique pas seulement à la détection des feux, mais aussi au sauvetage, aux missions de recherche, aux effets secondaires (par





exemple la pollution, la qualité de l'air et à la protection des intervenants.

5. Limites et points de vigilance

Malgré les progrès, plusieurs défis freinent la généralisation de ces systèmes :

- **fiabilité et faux positifs ou négatifs** : une détection erronée ou manquée peut nuire à la confiance ou gaspiller des ressources ;
- **infrastructure** : les réseaux (fibre, connectivité dans les zones rurales) et l'énergie (alimentation des capteurs, systèmes embarqués) représentent un coût non négligeable ;
- **acceptation opérationnelle** : l'IA doit s'intégrer aux processus existants, respecter les doctrines d'intervention, et être comprise par les sapeurs-pompiers (explicabilité, transparence) ;
- **réglementation** : en France, certaines modalités de vol de drones ou de surveillance stricte sont encadrées légalement ;
- **souveraineté et open source** : l'option *open source* dans des projets comme Pyronear constitue un avantage pour la transparence et l'adaptabilité, mais pose des questions de maintenance, d'industrialisation et de support ;
- **robustesse en conditions extrêmes** : fumée, obscurité, structures instables, perturbations de communication, etc. ;

- **interopérabilité** : les systèmes doivent pouvoir dialoguer avec les centres de commandement, les systèmes d'information géographique (SIG), les bases de données météo, etc.

Développements internationaux : ce que font les sapeurs-pompiers dans le monde

Dans d'autres pays, l'IA et la robotique appliquées à la lutte contre les incendies ou aux missions de secours se développent activement. Voici quelques exemples saillants.

1. Prédiction, modélisation et avertissement anticipé

- **P-Flash**⁷. L'institut américain *National Institute of Standards and Technology* (NIST) a développé P-Flash, un modèle d'IA capable de prédire des phénomènes de *flashover* (ce moment dangereux où une pièce s'enflamme violemment) dans les bâtiments. Même avec des capteurs thermiques partiellement défectueux, le modèle peut anticiper une situation critique.
- **AI enabled smart firefighting**⁸. Le NIST a aussi monté un projet destiné à définir des modèles de prévision en temps réel (propagation, évacuation, scénarios) afin d'aider l'intervention.
- **Technosylva**⁹. En Californie, des plateformes d'IA utilisent des données

météorologiques, de végétation, de topographie pour produire des cartes de risque et aider les sapeurs-pompiers à prévoir les incendies et leur dynamique.

- **The European centre for medium range weather forecasts (ECMWF)**¹⁰. Le projet du centre européen combine l'IA avec des données satellites¹¹ pour prévoir des incendies au niveau global sur des résolutions de l'ordre de 9 km.

2. Robotique, drones et systèmes autonomes

- **Robots terrestres** : des entreprises comme **Shark robotics** (France) exportent leurs solutions à l'international. Le robot **Colossus** est utilisé aussi dans d'autres contextes (par exemple en Ukraine).
- **Drones IA** :
 - En Allemagne, **Dryad networks**¹² a présenté le drone **Silvanguard**, combiné à un réseau de capteurs (Silvanet), pour détecter des incendies naissants et intervenir rapidement.
 - **Data blanket**¹³ (États-Unis) utilise des drones autonomes et l'IA pour cartographier le périmètre des feux, fournir des informations temps réel aux pompiers.
 - En Europe, des drones à longue portée intégrés avec AI sont testés aux Pays-Bas (par exemple ceux de l'entreprise Avy BV¹⁴) pour la détection précoce des feux.

- **Robots polyvalents** :

- **Shark robotics**, déjà mentionné, promeut des robots pouvant agir dans diverses missions (transport de charge, reconnaissance, sauvetage)¹⁵.
- L'initiative **FireAid project** (en collaboration avec le *World Economic Forum* – WEF) vise à structurer un réseau mondial d'IA et de fournisseurs de technologies pour les incendies, promouvoir le partage de données et l'expérimentation multisectorielle.

3. Systèmes embarqués, vision artificielle et réalité augmentée

- De nombreuses études universitaires montrent l'intérêt de l'IA appliquée à la perception dans des milieux encombrés d'obscurité ou de fumée. Par exemple, le dataset **Fire360**¹⁶ propose un banc de test pour l'IA en images dégradées, intégrant localisation, reconnaissance d'actions et raisonnement en contexte d'urgence ; porté par l'université Cornwell (États-Unis).
- Des travaux intègrent la **réalité augmentée**¹⁷ et le *deep learning* pour aider les sapeurs-pompiers à localiser les chemins de secours, repérer les points d'intérêt (victimes, obstacles), surtout dans des environnements complexes (*integrating deep learning and augmented reality...*).





Comparaison France / monde : points forts et freins

Dimension	France	Ailleurs / modèles internationaux
Proximité terrain, embarqué	Pyronear montre la capacité à déployer des algorithmes sur du matériel simple, <i>open source</i> .	À l'international, beaucoup d'efforts restent centralisés ou <i>via</i> des plateformes <i>cloud</i> .
Robotique avancée	Robot Colossus de Shark robotics offre un cas crédible, déjà utilisé.	Des robots similaires existent, mais ils sont rares. La coordination robot-humain reste expérimentale.
Data et capteurs	Caméras fixes, réutilisation de réseaux existants, <i>open source</i> .	Combinaison de satellites, drones, capteurs IOT variés, mais avec coûts plus élevés.
Prédiction / modélisation	Initiatives nationales limitées en nombre.	Projets comme P-Flash, ECMWF, Technosylva ayant des ressources académiques et industrielles plus grandes.
Acceptation opérationnelle / doctrine	En expérimentation, avec prudence et pilotage.	Dans les zones à fort risque (Californie, Australie), l'IA est aujourd'hui déjà intégrée dans les processus stratégiques.
Contraintes réglementaires et infrastructures	Débits, réseau, réglementation du survol de drones, vie privée.	Ces contraintes existent partout, mais certains pays ou états fédérés disposent de cadres plus permissifs pour l'innovation.

- Le projet **PyroGuardian**¹⁸ propose un système *Internet of Thing* (IOT ou Internet des objets)/IA combinant capteurs portés (température, fréquence cardiaque, position GPS) pour surveiller en temps réel l'état des sapeurs-pompiers sur le terrain, permettant aux commandants des opérations de secours de retirer automatiquement des unités en danger.
- Des systèmes embarqués portables multispectres (caméra thermique, capteurs gaz, image visible¹⁹) peuvent inspecter l'environnement post-incendie ou soutenir les recherches, détecter des *hot spots* ou des gaz dangereux.

4. Perspectives régionales et retours d'expérience

- Dans des zones sujettes à des incendies fréquents (Californie, Australie, Méditerranée), l'IA est déjà intégrée dans la planification, la surveillance (satellites, capteurs), l'alerte et les prévisions.
- En Europe, certaines expérimentations combinent satellites, drones et IA pour couvrir des zones étendues, avec une cadence de prédiction d'un point tous les jours sur dix jours (par exemple ECMWF) pour alerter les zones vulnérables.
- Le déploiement à grande échelle reste souvent limité par le coût, les infrastructures, la coordination institutionnelle,

les contraintes réglementaires (air, vol de drone, vie privée).

On voit que la France occupe une position pertinente, notamment pour ce qui est de l'*open source*, ses robots autonomes, et de l'ancrage sur le terrain.

Toutefois, les ressources, l'échelle et la capacité de modélisation globales restent souvent plus modestes que dans les grands projets internationaux.

Enjeux, défis et orientations futures

Le développement de l'IA chez les sapeurs-pompiers n'est pas qu'une question technologique : il s'agit de penser l'intégration dans un système opérationnel, humain, institutionnel. Voici quelques pistes de réflexion :

- Interopérabilité et standardisation.** Pour qu'un capteur, un drone, un robot ou un module IA puissent « parler » avec un centre de commandement, il faut définir des protocoles, des formats de données (géolocalisation, métadonnées, alertes), des *application programming interface* (API ou interface de programmation d'application). L'adoption de standards internationaux est un atout.
- Formation et acceptabilité humaine.** L'IA ne doit pas rester une boîte noire. Les sapeurs-pompiers doivent comprendre les alertes, pouvoir les





remettre en question, et garder la main sur la décision. L'explicabilité, la confiance, la formation sont des enjeux essentiels.

