GOUVERNEMENT

Liberté
Égalité
Fraternité

Pour un usage **responsable et acceptable** par la société des **technologies de sécurité**

Rapport au Premier ministre par Jean-Michel Mis, député de la 2e circonscription de la Loire

Volume I
Rapport

Septembre 2021

Avec la participation de :

François de Charette
Inspecteur de l'administration

Nina Fabrizi
Doctorante en droit public, université Paris II

Sont remerciés celles et ceux qui, par leurs auditions, contributions et participations, ont permis la production de ce rapport.

Table des matières

Synthèse

Les nouvelles technologies offrent de nombreuses perspectives aux acteurs publics, y compris dans le champ des missions de sécurité. Les missions des forces de sécurité sont tout d'abord impactées par la numérisation croissante des activités. Se développe en effet une nouvelle criminalité à laquelle les forces de sécurité doivent pouvoir répondre pour assurer la protection des citoyens et des institutions, comme en témoigne encore récemment l'affaire *Pegasus*. Les nouvelles technologies qui sont utilisées dans la société font peser le risque d'une asymétrie de moyens entre les forces et leurs adversaires. Par ailleurs, les technologies sont des outils d'assistance dans la prise de décision et d'appui dans l'alerte, l'enquête et la planification opérationnelle qui peuvent aider les forces de sécurité à faire face à ces nouvelles complexités. C'est notamment le cas pour les grands évènements sportifs que la France accueillera en 2023 (coupe du monde de rugby) et 2024 (jeux olympiques et paralympiques), qui concentreront des enjeux forts en matière de sécurité. Plus largement, la question se pose des emplois plus pérennes de nouvelles technologies en matière de sécurité.

Celles-ci sont aussi un enjeu industriel et économique. La France dispose en effet d'acteurs industriels de pointe dans le secteur de la sécurité qui sont pourvoyeurs d'emploi (130 000 emplois directs et indirects) et réalisent près de la moitié de leur chiffre d'affaires à l'international. Le renforcement de notre base industrielle est un enjeu de souveraineté technologique afin de conserver l'autonomie de la France dans la définition de ses choix stratégiques. Les développements industriels peuvent aboutir à des technologies fondées sur le *privacy-by-design*. Celle-ci permettra de différencier l'offre française et européenne par rapport à celles de ses concurrents, dans la mesure où la société porte un intérêt croissant à la question de la protection des données personnelles.

Le recours aux nouvelles technologies soulève cependant des enjeux majeurs pour les libertés, et notamment pour la protection de la vie privée. Les grandes technologies récentes reposent sur la captation et l'exploitation massive de données. Ces technologies peuvent être utilisées en mobilité et interconnectées, ce qui leur donnent un potentiel de quasi-ubiquité. Les principales craintes pour la préservation des libertés concernent le traitement de données personnelles, dont les données biométriques, mais aussi l'opacité associée à l'emploi de certaines technologies (effet « boîte noire » des algorithmes d'intelligence artificielle par exemple). L'emploi des nouvelles technologies par les forces de sécurité est souvent perçu comme ayant pour objectif la surveillance de masse. Ce sentiment est nourri par la méfiance que ressent une partie de la population vis-à-vis de l'État et la fonction de sécurité qui lui est confiée. Au-delà des effets directs de ces technologies, par exemple sur les données personnelles et la vie privée, il existe des risques indirects traduits par le « *chilling effect »,* soit une modification des comportements individuels par la simple sensation d'être observé ou surveillé. L'emploi de ces technologies par les forces de sécurité n'est donc pas anodin. C'est la raison pour laquelle les cas d'usage doivent être déterminés au cas par cas, si nécessaire avec le concours de la société civile, et assortis de garanties strictes. Plus largement, l'emploi des technologies de sécurité s'inscrit dans le pacte de confiance qui doit exister entre les forces et la population.

Face au large champ des nouvelles technologies de sécurité, la mission a retenu une approche opérationnelle et pragmatique en définissant les usages qui lui semblent prioritaires au regard de trois objectifs : répondre aux besoins des forces de sécurité, préserver les libertés et privilégier les technologies mures d'un point de vue technique.

Tout d'abord, dans le champ des technologies d'aide à l'identification des situations de danger, il est proposé de procéder à des expérimentations dûment encadrées en situation réelle. La détection automatisée d'anomalies dans l'espace public (ex : mouvements de foule, bagarres) ainsi que le renforcement des contrôles d'accès à des sites sensibles (par exemple par des scanners corporels) pourraient être autorisés par voie législative, à des fins de test. Leur utilité serait particulièrement marquée dans la préparation des grands évènements de 2023 et 2024, ce qui nécessite à court terme de mener des expérimentations afin de vérifier les apports opérationnels réels, les conditions de déploiement et le cadre d'emploi. Par ailleurs, il peut être envisagé d'ouvrir à moyen terme dans la loi un cadre expérimental de recueil automatique de données librement accessibles en sources ouvertes afin d'identifier des situations de danger par recueil de faisceaux d'alerte partagés par la population. Enfin, une évolution législative pourrait permettre de constituer des jeux d'apprentissage issus de données réelles afin de permettre aux acteurs de la recherche-innovation de perfectionner les algorithmes d'intelligence artificielle.