3. **Évaluation et rétroaction sur le terrain.** Il faut mettre en place des boucles de retour (*feedback*) pour ajuster les modèles, capturer les erreurs, corriger les biais. Des phases pilotes sont indispensables avant déploiement massif.
4. **Robustesse et résilience.** Les systèmes doivent résister aux conditions extrêmes : fumée dense, chaleur, destruction d'infrastructures, interruption de communication. Il faudra prévoir des modalités de fonctionnement dégradé.
5. **Hybrider physique et *data-driven*.** L'IA pure, fondée uniquement sur les données, peut être complétée par des modèles physiques (modèles de propagation, thermodynamique) ou des modèles hétérogènes hybrides. Cette approche combinatoire est souvent plus robuste.
6. **Déploiement progressif, modularité.** Plutôt que de viser un système monolithique, on gagne à déployer des modules successifs : détection, modélisation, robotique, assistance aux équipes, etc.
7. **Souveraineté numérique et *open source*.** En France et en Europe, privilégier des solutions qui respectent la souveraineté des données, la confidentialité, et qui soient maintenables

à long terme est un avantage stratégique (par exemple, Pyronear est un système *open source*).

8. **Financement, coûts et partenariats publics/privés.** Les coûts (capteurs, réseaux, calcul, recherche et développement) restent un frein. Les partenariats avec des start-up, des centres de recherche, des fonds publics (par exemple des dispositifs d'innovation territoriale) seront cruciaux.
9. **Éthique, vie privée et régulation.** La surveillance (caméras, drones), le traitement d'images ou de données sensibles, la responsabilité des décisions prises par des IA, doivent être encadrés. Il faut un cadre juridique et éthique clair.
10. **Mutualisation et partage de données.** Les gains seront plus significatifs si les Sdis, les régions et les pays partagent les données (sous conditions sécurisées). Le partage des retours d'expérience accélère l'innovation.

Conclusion

Le développement de l'IA dans le domaine des sapeurs-pompiers est en pleine émergence. En France, des projets tels que Pyronear, l'implantation de caméras intelligentes dans les Sdis ou l'usage de robots comme Colossus montrent les premiers jalons d'une trans-formation.

À l'international, des initiatives de modélisation prédictive, de drones autonomes, de systèmes embarqués et de réalité augmentée montrent l'étendue du potentiel.

Cependant, pour que l'IA devienne un outil de terrain crédible et durable, il faut surmonter des obstacles techniques, humains, réglementaires et organisationnels. Le chemin est encore long, mais les enjeux (en termes de vies sauvées, de ressources optimisées et de sécurité des intervenants) justifient largement l'effort.

¹ <https://portail.free.fr/actualites/monde/dans-la-foret-de-fontainebleau-une-ia-eco-responsable-sentraine-a-detecter-les-incendies/>

² <https://www.france24.com/fr/info-en-continu/20250923-%C3%A0-fontainebleau-une-ia-sobre-en-%C3%A9nergie-s-entra%C3%A9ne-%C3%A0-d%C3%A9tecter-les-feux-de-for%C3%AAt?>

³ <https://www.banquedesterritoires.fr/ia-territoriale-reutiliser-les-donnees-existantes-reste-le-grand-defi>

⁴ https://fr.wikipedia.org/wiki/Colossus_%28robot%29

⁵ <https://pnrs.ensosp.fr/Default/~~/default/sous-thematique-recherche-et-innovation.aspx>

⁶ <https://www.helicomicro.com/2025/02/25/open-rescue/>

⁷ <https://www.nist.gov/news-events/news/2021/06/how-ai-could-alert-firefighters-imminent-danger>

⁸ <https://www.nist.gov/programs-projects/artificial-intelligence-enabled-smart-firefighting>

⁹ <https://www.theguardian.com/world/article/2024/aug/15/how-ai-is-revolutionising-how-firefighters-tackle-blazes-and-saving-lives>

¹⁰ <https://www.ecmwf.int/en/about/media-centre/news/2025/ecmwfs-ensemble-ai-forecasts-become-operational>

¹¹ <https://www.lombardodier.com/fr/insights/2025/june/predicting-the-flame.html>

¹² <https://apnews.com/article/germany-drones-wildfires-ai-b6ba6b7729f383fe4ffad4dee609f3f1>

¹³ https://en.wikipedia.org/wiki/Data_Blanket

¹⁴ https://en.wikipedia.org/wiki/Drones_in_wildfire_management

¹⁵ https://aiforgood.itu.int/robotics-and-ai-to-predict-and-fight-wildfires/?utm_source=chatgpt.com

¹⁶ <https://arxiv.org/abs/2506.02167>

¹⁷ <https://arxiv.org/abs/2107.11043>

¹⁸ <https://arxiv.org/abs/2411.03654>

¹⁹ <https://arxiv.org/abs/2104.00876>

Parole d'experts de la sécurité publique



Marc BOGET

Général de corps d'armée,
directeur de l'Agence
du numérique des forces
de sécurité intérieure (ANFSI)

Dans un paysage sécuritaire en constante évolution, le numérique a émergé comme un pilier essentiel pour la gendarmerie nationale. Les gendarmes utilisent aujourd'hui une multitude d'outils numériques pour optimiser leur action, allant de la collecte de renseignements à la gestion opérationnelle sur le terrain. Cette transformation numérique facilite les interactions avec les usagers et offre une efficacité accrue dans la résolution des enquêtes, la coordination des opérations tout en permettant une meilleure gestion des ressources. Pour autant, à ces avantages, sont associés des défis complexes, notamment en matière de gestion des compétences numériques dans la durée, de cybersécurité, d'intelligence artificielle, de mobilité, de protection des données ou de conduite des projets.

À ce titre, les résultats de l'enquête sur les technologies de sécurité innovantes, réalisée en juillet 2024 auprès d'un échantillon de la population française, confirment que ces défis demeurent prioritaires et bénéficient d'une vision largement favorable (par exemple 65 % des répondants estiment que l'intelligence artificielle est utile pour les forces de l'ordre).

”

La gendarmerie nationale a mis en place des outils numériques performants et résilients correspondant aux besoins des concitoyens et des gendarmes.

Ces priorités numériques viennent compléter le plan de gouvernance numérique de la gendarmerie nationale de 2025 et devront permettre de construire des outils adaptés aux besoins, s'appuyant sur une structure résiliente et sécurisée, en éveil sur les évolutions technologiques, développés par une ressource interne formée et coordonnés grâce à une gouvernance modernisée.

Force armée placée au plus près de nos concitoyens, la gendarmerie nationale a, depuis plusieurs années, investi dans le domaine des technologies de sécurité innovantes permettant un meilleur rendu de services au profit de nos concitoyens tout en accélérant et facilitant le travail des gendarmes en charge de la protection de 98 % du territoire métropolitain et ultramarin. Se réformant en permanence, faisant de la transition numérique une priorité forte du général d'armée Hubert Bonneau, directeur général de la gendarmerie nationale (DGGN), l'institution veille à placer en permanence l'humain au cœur de ses actions.

S'inscrivant parfaitement dans les priorités de la Direction générale de la gendarmerie nationale (DGGN), s'appuyant

Recruté sur titre et diplômé de l'école CentraleSupélec, le Général de corps d'armée **Marc BOGET** dirige l'Agence du numérique des forces de sécurité intérieure (ANFSI) depuis le 1^{er} juillet 2025.

Fort d'un parcours riche, il a été commandant de peloton de gendarmerie mobile, commandant de la compagnie de gendarmerie départementale de Besançon, commandant du groupement de gendarmerie départementale de l'Oise, directeur adjoint du numérique au ministère de l'Intérieur, expert en gouvernance des systèmes d'information et de communication, commandant de la gendarmerie dans le cyberspace, et chargé de la stratégie digitale et technologique auprès du directeur général de la gendarmerie nationale.





résolument sur l'Agence du numérique des forces de sécurité intérieure (ANFSI), acteur technique majeur, ces priorités s'insèrent dans une démarche de transformation numérique volontariste.

Dans un monde en constante mutation technologique et face à l'émergence de nouvelles formes de menaces, la gendarmerie nationale innove pour maintenir son efficacité opérationnelle et sa proximité avec les citoyens. La transformation numérique, incarnée par le concept de « Gendarmerie numérique 4.0 », représente non seulement une évolution nécessaire, mais une véritable révolution dans son approche de la sécurité publique et de la police judiciaire.