La mission recommande ensuite de dresser un ordre des priorités en tenant compte du caractère

intrusif des technologies biométriques. Les dispositifs d'authentification biométrique pourraient être déployés dans le cadre des grands évènements sportifs afin de faciliter et de sécuriser l'accès aux sites réservés et sensibles (village des athlètes par exemple). En revanche, l'identification biométrique en temps réel dans l'espace public par reconnaissance faciale mérite une approche plus prudente et progressive compte tenu de son caractère intrusif pour la vie privée. Les possibilités actuelles qui reposent sur le consentement des participants (ex : expérimentation à Nice en 2019) ne permettent pas de vérifier les usages en conditions réelles. Dès lors, sans préjudice de ce qui peut être fait à droit constant, l'ouverture d'un cadre d'expérimentation en situation réelle pourrait être soumise au débat public. La finalité devrait retenir le cas d'usage le plus grave (lutte contre le terrorisme) et l'expérimentation, décidée par le Parlement, devrait alimenter un débat public sur le bilan coûts/bénéfices de tels dispositifs.

Enfin, les équipements de projection et de mobilité des forces de sécurité peuvent être modernisés par les technologies les plus récentes, qui nécessitent un cadre d'emploi clair. Il est souhaitable de clarifier dans la loi le régime juridique qui encadre la captation d'images par drones. Le recueil d'images par les véhicules (« caméras embarquées »), qui présente des avantages opérationnels pour les forces de sécurité, doit aussi être juridiquement encadré.

Conformément à la demande du Premier ministre, la mission propose plusieurs garanties qui peuvent être apportées lors de l'emploi des technologies de sécurité afin de construire une relation de confiance entre les forces et les Français.

Tout d'abord, un certain nombre de principes, communs à l'ensemble des technologies de sécurité, peuvent venir guider l'action des forces de sécurité. Les forces sont soumises à des contraintes d'ordre technique et juridique qui sont souvent perçues comme autant de freins pour expérimenter de nouveaux usages. Il s'agit au contraire d'intégrer ces contraintes (maturité technologique, solutions souveraines, protection des données personnelles) tout en conservant l'agilité nécessaire pour tester et éprouver les technologies. Les expérimentations permettent de déterminer si elles présentent un intérêt réel pour les forces de sécurité. Si elles sont décidées, elles devraient être menées à brève échéance, afin que les forces puissent disposer des outils utiles et collectivement acceptés pour la sécurisation des grands évènements sportifs de 2023 et 2024.

Ensuite, la société civile peut être davantage mobilisée afin d'assurer une meilleure compréhension des enjeux et une définition collective des usages des nouvelles technologies. Plusieurs facteurs viennent expliquer les difficultés à accepter l'emploi des technologies dans le champ de la sécurité : le manque d'information et la polarisation croissante du débat public, la réticence au partage de données et la défiance institutionnelle qui dépasse le seul champ de la sécurité. Il est possible de résorber la défiance vis-à-vis des technologies en permettant au grand public de s'approprier les enjeux et de monter en compétence sur le numérique par la voie de la sensibilisation et de la formation mais aussi en gagnant en transparence en organisant la feuille de route du ministère sur l'ouverture des données et des codes sources. Compte tenu des enjeux, il est souhaitable de définir collectivement des choix de société en faisant participer les citoyens à l'élaboration des politiques publiques, mais surtout en organisant un débat de société sur les grandes évolutions technologiques, sur le modèle des lois de bioéthiques, qui soit structuré par les corps intermédiaires et la communauté scientifique.

Enfin, la mise en place de moyens d'évaluation et de contrôle pour superviser l'emploi des technologies de sécurité par les forces est une garantie essentielle. L'action des forces de sécurité pourrait être mieux évaluée en sollicitant, de manière plus systématique, les inspections sur l'emploi par les forces de sécurité des nouvelles technologies. Les enjeux budgétaires rendent nécessaire une appréciation objective de l'efficacité des dispositifs qui sont mobilisés. Les procédures et les moyens qui sont alloués aux autorités de contrôle méritent d'être renforcés dans la mesure où ils sont nécessaires pour articuler les libertés avec les nécessités de sécurité publique.

Synthèse des recommandations

La liste présente de manière simplifiée les principales recommandations détaillées dans le corps du rapport.

Soutenir le tissu industriel français pour préserver notre souveraineté

Recommandation 1 : accompagner le développement des entreprises françaises en encourageant les solutions technologiques en *privacy-by-design*.

Recommandation 2 : investir davantage dans les enjeux de normalisation et de certification à l'échelle internationale.

Recommandation 3 : compléter l'offre française en matière d'infrastructures de base (ex : cloud) et sécuriser certains approvisionnements (ex : données).

Recommandation 4 : faciliter le développement des technologies françaises en permettant aux entreprises de la filière de recourir à des expérimentations en situation réelle et en mobilisant l'investissement et la commande publics.

Expérimenter les technologies d'aide à l'identification de situations de danger

Recommandation 5 : permettre la détection automatisée en direct d'anomalies dans les espaces publics en expérimentant la vision par ordinateur sur des sites sensibles en amont des grands évènements sportifs de 2023 et 2024.

Recommandation 6 : ouvrir par voie législative un cadre d'usage expérimental de la captation automatique de données librement accessibles en sources ouvertes dans le but d'améliorer la détection précoce de situations de danger dans les domaines de la sécurité et du secours.

Recommandation 7 : faciliter la constitution de jeux de données réelles pour la recherche et l'innovation en matière d'intelligence artificielle.

Recommandation 8 : autoriser, par voie législative, le déploiement expérimental pluriannuel de scanners corporels pour contrôler l'accès aux sites sensibles liés à des grands événements.

Développer l'usage des techniques biométriques

Recommandation 9 : proposer l'authentification forte des accès aux sites sensibles des grands événements sportifs (ex : village olympique, des sites de compétition) sans constitution de base biométrique centralisée.

Recommandation 10 : expérimenter l'identification biométrique par reconnaissance faciale en temps réel dans l'espace public à droit constant sur la base du volontariat, comme lors de l'expérimentation menée à Nice en 2019.

Recommandation 11 : ouvrir un débat sur l'expérimentation de l'identification biométrique par reconnaissance faciale en temps réel dans l'espace public. L'inscrire dans un débat de société plus large sur l'emploi des nouvelles technologies en matière de sécurité.

Moderniser les équipements de projection et de mobilité

Recommandation 12 : clarifier dans la loi le cadre juridique d'emploi des drones et aéronefs associés par les forces de sécurité et de secours.

Recommandation 13 : procéder à des expérimentations en matière de lutte anti-drones dans le cadre des grands événements.

Recommandation 14 : clarifier dans la loi le cadre juridique d'emploi des dispositifs de captation d'image intégrés aux véhicules des forces de sécurité et de secours (« caméras embarquées »).

Guider par des principes l'usage des technologies par les forces de sécurité

Recommandation 15 : s'assurer du niveau de maturité de la technologie dont l'emploi est envisagé et privilégier des solutions souveraines pour les usages les plus critiques. S'assurer de l'intervention humaine dans l'emploi des technologies de sécurité à des niveaux proportionnés à la sensibilité des usages.

Recommandation 16 : se doter d'une politique de la donnée qui intègre pleinement les enjeux de protection de données personnelles afin de déterminer dans quelle mesure les technologies de sécurité peuvent se concilier avec la protection des données.

Recommandation 17 : recourir aux expérimentations en déterminant quelles sont celles qui peuvent être menées à droit constant et quelles sont celles qui nécessitent de prendre des dispositions législatives ou réglementaires. Prioriser les emplois potentiellement utiles pour la sécurisation des grands évènements. Ouvrir les crédits nécessaires au financement des expérimentations.

Construire une relation de confiance avec la société autour des technologies

Recommandation 18 : favoriser la sensibilisation aux nouvelles technologies afin d'assurer la montée en compétence du grand public sur les sujets technologiques.

Recommandation 19 : faire mieux connaître l'action des forces de sécurité intérieure et l'emploi des technologies de sécurité.

Recommandation 20 : valider les compétences numériques de la population à l'occasion du service national universel.

Recommandation 21 : recruter des profils à la fois juridiques et techniques au sein du ministère de l'Intérieur.

Recommandation 22 : organiser la feuille de route du ministère de l'Intérieur sur l'ouverture des données en l'articulant avec les nécessités de sécurité publique.

Recommandation 23 : associer les citoyens à la conception et à la mise en œuvre des politiques publiques dans le domaine de la sécurité en recourant à des ateliers participatifs au moment des expérimentations et en organisant des consultations publiques en amont de la présentation des projets de texte.

Recommandation 24: lancer un débat public sur les grandes innovations technologiques, à l'image des lois bioéthiques, afin d'apprécier à intervalle régulier les évolutions techniques et leurs conséquences sur la société.

Superviser l'action des forces de sécurité

Recommandation 25 : intégrer la prévention des risques dans les évaluations techniques et opérationnelles qui sont réalisées par les forces de sécurité intérieure.

Recommandation 26 : mieux évaluer en amont les besoins des forces de sécurité mais aussi renforcer la qualité des textes relatifs aux technologies de sécurité (études d'impact, avis).

Recommandation 27 : solliciter, de manière plus systématique, les inspections afin d'évaluer le recours aux technologies de sécurité en associant des chercheurs et des experts au processus d'évaluation.

Recommandation 28 : renforcer les procédures qui encadrent actuellement l'emploi des technologies de sécurité (ex : encadrement de la vidéoprotection) par les forces et les adapter, quand cela est possible, aux évolutions technologiques (ex : nouveaux outils de recueil d'images).