S'appuyant résolument sur des technologies *open source* qui permettent une plus grande maîtrise interne, le poste de travail des gendarmes est passé sous système d'exploitation Linux dès 2005. Par ailleurs, pour renforcer notre souveraineté numérique, le système d'exploitation des terminaux Néo est basé sur un socle *open source* entièrement maîtrisé par l'ANFSI en lien avec l'Opérateur des systèmes d'information interministériels classifiés (OSIIC) relevant du Secrétariat général de la défense et de la sécurité nationale (SGDSN).

C'est ainsi que la gendarmerie nationale a mis en place des outils numériques performants et résilients correspondant

aux besoins des concitoyens et des gendarmes.

En effet, le numérique est au cœur des nouveaux modes de consommation de services, la sécurité en faisant pleinement partie. C'est dans ce cadre que la gendarmerie a porté un effort tout particulier pour offrir de nouveaux services numériques aux Français.

La plainte en ligne (PEL) dont le lancement a été effectué en octobre 2024, continue par exemple à évoluer à la lumière des nouvelles technologies offertes et des nouveaux besoins des concitoyens. Elle voit ainsi son périmètre infractionnel augmenté et la mise en place, avant la fin de l'année 2025, de la visioconférence comme modalité d'échanges avec la police et la gendarmerie nationale, qui permettra de limiter les besoins de déplacement des victimes. Véritable plateforme d'échange entre le plaignant et les forces de sécurité intérieure, les capacités du coffre-fort numérique permettant à tous de suivre l'évolution de la procédure seront améliorées. Ayant l'objectif d'agglomérer tous les parcours des victimes, cette plateforme verra l'intégration, dans les trois prochaines années, de l'ensemble des télé-services de plainte et de signalement (Perceval, Thésée, Pharos, Signal IGGN...).

La démocratisation du numérique est également synonyme d'augmentation

des risques cyber et des besoins de sécurité associés. Consciente du caractère exponentiel de cette menace qui touche l'ensemble de nos concitoyens, la gendarmerie nationale s'est rapidement investie dans ce domaine et a contribué, en lien avec Cybermalveillance et la police nationale, à la mise en place fin 2024 de la plateforme 17Cyber pour une meilleure prise en compte des victimes de ces cybermalveillances. Fortement sollicitée, cette plateforme sera amenée à évoluer pour s'adapter aux nouvelles menaces et à leur bonne prise en compte. Un effort tout particulier sera réalisé pour continuer de faire connaître ce dispositif et accentuer l'intégration du *widget* associé sur l'ensemble des sites institutionnels et professionnels. Plus de 10000 cyber-enquêteurs sont par ailleurs formés à ces nouvelles menaces. Conscient que l'ensemble des services doit être accessible par tous, un investissement particulier est également réalisé pour faire en sorte qu'il soit compréhensible et utilisable par les personnes en situation de handicap en appliquant, dès sa conception, le référentiel général d'amélioration de l'accessibilité (RGAA) à tout nouvel outil tout en expertisant la mise à niveau de ceux existants.

Enfin, un service efficient pour le citoyen passe également par une réponse la plus immédiate possible lorsqu'il est au contact des gendarmes, d'où la nécessité pour ces derniers de disposer des outils

leur permettant de travailler en parfaite mobilité. Le principe du « aller vers » conduit les gendarmes au plus près des victimes dans une logique d'une plus grande proximité.

La gendarmerie numérique 4.0 incarne ainsi l'ambition de construire une force de sécurité augmentée, au plus près des territoires et des élus locaux en leur apportant des solutions adaptées aux spécificités des collectivités, où l'humain demeure au cœur du dispositif, soutenu par les technologies les plus avancées. Cette transformation s'articule autour de trois dimensions fondamentales qui se complètent et se renforcent mutuellement : l'innovation technologique (déploiement de l'intelligence artificielle par exemple), l'adaptation de notre organisation et de notre processus (renforcement de la résilience numérique) et enfin le développement du capital humain (valorisation des compétences numériques).

S'inscrivant dans une vision prospective à 360 degrés, cette transformation numérique permet à la gendarmerie nationale de maintenir son excellence opérationnelle tout en renforçant sa capacité à protéger les citoyens dans l'espace numérique. Son engagement reste intact : assurer la protection des personnes et des biens au service de la Nation, en adaptant ses moyens et ses méthodes aux défis du XXI^e siècle. ■



Louis LAUGIER

Directeur général
de la police nationale

Technologies de sécurité : avancer avec la confiance de nos concitoyens, agir avec responsabilité

Alors que les évolutions technologiques transforment nos sociétés, les forces de sécurité ne peuvent ni ne doivent rester à l'écart de ces mutations. Pour la police nationale, l'enjeu n'est pas seulement d'accompagner ces évolutions, mais de les maîtriser, les encadrer, et les expliquer. Cette enquête nous donne un signal clair : nos concitoyens soutiennent, dans leur immense majorité, l'usage par la police nationale des technologies de sécurité. 91 % des sondés font confiance aux forces de l'ordre pour exploiter des outils d'analyse d'images enregistrées sur la voie publique et 84 % pour le traitement de leurs données biométriques qui repose pourtant sur des techniques plus intrusives. Ce soutien, nous le recevons avec le sens des responsabilités. Il nous engage à faire toujours mieux. Et surtout, à ne jamais dévier de nos valeurs fondamentales : le respect des droits, la transparence et la confiance de nos concitoyens.



*Pour la police nationale,
l'enjeu n'est pas seulement
d'accompagner ces évolutions,
mais de les maîtriser,
les encadrer et les expliquer.*

Une adhésion forte, reflet d'un besoin de protection et d'efficacité de l'action policière

Près de 90 % des Français approuvent l'usage de la vidéoprotection dans l'espace public. 91 % des sondés font confiance aux caméras fixes. Les caméras piétons, utilisées lors de nos interventions, sont également largement soutenues : 87 % des sondés y sont favorables. Pour 76 % d'entre eux, ces outils permettent de mieux assurer la sécurité de la voie publique et contribuent à la résolution des enquêtes. Même les technologies les plus avancées – analyse d'images par intelligence artificielle (IA), usage ponctuel de drones et utilisation de la biométrie – sont perçues comme utiles, notamment dans la gestion des grands événements ou des situations de crise et pour la résolution des enquêtes. Ces chiffres traduisent un besoin profond de sécurité, mais aussi une attente d'efficacité à laquelle la police nationale s'efforce de répondre. À titre d'illustration, en 2024, ce sont près de 12 500 suspects qui ont été identifiés grâce au fichier des empreintes digitales et plus de 41 000 avec le fichier des empreintes génétiques. Le recours à la biométrie pour les besoins d'en-

Louis LAUGIER, né le 2 septembre 1965 à Paris, est diplômé de l'École spéciale militaire de Saint-Cyr et titulaire du diplôme d'état-major (DEM). Officier de l'armée de terre à partir de 1990, il sert comme chef de section dans un bataillon de chasseurs alpins avant d'intégrer le corps préfectoral en 2000.

Il occupe des postes de direction en préfecture et en administration centrale : secrétaire général des Hautes-Alpes, chef du service de gestion des personnels de la police nationale à la préfecture de police de Paris, puis directeur de cabinet du directeur général des collectivités locales. Spécialiste des ressources humaines et de l'organisation policière, il devient sous-directeur à la direction générale de la police nationale (DGPN), puis secrétaire général de la préfecture des Bouches-du-Rhône. Nommé préfet en 2015, il exerce en Aveyron, Savoie, Haut-Rhin et Isère. Depuis novembre 2024, il est directeur général de la police nationale. Louis Laugier est officier de la Légion d'honneur et officier de l'ordre national du Mérite.



quêtes judiciaires permet la résolution tant d'affaires relatives à la délinquance du quotidien tels que les cambriolages ou les faits commis à l'occasion de violences urbaines, que des actes les plus graves (vols avec arme, meurtres, viols...), mais également les plus anciens (*cold cases*).

Le recours à des logiciels d'analyse vidéo est également de nature à faciliter l'exploitation des enregistrements d'images saisis au cours d'enquêtes judiciaires et à favoriser leur élucidation.