Recommandation 29 : renforcer les moyens des autorités de contrôle en évaluant les besoins en ressources humaines de la CNIL afin qu'elle puisse accompagner les entreprises et les administrations.

Recommandation 30 : étudier la création d'un parquet national cyber disposant de ressources et des expertises suffisantes pour instruire les affaires de cyber délinquance les plus complexes.

Introduction

Par une lettre du 23 avril 2021, le Premier ministre a confié au député Jean-Michel Mis une mission relative à l'usage des nouvelles technologies dans le domaine de la sécurité.

L'objectif principal fixé à la mission était de déterminer les apports des nouvelles technologies de sécurité pour l'État tout en proposant des garanties pour encadrer strictement leur usage afin de protéger les libertés publiques et les libertés individuelles.

Le rapport issu des travaux de la mission dresse un état des lieux des principaux enjeux soulevés par les nouvelles technologies dans le domaine de la sécurité : enjeux pour les libertés, enjeux de sécurité, enjeux économiques et industriels (**Partie 1**). Les récentes évolutions technologiques posent des questions nouvelles pour les libertés, en particulier lorsque les technologies sont utilisées à des fins sécuritaires. En outre, les technologies les plus récentes offrent de nouvelles capacités aux forces et font évoluer leurs missions et leurs besoins. Enfin, la France dispose d'un secteur économique dynamique, à forte valeur ajoutée et hautement stratégique pour sa souveraineté, qu'il convient de préserver et d'accompagner.

La mission identifie les principaux apports attendus des nouvelles technologies pour les forces de sécurité et de secours (**Partie 2**). Face à l'ampleur du champ des technologies envisageables, la mission a retenu celles qui lui paraissaient les plus pertinentes au regard des besoins des forces, des enjeux pour les libertés et de la maturité de l'offre technologique. Elles donnent aux forces de sécurité et de secours des outils d'aide à la décision pour mieux identifier les situations de danger, suivre les personnes qui représentent une menace pour la sécurité et agir en mobilité.

Le rapport fixe enfin les garanties qui devraient accompagner l'emploi des technologies de sécurité afin de construire une relation de confiance entre les forces et la société (**Partie 3**). Cela passe par la définition d'un socle de principes communs pour guider l'action des forces mais aussi par la montée en compétence du grand public sur le numérique et une définition collective des usages. La supervision de l'action des forces est une garantie essentielle dans la mesure où elle est à la fois un gage d'acceptabilité et d'efficacité dans l'emploi des technologies de sécurité. Enfin, la mise au débat des nouvelles technologies favorise une bonne compréhension des enjeux et permet d'élaborer un cadre d'emploi consensuel.

I. La sécurité à l'aune du numérique pose des enjeux fondamentaux en matière de libertés

A. La société numérique se développe et pose de nouveaux défis

La question des nouvelles technologies de sécurité ne peut se poser sans considérer la révolution technique d'ensemble que traversent nos sociétés. L'ensemble des interlocuteurs de la mission a en effet, de manière plus ou moins marquée, souligné les évolutions techniques et éthiques affectant la quasi-intégralité de nos usages.

Celle-ci se traduit tout d'abord par le développement d'un cyberespace dans lequel se réalisent une part croissante des activités individuelles et des échanges (transactions, correspondance, communication/information). Le cyberespace se forme par la dématérialisation croissante de ce qui était traditionnellement réalisé au moyen d'un acte ou d'une interaction physique. Dans la vie courante, le recours aux services en ligne est de plus en plus fréquent. Ainsi, 13 % du commerce de détail des biens est réalisé en ligne[1]. Près de 200 000 entreprises (commerciales, industrielles, artisanales, agricoles) disposent de sites marchands. Le service public se numérise également au travers de télé-procédures mises en place pour le citoyen. Selon une étude réalisée pour le compte de la direction interministérielle à la transformation publique (DITP), la part des usagers qui effectuent leurs démarches administratives en ligne a augmenté de plus de 10 points entre 2014 et 2018, même si le mode d'accès privilégié restait le guichet (57 % contre 36 % pour Internet)[2]. La stratégie « Action publique 2022 » prévoit de dématérialiser prioritairement les 250 procédures les plus utilisées. Fin 2020, l'Observatoire de la qualité des démarches en ligne estimait que 70 % de ces démarches étaient réalisables en ligne.

Comme tous les domaines de la vie quotidienne (santé, transports, vie culturelle, consommation courante), la politique de sécurité est affectée par ces changements. Elle doit s'adapter à un cyberespace et à la criminalité associée. La petite criminalité ou la criminalité organisée se sont en effet emparées du monde numérique pour y trouver de nouvelles opportunités délictuelles et criminelles ou pour y dissimuler leurs activités. En outre, le monde numérique expose la société à des risques spécifiques, par exemple pour les particuliers (arnaques en ligne) ou de façon plus systémique (cyberattaques). Par ailleurs, les forces de sécurité ont la possibilité de revoir profondément leurs processus de décision et leurs capacités opérationnelles en ayant recours aux nouvelles possibilités offertes par les données, les outils (équipements mobiles) et les moyens (intelligence artificielle).