L'utilisation de la technologie est encadrée

La même opinion publique exprime aussi des réserves. 12 % des sondés ne sont pas favorables à l'utilisation de la vidéoprotection sur la voie publique et s'inquiètent des dérives possibles de certaines technologies, comme la reconnaissance faciale. Beaucoup s'interrogent sur les limites de l'automatisation, les garanties juridiques, les contrôles indépendants. Ces préoccupations sont légitimes. Elles nous obligent.

Ces technologies ne sont employées par les forces de l'ordre que dans le strict respect du cadre légal. En l'état actuel du droit, la reconnaissance faciale est autorisée uniquement dans deux applications disposant d'un encadrement strict :

- la fonction « rapprochement photo de personne » dans le traitement d'an-

técédents judiciaires (TAJ) où le résultat du rapprochement est validé *in fine* par un policier ;

- la fonction « rapprochement photo de personne » dans le traitement du passage rapide aux frontières extérieures (Parafe).

La police nationale utilise également l'IA dans d'autres cas d'usages : l'analyse de vidéos de masses saisies dans un cadre judiciaire, la retranscription des auditions de mineurs dans les salles Mélanie [un espace adapté au recueil de la parole des jeunes victimes ou témoins, NDLR] dont le bilan est très positif (un audio d'une heure est traité en 6 minutes et il permet un gain de temps pour l'enquêteur de 6 à 7 heures), ou encore la retranscription des écoutes téléphoniques.

D'autres cas d'usages ne sont à ce stade pas juridiquement autorisés, par exemple l'utilisation des outils de recherche en sources ouvertes (Osint ou *open source intelligence*), alors même que 78 % des sondés estiment utiles les outils d'analyse de contenus sur les réseaux sociaux.

Une police moderne, humaine, transparente

La police nationale n'est pas une entité désincarnée. Elle est composée de femmes et d'hommes qui agissent avec discernement, parfois dans des conditions difficiles. Pour eux, les outils technologiques ne sont ni gadgets, ni instru-

ments de contrôle aveugle, mais bien des leviers de précision, d'accélération, de protection et de confiance de la population.

C'est aussi en ce sens que la direction générale de la police nationale investit dans des formations spécifiques sur l'utilisation de ces outils (par exemple sur les outils d'analyse de données) et dans une relation de dialogue avec les citoyens (à travers le développement et l'enrichissement du site internet masecurite.interieur.gouv.fr).

Nous faisons également davantage d'efforts de communication sur l'utilisation par la police nationale des technologies de sécurité (la majorité des répondants – près de 60 % – s'estimant mal informée sur les technologies de sécurité actuelles).

Protéger, sans jamais surveiller à outrance

La majorité des sondés (63 %) estime que les expérimentations de technologies de sécurité permettent de concilier les impératifs de préservation des libertés et de renforcement de la sécurité publique. C'est dans cet objectif que la police nationale soutient la création d'un cadre juridique de l'expérimentation, inexistant aujourd'hui, permettant de rejeter les technologies instables ou non matures.

L'expérimentation de la vidéo augmentée dans l'espace public a ainsi permis

de tester les traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection autorisés pour détecter, en temps réel, des événements prédéterminés (zones interdites, sens interdits, densités, mouvements de foule, bagages abandonnés, personnes au sol, armes, départs de feux) et de les signaler en vue de la mise en œuvre des mesures nécessaires par les services de la police nationale. Cette expérimentation a montré que la maturité de la technologie est aujourd'hui suffisante pour être opérationnelle dans certains cas d'usage (zones interdites), moins sur d'autres (détection des armes, personnes au sol et départs de feux). Une enquête réalisée fin 2024, dans le cadre de l'évaluation de cette expérimentation, a permis de montrer qu'une grande majorité des personnes interrogées se sentirait également « *beaucoup plus en sécurité* » et « *parfaitement à l'aise et libre* » en présence d'un tel dispositif. D'ailleurs, 63 % des personnes sondées souhaitaient la généralisation de cette expérimentation.

Protéger sans surveiller à outrance dans un cadre juridique strict et transparent : c'est avec cet équilibre que nous continuerons à agir. Et c'est dans cette vision que j'invite les Français à continuer à faire confiance à la police nationale. ■



CONCLUSION

Cette enquête, relative à la perception des technologies de sécurité par les Français, met en lumière leur perception globalement favorable de ces dispositifs, couplée à un niveau de confiance notable par-delà les clivages générationnels et politiques. Les dispositifs tels que la vidéoprotection, l'analyse automatisée, l'intelligence artificielle ou encore la biométrie bénéficient d'un soutien solide basé principalement sur la finalité de leur usage (la sécurité collective) et la légitimité reconnue aux acteurs chargés de leur mise en œuvre en tant que serveurs de l'intérêt général. Cependant, cette acceptation sociétale des technologies de sécurité est doublement conditionnée par l'expression d'un besoin constant de transparence, d'information et de régulation face à leur caractère potentiellement attentatoire aux libertés individuelles d'une part, et par le rejet ferme de la substitu-

tion totale à la présence humaine, qui demeure perçue comme le fondement incontournable de la sécurité publique.

Cette enquête révèle également que l'acceptation sociétale des technologies de sécurité augmente proportionnellement à leur antériorité et à leur degré d'intégration dans la vie quotidienne des citoyens. Les innovations les plus récentes doivent encore démontrer à la fois leur efficacité opérationnelle et leur innocuité pour les libertés fondamentales, ce qui implique une période nécessaire d'acculturation progressive et un encadrement juridique rigoureux.

À cet égard, l'État et son administration, perçus comme garants de l'intérêt général et soumis à des obligations juridiques strictes, jouissent d'une légitimité forte auprès de la population française, tandis que les acteurs privés, notamment les géants technologiques (Gafam), sont

regardés avec davantage de circonspection, en raison d'une suspicion de dérives commerciales ou de risques d'usages déviés des données personnelles qu'ils recueillent. Le secteur privé n'en reste pas moins reconnu pour son apport en matière de recherche et d'innovation, à condition que son action s'inscrive en soutien des dispositifs publics dans la logique du continuum de sécurité nationale.

Un dernier enseignement de cette enquête est que les expérimentations menées lors des Jeux olympiques et paralympiques de Paris 2024, notamment en matière de vidéoprotection algorithmique, ouvrent la voie à une possible généralisation de ces dispositifs à l'échelle nationale. Une telle perspective suscite nécessairement un débat public sur l'équilibre délicat à maintenir entre l'efficacité opérationnelle et la préservation stricte des libertés fonda-

mentales, ce qui traduit, derechef, l'ambivalence de l'opinion publique, favorable à l'innovation technologique mais également préoccupée par les risques en termes de surveillance généralisée et de libertés individuelles.

Au bilan, cette enquête met en lumière la nécessité d'un cadre législatif clair, rigoureux et transparent, indispensable pour accompagner le développement et l'intégration des technologies de sécurité en France. Un tel cadre permettrait de répondre aux attentes d'une société à la fois exigeante et lucide, capable d'accepter les évolutions technologiques à condition qu'elles soient strictement encadrées et contrôlées.

L'avenir des technologies de sécurité repose donc sur une gouvernance équilibrée associant étroitement l'efficacité opérationnelle, l'innovation et la protection inconditionnelle et absolue des libertés fondamentales.



Éclairage d'experts

sur les prochaines évolutions législatives
et réglementaires à propos des technologies
de sécurité innovantes



Caroline LEQUESNE

Maîtresse de conférences en droit à l'université Côte d'Azur

Libertés individuelles et sécurité : l'incertain pari technologique

Les technologies de sécurité ont le vent en poupe. Conformément à la volonté politique du gouvernement, qui annonçait, dès 2020, le renforcement de l'action des forces de l'ordre par le renouvellement technologique des équipements¹, la dynamique de déploiement des technologies de sécurité est en plein essor. Quelques illustrations récentes pour s'en convaincre : au cours de l'année 2024, plus de 1 800 autorisations de survol du territoire par drone auraient été délivrées. La période fut également marquée par la première expérimentation à grande échelle de la vidéosurveillance algorithmique en temps réel dans les espaces publics, la pérennisation du port de caméra individuelle par les agents assermentés des services de transports ou le renforcement du maillage de la vidéoprotection des communes, à l'image du « bouclier de sécurité » de la région Île-de-France. Si l'exceptionnalité a souvent été mobilisée comme *leitmotiv* impérieux, à la faveur de la sécurisation des grands événements sportifs dont les Jeux olympiques

et paralympiques (JOP) furent le point d'orgue, force est de constater que l'adoption des technologies de sécurité relève bien davantage de la normalisation. La bataille entre sécurité et libertés individuelles qui se joue dans les prétoires – du référé au contrôle de constitutionnalité – participe tendanciellement de leur acculturation. De nombreux usages, « proportionnés et nécessaires » rentrent ainsi dans l'outillage démocratique du « continuum de sécurité ».

Quelques résistances se font toutefois jour sur les technologies les plus avancées pour certains, intrusives pour d'autres. La biométrie et son traitement algorithmique sont pour l'heure étroitement circonscrits aux procédures judiciaires, dans des utilisations *a posteriori*. Si quelques velléités d'usages ont été signifiées en amont des JOP, elles ont finalement été écartées au bénéfice de la vidéosurveillance algorithmique. Ces traitements d'images automatisés grâce aux outils d'intelligence artificielle (IA) soulèvent eux-mêmes quelques atermoiements ; en témoignent les résultats mitigés du rapport d'évaluation de la commission indépendante nommée par le ministère de l'Intérieur ou l'absence

”

L'adhésion repose sur des conditions de déploiement à la fois techniques et démocratiques.

Caroline LEQUESNE est maîtresse de conférences en droit, habilitée à diriger les recherches (HDR), à l'université Côte d'Azur. Elle est membre du Groupe de recherche en droit, économie et gestion (Gredeg), unité mixte de recherche (UMR) 7321 sous la double tutelle du Centre national de la recherche scientifique (CNRS) et de l'université Côte d'Azur. Elle est aussi membre du Centre Perelman de philosophie du droit, de l'Université libre de Bruxelles (ULB).

Formée en droit et en philosophie, ses travaux portent sur les enjeux de régulation de l'intelligence artificielle (IA). Ils concernent plus spécifiquement les technologies de surveillance, l'automatisation des services publics et la transformation des rapports de pouvoir qu'ils engagent. Elle a fondé, et dirige depuis 2019, le master Droit algorithmique et gouvernance des données.

En 2024, elle est désignée par la Commission nationale de l'informatique et des libertés (Cnil) comme personnalité qualifiée en tant que membre du comité d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs.



de pérennisation à l'issue de l'expérimentation. La coloration autoritaire qui les entoure, nourrie d'exemples étrangers peu enviables, conduit le législateur français à une position de façade, sinon plus libérale, plus prudente.

La présente enquête offre une résonance sociale à ces constats. Elle fait état d'une adhésion relativement forte à l'adoption des technologies de sécurité, justifiée par un besoin manifeste de sécurité, qui tend ainsi à minorer la perte de liberté. La vision « spontanée » de ces technologies est majoritairement « plutôt positive » (27 %), bien que le niveau d'information soit assez faible (pour 59 %) ; l'opinion est majoritairement favorable à la vidéoprotection (87 %), juge « utile » le recours à l'IA par les forces de police (65 %) et « acceptable » la plupart des usages de données biométriques par celle-ci. De manière plus granulaire toutefois, les résultats apportent des éclairages plus nuancés : l'adhésion repose sur des conditions de déploiement à la fois techniques et démocratiques. D'une part, il convient de corréliser les résultats de la confiance avec ceux de l'efficacité présumée des systèmes. L'enquête ne fait pas état des résultats des technologies, mais de leur perception. La croyance en ceux-ci apparaît importante :

76 % des personnes interrogées « estiment » que la présence d'outils de vidéoprotection permet de mieux assurer la sécurité de la voie publique et 65 % que l'IA permet aux forces de l'ordre d'être plus efficaces, ces outils étant majoritairement considérés comme « fiables » (6,1/10). Aussi, l'efficacité apparaît comme un facteur décisif dans la formation de l'opinion. Pour autant, rappelons qu'elle est encore incertaine : outre les résultats de l'expérimentation déjà mentionnés, les exemples étrangers et plusieurs études récentes² mettent fortement en cause la performance de ces systèmes. Des erreurs ou des biais, dont tout un chacun peut se retrouver demain victime, pourraient compromettre l'acceptation du compromis liberté/sécurité auquel l'opinion semble ici souscrire. D'autre part, l'étude décrit de fortes variabilités de confiance en fonction des acteurs impliqués. La confiance accordée aux acteurs publics – au premier rang desquels les pompiers, la gendarmerie et la police nationales – pour utiliser les outils d'analyse en temps réel, ou posséder et exploiter les données biométriques est majoritairement plus importante que celle dévolue au secteur privé. Cette lecture très française des rapports avec le corps civil laisse apparaître que le déploiement des techno-

logies de sécurité devra nécessairement se faire sous le joug de la puissance publique. De là à envisager la question de la souveraineté technologique, il n'y a qu'un pas, comme en attestent les priorités d'actions identifiées : 85 % des personnes interrogées estiment que l'État doit investir dans la recherche de nouvelles formes de technologies. Cependant, l'indépendance et la force de l'action publique ne sont pas encore pleinement alignées à cette réalité.

Certes, la France fait partie des États européens qui ont investi les solutions *in-house*. Mais elles sont loin de couvrir l'ensemble des besoins ou des fantasmes techno-solutionnistes alimentés par l'industrie sécuritaire. Or, les scandales Clearview et Briefcam rappellent combien le choix de recourir à ces puissants acteurs peut être très dommageable en démocratie : surveillance de masse, absence de contrôle et de contre-pouvoirs, ultimement fuite des données à l'étranger. Le présent rapport rappelle ainsi que la croyance dans les vertus technologiques ne suffira pas : le déploiement des technologies de sécurité ne peut faire l'économie d'un test d'efficacité et de contrôles démocratiques sans craindre d'émailler le fragile contrat social. ■

¹ Ministère de l'Intérieur, *Livre blanc de la sécurité intérieure*, 16 novembre 2020.

² Voir notamment l'étude des trois chercheurs d'Oxford mettant en cause les rapports de référence du *National Institute of Standards and Technology* (NIST) dans les conditions en temps réel : Teo Canmetin, Juliette Zaccour, Luc Rocher, *Why we shouldn't trust facial recognition's glowing test scores*, Aug 18, 2025, www.techpolicy.press/why-we-shouldnt-trust-facial-recognitions-glowing-test-scores/



Philippe LATOMBE

Député de la première circonscription de la Vendée et secrétaire de la commission des lois

L'enquête menée par le Continuum Lab, Centre de recherches politiques de Sciences Po et Opinion-Way constitue une approche inédite, mais qui était indispensable, de la perception et de l'opinion des Français concernant les technologies innovantes de sécurité. Dans un climat ambiant qui tend bien trop souvent à polariser les débats, il faut reconnaître que, loin des postures idéologiques, les résultats de ce sondage restituent une certaine forme de sagesse populaire, en recherche d'un équilibre entre le besoin de protection et le respect des libertés individuelles et collectives, ce qui est tout à fait rassurant. Ils soulignent aussi la confiance de nos concitoyens en la capacité de nos forces de l'ordre à assurer leur protection, ce qui est une bonne nouvelle.

La technicité des technologies innovantes, par nature complexe, pouvait sembler représenter un obstacle à la compréhension éclairée des enjeux qu'elles portent, mais les personnes sondées en ont, dans l'ensemble, compris les avantages et les dangers, la nécessité de trouver un point d'équilibre pour que l'usage qui en est fait se pratique dans l'intérêt général.

”

Pour les citoyens, le recours à des usages numériques de plus en plus sophistiqués ne doit pas conduire au moindre compromis vis-à-vis de la sécurité de leurs données.

C'est ce même chemin de crête que nous avons choisi d'emprunter, le député Philippe Gosselin et moi-même, à travers les 41 recommandations de notre rapport d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité, travail qui reste d'une totale actualité.

Ce rapport, rédigé il y a plus de deux ans, portait sur l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité, mais ses conclusions générales valent pour l'ensemble des technologies innovantes de sécurité. Il convient, en effet, de définir à chaque fois un cadre juridique clair et précis, qui ne doit être ni lacunaire ni rigide, car il peut être amené à être retouché au fur et à mesure des progrès rapides de ces technologies, mais aussi des évolutions sociétales auxquelles nous sommes collectivement confrontés.