Plus fondamentalement, les processus politiques ont été affectés par cette révolution numérique. Le scandale « Cambridge Analytica » est ainsi régulièrement cité comme exemple d'une manipulation de la donnée à des fins d'influence électorale. Par ailleurs, le rôle des réseaux sociaux dans la constitution de communautés d'action a été souligné dans de nombreux mouvements sociaux et politiques. Ces plateformes en ligne ont en effet proposé de nouveaux moyens d'échange, de communication, de mobilisation, d'agrégation en communautés avec une rapidité et une ampleur peut-être sans précédent.

Cette translation du physique au numérique a engendré **une révolution de la donnée**, dont le rôle comme matière première de production de services s'est renforcé, qu'il s'agisse de prestations commerciales ou de service public. Les possibilités offertes par les données ne sont pas nouvelles, en témoigne le recours ancien aux sondages à des fins commerciales ou la statistique dans la décision publique. Mais cette dernière décennie a été marquée par le double phénomène de massification et de valorisation accrue de la donnée (qu'elle soit textuelle/écrite, visuelle, vocale). La multiplication et la démocratisation des capteurs de données, la massification de la donnée produite et collectée, la facilitation technique de la duplication des données et l'automatisation possible du traitement par des techniques algorithmiques constituent certains des aspects fondamentaux de cette révolution numérique.

Compte tenu de tels enjeux et effets réels, la révolution de la donnée a eu des répercussions majeures sur le concept de données personnelles. La révolution numérique n'a pas révélé le potentiel de création de valeur contenu dans les données ; c'est bien le bond quantitatif et qualitatif réalisé

(1) France Stratégie, « Pour un développement durable du commerce en ligne », mars 2021.
(2) Enquête « Événements de vie 2018 » par BVA pour le compte de la DITP.

ces dernières années qui a conduit à repenser l'approche de la donnée personnelle. Les capacités de collecte, qui peut se faire sur une base volontaire mais sans consentement explicite ou pleine conscience des enjeux, ont en effet augmenté les données disponibles(3) et parfois leur précision. Il est ainsi estimé que le volume des données produites dans le monde sera multiplié par plus de cinq d'ici 2025, passant de 33 zettaoctets à 175 zettaoctets. En outre, la nature des données a évolué : les capteurs vidéo et sonores se sont en effet multipliés (vidéoprotection, par exemple) et démocratisés (smartphones). Les données personnelles figurent au cœur des préoccupations sur les libertés individuelles, comme l'ont souligné de nombreux interlocuteurs auditionnés.

L'émergence de l'intelligence artificielle (IA) moderne donne aux révolutions numérique et de la donnée une dimension supérieure. L'IA recouvre des technologies qui combinent des données, des algorithmes et une puissance de calcul. Schématiquement l'IA s'est d'abord, et de manière récente, portée sur l'image – le premier réseau de neurones a été appliqué à la reconnaissance de l'image en 2012 -, pour ensuite se déplacer vers les données textuelles écrites et orales.

Pour de nombreux contributeurs au débat public et une partie des interlocuteurs de la mission, l'IA représente bien davantage qu'un progrès technique ; elle est le vecteur d'une profonde évolution de société. En effet, poussées à l'extrême, ses potentialités peuvent changer radicalement le rapport de l'Homme à la décision et au libre-arbitre. D'une part, l'IA affectée au traitement des données exerce une influence cognitive sur la perception qu'a l'être humain de son environnement en l'orientant, au risque de créer des zones d'enfermement algorithmique. Ainsi, des plateformes de visionnage de vidéos en ligne tendent à recommander des contenus en suivant les historiques de consultations. L'avantage, indéniable, est une offre sur mesure ; l'inconvénient peut être une moindre possibilité d'ouverture à la diversité et à la découverte, au risque d'inscrire l'individu dans un univers uniforme. D'autre part, avec l'IA, l'Homme peut confier une partie toujours croissante du processus de réflexion et de décision aux technologies. Si la quasi-intégralité des personnes auditionnées a insisté sur le nécessaire contrôle humain de la machine, le potentiel de la technologie n'interdit pas une autonomie quasi intégrale. Les technologies actuelles peuvent déjà dépasser la seule étape du tri et de la sélection d'information pour proposer des conseils et challenger des décisions. Les atouts de tels outils face à une masse de données sont indéniables mais ils ne vont pas sans risques.

C'est dans ce cadre dressé à grands traits que se place le débat sur l'utilisation des nouvelles technologies en matière de sécurité. La question est d'autant plus sensible qu'elle réunit en une seule problématique deux sujets fondamentaux : d'une part, la nature du contrat social des démocraties occidentales modernes, qui, dans la substitution de la liberté civile à la liberté naturelle, délèguent l'exercice de la puissance à la force publique ; d'autre part, le possible repositionnement de l'Homme comme être doué de raison et de libre-arbitre induit par la révolution technologique en cours.