Le législateur ne doit pas être en retard sur les usages comme cela s'est passé, par exemple, dans l'affaire du logiciel israélien Briefcam, utilisé en dehors du cadre légal prévu par la directive européenne et la loi Informatique et libertés,

Philippe LATOMBE est député de la première circonscription de la Vendée. Il est secrétaire de la commission des lois et membre du groupe démocrate. Il effectue actuellement son troisième mandat. Il est aussi commissaire à la Commission nationale de l'informatique et des libertés (CNIL). Particulièrement investi sur les questions relatives au droit du numérique, il a ainsi participé activement aux travaux du groupe de travail sur les droits et libertés constitutionnels à l'ère numérique, ainsi qu'à ceux de la mission d'information parlementaire sur la *blockchain*. Il a été le rapporteur de la mission parlementaire « Bâtir et promouvoir une souveraineté numérique nationale et européenne¹ » et corapporteur de la mission d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité². Il est actuellement président de la commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

¹https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299_rapport-information

²https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information





par les services de la police judiciaire, les préfetures de police de Paris et Marseille, la sûreté publique et la gendarmerie nationale.

C'est au Parlement qu'il revient de se saisir régulièrement de l'ensemble de ces questions, et de suivre attentivement les évolutions techniques, politiques et sociétales auxquelles nous sommes collectivement confrontés. C'est aux parlementaires de choisir librement les règles permettant de concilier, aujourd'hui et demain, la préservation de l'ordre public et le respect des droits fondamentaux. Cela demande de leur part, sinon une appétence pour ce domaine, du moins une acculturation leur permettant d'appréhender cette thématique de façon éclairée, ce dont il faut bien reconnaître que ce n'est pas encore suffisamment le cas.

Dans un contexte géopolitique tourmenté et de cyberguerre, l'État doit se prémunir des attaques informatiques d'ampleur et être capable de faire évoluer ses modes d'intervention, tout en conservant la maîtrise des processus utilisés. L'intelligence artificielle, la biométrie, la blockchain, la cybersécurité renforcée, les systèmes avancés de surveillance sont amenés à être de plus en plus

utilisés pour améliorer l'analyse des données, la détection des menaces et renforcer la sécurité des données pour contrer ceux qui veulent nous nuire.

Cependant, les technologies de sécurité ne peuvent mériter pleinement cette appellation que si les solutions qu'elles proposent sont souveraines, car elles doivent aussi être en mesure de protéger les données qu'elles utilisent et ne pas être assujetties à des lois d'extraterritorialité, d'où qu'elles viennent.

Pour les citoyens, le recours à des usages numériques de plus en plus sophistiqués ne doit pas conduire au moindre compromis vis-à-vis de la sécurité de leurs données. Pour les entreprises, cet enjeu de souveraineté est une question de confiance vis-à-vis de leurs clients, de liberté dans leurs stratégies de croissance et de transformation, de sécurisation de leur activité.

Pour y parvenir, le soutien à apporter aux acteurs technologiques nationaux doit être une priorité, ce qui appelle un changement d'état d'esprit et de pratiques, comme le soulignent les travaux remarquables de la récente commission d'enquête sénatoriale sur la commande publique¹. ■

¹ <https://www.senat.fr/rap/r24-830-1/r24-830-1.html>

Les propositions du Continuum Lab

pour améliorer l'usage des technologies
de sécurité innovantes par le continuum
de sécurité et de justice

Création d'un groupe de travail au sein du Continuum Lab pour formuler des propositions afin de faciliter l'utilisation des technologies de sécurité innovantes par les acteurs du Continuum de sécurité et de justice

Sa composition

Le groupe de travail « Technologies de sécurité innovantes » a été constitué à la suite de l'enquête inédite réalisée par le Continuum Lab avec le Centre de recherches politiques de Sciences Po (Cevipof) et OpinionWay (en juin-juillet 2024) sur la perception des technologies de sécurité par les Français.

Son ambition : transformer les enseignements des Jeux olympiques et paralympiques (JOP) 2024, ainsi que les données de l'enquête du Continuum Lab, en recommandations opérationnelles à l'attention des pouvoirs publics.

Trois priorités ont conduit nos travaux : pérenniser les dispositifs expérimentaux déployés pendant les JOP 2024, ouvrir de nouveaux cas d'usage pertinents et trouver un point d'équilibre exigeant sur le traitement algorithmique (juridique, éthique, technique).



Le conseiller d'État et essayiste,
Christophe Eoche-Duval



Le professeur affilié à l'École d'affaires publiques de Sciences Po Paris, **Guillaume Farde**



Le chef du Service de l'innovation et de la prospective au sein de la préfecture de police de Paris, **Johan Cavirot**



Le directeur des affaires publiques d'INTÉRIALE et directeur du Continuum Lab, **Laurent Michel**



Le chargé de mission en affaires publiques d'INTÉRIALE et du Continuum Lab, **Axel Haverbeke**

Sa méthode

Ce groupe de travail a complété la réflexion de ses membres par des auditions d'acteurs publics et privés, adossées à des analyses réglementaires, juridiques, opérationnelles et politiques couvrant l'ensemble des enjeux de ce sujet : l'efficacité opérationnelle, l'acceptabilité sociale, le cadre juridique et éthique, la protection des données, la transparence et la gouvernance, l'innovation et la souveraineté, l'interopérabilité, les compétences, les risques/biais et les perspectives européennes.

Liste des personnalités auditionnées

- **Christian Meyer**, sous-directeur régional de police des transports à la Direction de la sécurité de proximité de l'agglomération parisienne (DSPAP) de la préfecture de police de Paris, le 5 février 2025 ;
- **Anne-Florence Canton**, directrice de l'innovation, de la logistique et des technologies (DILT) de la préfecture de police de Paris, le 5 février 2025 ;
- **Pascal Girault**, inspecteur général de l'administration, le 19 février 2025 ;
- **Anne Cornet**, préfète et inspectrice générale de l'administration, le 19 février 2025 ;
- **Philippe Latombe**, député de Vendée (1^{re} circonscription), le 17 mars 2025.

En sus de ces auditions, de nombreuses discussions ont pu être établies avec différents décideurs publics et privés, à l'occasion de rencontres informelles, pour échanger sur les besoins et les retours d'expérience opérationnels sur ces technologies de sécurité innovantes.

Propositions du groupe de travail sur les technologies de sécurité innovantes

Codification et harmonisation du droit de la vidéoprotection et de l'intelligence artificielle en matière de sécurité-justice

Problème identifié

La réglementation actuelle est dispersée entre plusieurs textes (Code de la sécurité intérieure, lois spécifiques, décisions du Conseil constitutionnel, etc.), rendant difficile une lecture cohérente et sécurisée pour les acteurs concernés.

Proposition n°1

Créer un cadre législatif unifié et pérenne via un chapitre dédié dans le Code de la sécurité intérieure.

Le cadre actuel est effectivement morcelé entre le Code de la sécurité intérieure, la loi du 19 mai 2023 relative aux Jeux olympiques et paralympiques (JOP) de 2024, le règlement général sur la protection des données (RGPD), la directive « police-justice » (2016/680) et la jurisprudence du Conseil d'État (CE) et du Conseil constitutionnel. La Commission nationale de l'informatique et des libertés (Cnil) rappelle qu'en l'état, « les dispositifs de caméras augmentées poursuivant une finalité dite “police-justice” sont interdits en l'absence de cadre légal spécifique ». Autrement dit, hors dispositions expérimentales (loi JOP 2024), aucun outil d'analyse automatisée (détection en temps réel d'infractions, comportements suspects, etc.) n'est autorisé

dans la législation actuellement. Le RGPD s'applique à la vidéoprotection algorithmique et considère les données biométriques (empreintes, visages) comme sensibles, donc interdites sauf exceptions très limitées (consentement ou motif d'intérêt public majeur). De fait, l'usage de la reconnaissance faciale en public est strictement limité : l'Union européenne (UE) l'interdit en temps réel pour les forces de l'ordre, sauf cas ciblés (terrorisme, personne disparue) et avec autorisation préalable (juge ou administration). Ces principes européens devront être transposés en droit français unifié. Ainsi, un chapitre dédié dans le Code de la sécurité intérieure pourrait regrouper les règles existantes (JOP, RGPD, « police-justice », jurisprudence Cnil/CE) et préciserait :

- le périmètre légal de la vidéoprotection « augmentée » hors contexte exceptionnel – en s'inspirant par exemple des garde-fous de la loi JOP (détectations *ad hoc*, aucune reconnaissance faciale, pas de croisement de fichiers) mais en utilisation quotidienne et régulière ;
- l'autorisation conditionnelle des outils d'intelligence artificielle (gestion de flux, détection d'armements ou de situations anormales) sous contrôle administratif ou judiciaire ;
- l'interdiction générale de la reconnaissance faciale en continu, à l'exception de cas d'enquête ciblés avec l'autorisation du magistrat, comme l'illustre le règlement IA de l'UE.

Formalisation d'un cadre d'expérimentation technologique

Problème identifié

L'expérimentation de nouvelles technologies se heurte à des contraintes réglementaires rigides, freinant leur adoption.

Proposition n°2

Créer un « dispositif législatif d'expérimentation en sécurité publique ».

Sur le modèle des *regulatory sandboxes* (bac à sables réglementaires) permettant aux acteurs publics régaliens (forces de l'ordre, opérateurs de transport, collectivités) de tester des innovations technologiques sous supervision (cadre européen – IA). À l'échelle nationale, un dispositif législatif d'expérimentation permettrait aux forces de l'ordre, aux acteurs de la sécurité civile, aux régies de transport et aux collectivités de déroger temporairement à certaines règles (durée limitée, dérogations encadrées) pour tester de nouveaux outils (IA de détection, caméras intelligentes, etc.). Cette démarche puise sa base dans le droit constitutionnel à l'expérimentation : article 37-1 et article 72-4 sur l'expérimentation locale. Ce cadre inclurait :

- une autorisation temporaire d'expérimentation sous conditions (garanties en matière de libertés publiques, suivi régulier) après avis de la Cnil ;

- un comité d'évaluation mixte (experts techniques et parlementaires) dédié, chargé de rendre un avis public sur les résultats et les risques identifiés avant tout déploiement généralisé.

Renforcement du contrôle parlementaire et institutionnel

Problème identifié

La prolongation des expérimentations technologiques sans réel contrôle parlementaire peut poser la question de la légitimité démocratique de ces expérimentations.

Proposition n°3

Instaurer une procédure parlementaire avant toute extension des dispositifs d'expérimentation.

Les prolongations automatiques d'expérimentations sans débat soulevaient des critiques démocratiques. Pour y remédier, il faudrait instaurer une procédure de validation législative avant toute extension des dispositifs. Par exemple, la loi JOP prévoyait la remise d'un rapport au Parlement d'ici fin 2024, élaboré par un comité rassemblant députés, sénateurs et experts indépendants. Notre proposition vise à généraliser cette démarche : chaque expérimentation ferait l'objet d'une évaluation indépendante (pas uniquement interne) puis d'un **débat obligatoirement tenu au sein de la commission compétente à l'Assemblée nationale et au Sénat.**

Expérimentations en contexte quotidien

Problème identifié

Les expérimentations menées principalement dans le cadre des grands événements (JOP 2024) ne permettent pas de juger leur efficacité sur le long terme dans la sécurité quotidienne.

Proposition n°4

Élargir les expérimentations à des milieux urbains et ruraux pour mesurer l'impact des solutions de vidéoprotection algorithmique et d'IA hors périodes d'affluence exceptionnelle.

Les tests effectués essentiellement durant des « grands événements » (JOP 2024) ne reflètent pas les conditions réelles de terrain. Comme le soulignent certains observateurs, confiner les essais aux JOP est une « fausse bonne idée » : un événement exceptionnel est sur-sécurisé, ce qui ne permet pas de mesurer l'efficacité de l'IA en situation normale faute d'événement à détecter. Il faut donc élargir les pilotes aux zones et usages de tous les jours. Concrètement, on peut imaginer :

- **transports publics** : intégrer des caméras intelligentes dans les réseaux RATP/SNCF (gares, stations, bus) ou les enceintes aéroportuaires pour fluidifier les flux et repérer les anomalies (bagages abandonnés, mouvements de foule) – les régions ont d'ailleurs participé au projet européen Prevent (Horizon 2020) sur la détection automatisée de bagages.
- **espaces urbains et ruraux** : installer des dispositifs IA dans les centres-villes, les zones piétonnes ou à proximité de collèges, gares, hôpitaux et lieux sensibles comme

des ambassades ou lieux de culte menacés. Par exemple, les systèmes pourraient détecter des attroupements inhabituels, des comportements dangereux ou des véhicules à contresens. Lors des JOP, le texte prévoyait de déployer ces outils dans les stades, sur la voie publique et les transports (600 000 personnes attendues au feu d'artifice), mais on peut maintenant étendre hors événements.

- **circulation et parkings** : utiliser les caméras IA pour la régulation du trafic (détection de bouchons, de stationnements gênants) ou la sécurité des parkings. Ces expérimentations quotidiennes, variées, permettraient de valider les outils sur le long terme et d'ajuster les algorithmes selon les contextes réels.
- **événements ponctuels** : contrairement aux grands événements nationaux, des événements comme des festivals ou la fête de la musique peuvent générer très ponctuellement sur une surface géographique large un flux important de personnes.

Pérennisation et capitalisation sur les retours d'expérience

Problème identifié

L'absence de centralisation des résultats des expérimentations limite la diffusion des bonnes pratiques.

Proposition n°5

Créer un Comité national d'évaluation des technologies de sécurité.

Aujourd'hui, les bilans d'expérimentations sont dispersés, ce qui nuit à l'essaimage des bonnes pratiques. Il conviendrait donc de créer un Comité national d'évaluation des

technologies de sécurité permanent, chargée de centraliser les retours d'expériences (Retex). Ses missions seraient :

- **collecte et publication** : rassembler les rapports d'expérimentation (JOP 2024, projets locaux, tests inédits) et publier périodiquement une synthèse ;
- **référentiel de bonnes pratiques** : élaborer une charte ou guide (niveau national/UE) décrivant les conditions d'usage recommandées (sécurité, protection des données, acceptabilité sociale) à partir des retours terrain.
- **donner un avis avant le lancement d'une nouvelle expérimentation** : cela permettrait d'en évaluer la pertinence et éviter les redondances, voire d'organiser des mutualisations.

Fonds national dédié aux technologies de sécurité innovantes

Problème identifié

Les collectivités territoriales, notamment les communes ou agglomérations en zones rurales, peinent à financer ces dispositifs pourtant essentiels à la modernisation de la sécurité publique.

Proposition n°6

Créer un Fonds national pour une sécurité moderne (FNSM), dédié à la vidéoprotection et l'IA dans le domaine de la sécurité.

Pour moderniser la vidéoprotection et l'IA, il faut des moyens. Un Fonds national pour une sécurité moderne (FNSM) faciliterait l'acquisition d'équipements (caméras intelligentes, logiciels d'analyse IA, serveurs sécurisés) par les collectivités, notamment rurales. Il

fonctionnerait en cofinancement avec les communes et tirerait parti des financements européens disponibles. En effet, l'Union européenne investit massivement dans le numérique : le programme Digital Europe (8,1 milliards d'euros) finance notamment des projets dans l'IA et la cybersécurité, tandis que le mécanisme de relance et de résilience ou les fonds structurels (Fonds européen de développement régional – Feder) soutiennent la transformation digitale des collectivités.

Ce fonds pourrait être abondé par les conseils régionaux, les conseils départementaux, les métropoles, qui sont de plus en plus sensibilisées à la notion de continuum de sécurité (exemple du conseil régional d'Île-de-France qui a mis en place un fonds de dotation pour les communes de la région qui souhaitent s'équiper en caméras de vidéoprotection).

Le FNSM pourrait fournir des **subventions ciblées** (plus fortes pour les petites communes), encourager les **partenariats public-privé** pour développer des solutions souveraines (par exemple, avec des entreprises françaises d'IA), et servir de relais national pour mobiliser les crédits européens. Au niveau régional ou départemental, des délégations permettraient d'allouer ces fonds aux groupements communaux, sans alourdir la gestion administrative.

Ce fonds serait piloté par le préfet de département, le président du conseil départemental et auxquels seraient associés les autres niveaux de collectivités locales du département. Cet échelon de proximité permettrait de garantir la réalisation et l'utilisation concrète et rapide des fonds au plus près des besoins de sécurité des habitants.

Mutualisation des moyens entre collectivités et opérateurs privés

Problème identifié

Un déséquilibre entre les territoires.