L'une des questions qui émerge est : quand bien même il est souhaitable de prendre le temps de la décision en matière de nouvelles technologies (de quoi parle-ton ? pourquoi ? comment ?), est-ce encore possible ? Les acteurs associatifs mettent en garde contre la facilité qu'il y aurait à abdiquer face à de tels enjeux au motif qu'il serait impossible de « désapprendre » une technologie constituée et adoptée par une partie des usagers. Et il est vrai que les nouveaux usages technologiques, parmi lesquels les plus contestés comme la reconnaissance faciale, sont d'ores et déjà adoptés. Ils le sont dans la vie courante de tout un chacun, pour des opérations quotidiennes (ex : déverrouiller un téléphone par reconnaissance faciale, ouvrir une porte par reconnaissance digitale, passer une commande vocale) ; ils le sont aussi, de par le monde, par la puissance publique dans ses missions de police. Les drones par exemple ont aussi investi les usages quotidiens, notamment dans la vie civile.

En ne se saisissant pas du sujet, l'État en France prendrait donc le double risque de ne pas bénéficier des opportunités offertes par ces technologies pour l'exercice de ses missions et d'être dépassé technologiquement. Il serait dépassé par la base citoyenne qui a recours dans sa vie privée aux dernières technologies – au risque de ne plus savoir répondre correctement aux besoins et aux défis de ceux à qui elle destine le service public - et par d'autres pays, parfois inscrits dans des systèmes de valeurs différents ou économiquement concurrents. Face à cette possible contradiction, la ligne retenue dans ce rapport est pragmatique et prudente. Afin de ne pas nier les risques comme les opportunités que représentent les nouvelles technologies, il est

(3) Étude du cabinet IDC réalisée en 2019 pour le compte de la Commission européenne dans le cadre du Livre blanc sur l'intelligence artificielle : https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf

nécessaire d'en préciser les possibilités, les implications et les usages nécessaires et proportionnés dans un cadre admis collectivement.

B. Des enjeux fondamentaux pour les libertés

Les auditions, les contributions et les ressources réunies et consultées par la mission convergent pour affirmer que les nouvelles technologies de sécurité posent des enjeux fondamentaux en matière de libertés. Ce constat est sans surprise, tant il imprègne le débat public.

Certaines personnes entendues font la différence avec des évolutions techniques majeures qui ont pu avoir lieu par le passé. Ainsi, lorsque Alphonse Bertillon initie l'anthropométrie judiciaire et résout la première affaire criminelle française à l'aide d'empreintes digitales, ces méthodes ne sont pas fondées sur des équipements intelligents partiellement autonomes, interconnectables et mobiles. De la même manière, si le débat sur la vidéosurveillance (puis vidéoprotection), a été très vif dans les débuts du déploiement des systèmes de caméras, leur portée était encore limitée par les capacités techniques (qualité de l'image, fixité des dispositifs). La recherche de rationalité scientifique peut parfois conduire à des impasses comme nous l'avons connu au XIX^{e} siècle avec la phrénologie.

Les évolutions techniques en cours ont une portée tout autre. Elles se caractérisent par la puissance de nouveaux outils reposant sur la captation et l'exploitation de données, tant en précision qu'en masse, ainsi que par les possibilités en mobilité et en interconnexion qui leur donnent une quasi-ubiquité.

Les principales craintes portent sur le recueil ou la captation de données personnelles et notamment les plus sensibles (données biométriques). La CNIL, dans sa publication de novembre 2019 sur la reconnaissance faciale[4], rappelait la vigilance particulière qui devait être accordée à la biométrie du visage. Donnée personnelle non révocable, elle peut potentiellement être un moyen de reconnaissance dans l'espace public de personnes n'ayant effectué aucune démarche explicite et volontaire (à l'inverse par exemple de la présentation d'une pièce d'identité ou d'empreintes digitales). En outre, elle est potentiellement disponible partout dans un contexte de multiplication des capteurs d'images et d'interactions croissantes entres les sphères privées et publiques. L'intelligence artificielle concentre également nombre des inquiétudes, non sans lien avec le recueil et l'exploitation des données personnelles. L'IA interroge car elle permet un allégement de l'empreinte humaine dans la décision et induit une relative opacité de fonctionnement (effet « boîte noire »).

Les interrogations sont donc légitimes tant les libertés en jeu sont fondamentales : protection des données personnelles, respect de la vie privée, liberté d'expression et de réunion, dignité humaine, droit à un recours juridictionnel effectif et à un procès équitable. Ces principes énoncés revêtent des cas très concrets pour la vie quotidienne de chacun d'entre nous.

La protection des données personnelles est garantie par la loi « informatique, fichiers et libertés » (IFL)[5] et par le règlement général sur la protection des données (RGPD)[6].

Le respect de la vie privée est également fragilisé par nombre d'usages possibles des nouvelles technologies. La Défenseure des droits a ainsi, dans un avis sur la proposition de loi sécurité globale[7], considéré que l'usage des drones et l'accès élargi aux images de multiples caméras fixes et mobiles pouvaient porter une atteinte disproportionnée au droit à la vie privée.

La liberté de réunion peut être entravée par la pression indirecte exercée par des technologies de surveillance. De même, les capacités de collecte et de traitement de données textuelles automatisées et en masse peuvent conduire à une restriction de la **liberté d'expression** sur Internet. Sur l'exercice de ces libertés, la littérature en sciences humaines identifie un risque de « chilling effect », soit une autocensure par le simple fait de savoir qu'une technologie de sécurité peut être appliquée. Les impacts des technologies sur les libertés doivent donc s'entendre explicitement mais aussi par leurs effets indirects.

(4) Reconnaissance faciale : pour un débat à la hauteur des enjeux, CNIL, novembre 2019.
(5) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
(6) Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
(7) Avis 20-05 du Défenseur des droits sur la proposition de loi relative à la sécurité globale, novembre 2020.

La dignité humaine peut quant à elle être fragilisée par la captation, la diffusion, parfois une reproduction à l'infini, de données personnelles.

Enfin, **le droit à un recours juridictionnel effectif et à un procès équitable** peut se trouver entaché par l'asymétrie entre un citoyen lésé et l'entité utilisatrice d'une technologie complexe. Comment accéder à l'information permettant de départir le vrai du faux ? Comment assurer une compréhension suffisante des technologies par l'autorité judiciaire pour permettre le rendu d'une décision juste ?

Le contexte de frottements entre libertés et sécurité dans lequel s'inscrit l'approche des technologies dont il est question ne doit pas conduire à une lecture binaire qui serait trop simplificatrice. La complexité du sujet mérite en effet une réflexion plus fine que ce rapport ne saurait épuiser, s'il en avait seulement l'intention. Ces grands équilibres permettent néanmoins de ressaisir le cadre conceptuel qui influence l'appréhension politique de la mission.

Dans un certain imaginaire collectif, la force publique porte en elle des risques de dérive sécuritaire. La méfiance et la défiance que ressent une partie de la population envers l'État et la fonction de sécurité qui lui est confiée, nourrissent ces craintes. Elles interviennent dans un contexte où est largement répandu le sentiment que les droits et libertés fondamentaux tendent à reculer[8]. Cette relégation ressentie des libertés au second plan, au nom d'une sécurité qui doit pourtant permettre de protéger leur expression, n'est pas attribuée seulement à l'État. Celui-ci peut certes être tenté de trouver dans la restriction de libertés une réponse à des questions nouvelles. Mais, pour certains penseurs, les citoyens eux-mêmes, à l'exception des individus ou des groupes les plus actifs, risquent de renoncer d'eux-mêmes à l'exercice de leurs libertés par désintérêt ou par indifférence[9].

Les enjeux et craintes associés aux nouvelles technologies existent dans leur usage non-sécuritaire. Les usages à des fins commerciales ont d'ailleurs pu motiver pour partie les grandes évolutions législatives sur la protection des données personnelles. Cependant, la question prend une dimension supérieure dès lors qu'il s'agit d'un emploi par les forces de sécurité.

Une forme de méconnaissance des finalités plurielles et complexes des institutions, voire d'indifférence envers elles, contribue à cette dynamique. C'est notamment le cas pour ce qui concerne la fonction de sécurité de l'État. Celle-ci est parfois, lorsqu'il s'agit de technologies, assimilée à la surveillance. **L'emploi des nouvelles technologies n'est alors pas perçu comme contributeur à la sécurité collective, mais comme instrument de la surveillance de masse**. Si la surveillance peut être nécessaire pour assurer la sécurité individuelle et collective, toute politique de sécurité n'est pas une politique de surveillance. En outre, la surveillance elle-même semble automatiquement perçue comme massive, quand en fait elle peut n'être ciblée que sur des individus représentant un danger pour la société. Il faut enfin relever que les restrictions légales faites aux libertés sont l'émanation de la volonté de la représentation nationale. Le législateur cherche alors à concilier les objectifs de sécurité et de préservation des libertés.

La crainte qui porte sur les intentions de la force publique est amplifiée par les capacités qu'offrent les nouvelles technologies. Ainsi, la Commission européenne[10] reconnaît, pour en souligner le risque, le potentiel que les technologies utilisant de l'intelligence artificielle peuvent avoir en matière de surveillance de masse. Les inquiétudes sont nourries par la part d'inconnu qui entoure les nouvelles technologies. C'est en effet un ensemble mouvant, mal identifié, mal défini et mal compris. La conviction portée dans ce rapport est qu'il est nécessaire, pour avoir un débat public éclairé, de distinguer les capacités techniques des intentions et finalités et par conséquent des usages qui en sont faits.

Paradoxalement, et cela est souligné par de nombreux interlocuteurs de la mission, tout un chacun semble moins exigeant dans ses comportements de consommation que dans sa place de citoyen. Ainsi, la sensibilité accordée aux données personnelles apparaît relativement faible dans le rapport aux services numériques (plateformes de recherches et d'achats, réseaux sociaux) alors qu'une méfiance toute particulière entre en éveil dès lors qu'il s'agit d'utilisation des données par

(8) Sondage Odoxa pour le Conseil national des barreaux publié le 17 juin 2021 : 77 % des sondés ont le sentiment que les libertés et droits fondamentaux ont tendance à reculer.