Proposition n°7

Encourager les coopérations locales pour rationaliser les investissements, sur le modèle des syndicats mixtes territoriaux.

La mutualisation est déjà prévue par la loi « sécurité globale » (2021) via la création de syndicats mixtes spécialisés. Ce mode d'organisation permet de partager les coûts (acquisition de matériel de pointe, maintenance) et le personnel (centres de supervision partagés). Comme l'a noté un sénateur, mutualiser « *augmente les capacités d'investissement pour du matériel plus performant* »* et étend la couverture du système. Dans les faits, des **centres urbains de supervision** peuvent être gérés en commun par plusieurs communes ou établissements publics de coopération intercommunale (EPCI) : cela évite les redondances (plusieurs opérateurs dans la même zone) et optimise la capacité d'analyse vidéo. De même, le stockage des flux (environnements *cloud* ou serveurs régionaux) peut être mutualisé afin de réduire les coûts unitaires. La circulaire du 4 mars 2022 rappelle toutefois que cette mutualisation doit respecter certaines modalités (conventions entre membres, agréments préfectoraux pour le personnel visionnant les images).

Il s'agirait de lever les derniers obstacles réglementaires pour que, dans une convention d'entente intercommunale ou via un

syndicat mixte, tous les agents habilités (policiers, gendarmes, agents municipaux agréés et gardes champêtres) puissent visionner l'ensemble des images mutualisées. Cela permettrait de créer de nouveaux métiers territoriaux liés aux technologies de sécurité et renforcerait la notion de continuum de sécurité.

Sécurisation et certification des équipements

Problème identifié

Dépendance aux fournisseurs étrangers et risques liés aux failles de cybersécurité (*backdoors*, espionnage).

Proposition n°8

Imposer une certification obligatoire des équipements utilisés.

La confiance dans ces technologies passe par la cybersécurité des équipements et la souveraineté des données. On pourrait imposer des **labels de sécurité** obligatoires. Par exemple, la qualification *SecNumCloud* de l'Agence nationale de la sécurité des systèmes d'information (Anssi) impose que les données hébergées restent en Europe et répondent à des normes très strictes (chiffrement avancé, résilience, contrôle d'accès). De même, un label national type « CyberCaméra » garantirait qu'une caméra ou un logiciel d'analyse vidéo respecte des standards français/UE (absence de *backdoors*, mises à jour, audit indépendant). Par ailleurs, la loi pourrait exiger **l'hébergement des données de vidéo-protection dans un *cloud* souverain** (prestataire certifié), comme recommandé par le programme européen de *cloud* sécurisé. Le récent règlement européen de cybersécurité

(*Cybersecurity Act*) prévoit d'ailleurs des schémas de certification communautaires (par exemple pour l'Internet des objets, *Internet of things* – IOT, et les services *cloud*). En parallèle, l'État pourrait soutenir le développement de solutions 100 % françaises (caméras, IA) via le FNSM et des subventions, pour réduire la dépendance aux fournisseurs étrangers.

Proposition n°9

Instaurer une préférence nationale dans la procédure des appels d'offres relatifs à des infrastructures, équipements, enjeux relevant de la souveraineté nationale.

Instaurer une préférence *de facto* compatible avec le droit de l'UE en combinant cinq leviers cumulatifs :

1. activer, pour les segments réellement sensibles (vidéoprotection critique, analyse IA en temps réel, réseaux et sécurité de l'information, *Security operations center* – SOC), **l'exception de sécurité nationale** afin d'écarter les offres qui ne garantissent pas les intérêts essentiels de sécurité (motivation au cas par cas, traçabilité de l'analyse de risque) ;
2. exiger **l'hébergement souverain** et des **certifications de cybersécurité** de haut niveau (qualification *SecNumCloud* pour le *cloud*, exigences Anssi) ;
3. intégrer des **critères environnementaux et sociaux** (bilan carbone du service numérique, circuits courts, clauses d'insertion) dès l'analyse des besoins et dans l'attribution, ce qui avantage les acteurs de proximité ;
4. recourir au dispositif « **achats innovants** » (< 100 000 euros HT sans publicité ni mise en concurrence) pour tester et amorcer l'industrialisation de solutions françaises ;

5. prévoir des **clauses d'interopérabilité/résilience** avec les infrastructures critiques françaises (réversibilité, portabilité des données, auditable du code) pour filtrer les offres non conformes. Ces instruments, déjà prévus ou admis (sécurité nationale, commande publique durable, achats innovants, qualification Anssi), orientent la commande vers des offres françaises/européennes **sans discrimination explicite** et sécurisent juridiquement la mise en œuvre.

Utilisation des preuves technologiques dans la procédure pénale

Proposition n°10

Mettre en place des « référents technologies » dans chaque juridiction.

Ces magistrats formés aux enjeux numériques seraient chargés d'évaluer la valeur probante de preuves issues d'IA (vidéosurveillance intelligente, reconnaissance faciale, capteurs) dans le cadre d'une procédure pénale. Exemple : en Espagne, des unités spécialisées accompagnent déjà les juges dans la lecture d'éléments techniques complexes.

* Question de M. Devinaz Gilbert-Luc (Rhône - SER) publiée le 22/09/2022, à destination du ministre de l'Intérieur et des Outre-mer. (<https://www.senat.fr/questions/base/2022/qSEQ220902794.html>)

Éditeur : © Continuum Lab – 32, rue Blanche – 75009 PARIS – France • ISBN : 978-2-9590303-1-4 • Prix France : 18 € TTC • Dépôt légal : novembre 2025 • Création : Agence Ciem, 12 rue de l'Église, 75 015 Paris.

Le Code de la propriété intellectuelle et artistique n'autorisant, aux termes des alinéas 2 et 3 de l'article L. 122-5, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » (alinéa 1^{er} de l'article L. 122-4). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Imprimerie L'ARTESIENNE ZI de l'ALOUETTE, BP 99 – 62 802 LIEVIN (Haut-de-France – France). Achievé d'imprimé en novembre 2025, sur papier MAGNO certifié PEFC 100 % et Ecolabel Européen – Provenance Autriche. Taux de fibres recyclées : 0 % - Taux d'Eutrophisation PTot 0,049 kg/T.



Le **Continuum Lab** est le premier think tank des représentants des métiers de la sécurité et de la justice, cofondé en 2021 à l'initiative de la mutuelle INTÉRIALE et de six autres membres fondateurs. Il publie, en partenariat avec le Centre de recherches politiques de Sciences Po (Cevipof), une étude inédite consacrée à la perception et à l'acceptabilité des technologies de sécurité innovantes par les Français. Cette étude, réalisée par l'institut OpinionWay, sur un échantillon de 3 438 personnes représentatif de la population française âgée de 18 à 75 ans du 18 au 26 juin 2024, explore l'adhésion des Français, leurs attentes et les conditions de confiance à l'égard de dispositifs tels que la vidéoprotection (et ses usages dits « intelligents »), l'intelligence artificielle, la biométrie, les drones, les capteurs et l'analyse de données au service de la sécurité intérieure et de la justice.

Elle apporte une vision nouvelle du sujet et a suscité la volonté de proposer aux pouvoirs publics de nouveaux leviers d'action pour améliorer les conditions d'exercice de ces technologies de sécurité par les forces de sécurité intérieure et de justice. C'est la première étude à grande échelle permettant de comprendre les attentes et les craintes des citoyens à l'égard des outils et des acteurs en situation d'utilisation de ces technologies innovantes. Elle a vocation à nourrir le débat public et à permettre d'aboutir à des solutions pour améliorer l'usage responsable de ces outils par l'ensemble du continuum de sécurité et de justice.

Cette photographie met au jour quatre lignes de force : l'exigence d'efficacité opérationnelle et de résultats tangibles ; la primauté du facteur humain (formation, doctrine d'emploi, supervision) ; la demande d'un cadre éthique et juridique lisible (finalités précises, proportionnalité, traçabilité et contrôle indépendant) et la nécessité d'une transparence active pour entretenir la confiance.

Ainsi, le Continuum Lab reste fidèle à sa ligne stratégique : armer durablement les acteurs du continuum de sécurité et de justice face aux menaces contemporaines, connues ou à venir.

www.continuumlab.fr

in continuum-lab

🐦 @LabContinuum

CONTINUUM
LAB

Sécurité, Société, Justice

18 € TTC - France

ISBN : 978-2-9590303-1-4