(9) Dans *Sans la liberté*, publié en 2019, François Sureau estime que l'érosion des libertés s'accroît dans l'indifférence générale de la société. Il considère que « *Nous nous sommes déjà habitués à vivre sans la liberté* » (entretien accordé au journal Le Monde, publié le 24 septembre 2019).

(10) Livre blanc sur l'intelligence artificielle, Commission européenne, février 2020.

l'État, *a fortiori* dans sa fonction régalienne. **Ainsi, le consommateur consentirait plus facilement à ce que le citoyen refuserait catégoriquement.**

Ce surcroît de méfiance face à l'usage sécuritaire des technologies n'est pas illégitime et ne doit pas être écarté ou ignoré. Les nouvelles technologies en elles-mêmes présentent une force intrusive puissante à la fois par leur précision (par exemple, le ciblage algorithmique) et la densité des réseaux supports (par exemple, la multiplicité des capteurs de données). Dès lors qu'elles sont utilisées à des fins sécuritaires, elles doivent faire l'objet d'un encadrement, d'un contrôle et d'une pédagogie renforcés. Il ne s'agit donc pas de disqualifier les craintes mais de reconnaître leur légitime place et de les prendre en compte pleinement, en proposant une réponse qui soit à la hauteur de la profondeur des enjeux pour les libertés fondamentales.

C. Une approche de la sécurité challengée par les nouvelles technologies

Les forces de sécurité intérieure évoluent dans un environnement qui se numérise toujours plus et face à des acteurs qui ont un recours accru aux dernières technologies. Cela implique de savoir exploiter, pour des missions de sécurité, les nouveaux éléments générés par le numérique. La maîtrise de la donnée, par sa quantité et sa variété (texte, images vidéos et photos, sons – voix, bruits –, géolocalisation) et la multiplicité des capteurs, pose un défi nouveau. Il ne s'agit pas pour les forces de disposer de toute la donnée sans discrimination d'usage, mais de savoir exploiter la donnée utile, dans un cadre légal défini, pour des missions précises (alerte, planification, secours, enquête, etc.).

La numérisation des activités implique aussi de développer des capacités défensives face à la menace cyber qui se développe sous différentes formes. Les services numériques sont en effet exposés à des risques qui peuvent viser la déstabilisation des institutions (cyber-activisme), l'espionnage, le sabotage, la criminalité (rançongiciel, hameçonnage)(11).

La vulgarisation de certaines technologies, qui peut les rendre accessibles au plus grand nombre, implique que les forces de sécurité soient équipées au niveau de leurs adversaires ou, *a minima*, qu'elles maîtrisent suffisamment les technologies employées pour en contrer les usages malveillants. L'exemple des drones, qui sera développé dans la seconde partie, est éloquent. D'origine militaire, ces aéronefs ont été adaptés à des usages de loisir. En France, il s'est vendu près de 100 000 drones de loisirs en 2014, 300 000 en 2015 et 400 000 en 2016(12). Le durcissement de la réglementation a engendré une contraction des ventes, mais ces données montrent la capacité de popularisation de technologies initialement réservées à un public fermé, et qui peuvent être utilisées à des fins malveillantes. Le constat peut être étendu, par exemple, à la menace cyber : les cyberattaques d'individus isolés, parfois extraterritoriaux, peuvent porter atteinte à des systèmes entiers ou des institutions. Ces derniers doivent se prémunir en amont de la menace (cybersécurité), mais les forces de sécurité doivent aussi développer, pour l'aval, des outils d'investigation numérique. L'investigation numérique s'étend aussi aux activités criminelles qui se développent sur le Net, y compris le *dark web* (trafics divers : êtres humains, stupéfiants, armes, fausses identités, crypto délinquance). **Il est indispensable que les forces de sécurité ne se trouvent pas en asymétrie de capacités face à d'éventuels adversaires et puissent** a minima **déployer des contre-mesures.**

Les nouveaux outils d'aide à la décision permettent en outre de soutenir l'action des forces dans une société plus dense et complexe. L'accroissement démographique, la multiplication et la densification des flux et des rassemblements posent de nouveaux défis : risques d'accidents, cibles terroristes. En outre, les forces de sécurité relèvent que la criminalité a évolué : par le passé, un délinquant côtoyait quotidiennement un nombre limité de personnes sur le territoire national ; aujourd'hui, il peut être en relation avec un nombre significatif de personnes, dans un temps limité, à l'échelle mondiale, grâce aux réseaux numériques. Par conséquent, **les technologies d'aide à la décision, dans l'alerte, la planification opérationnelle, l'enquête, peuvent aider les forces de sécurité** à faire face à ces nouvelles complexités.

(11) Source : ANSSI.
(12) Source : Institut GfK.

Encadré : les enjeux de la sécurisation des Jeux olympiques et paralympiques de 2024

Les Jeux olympiques et paralympiques (JOP) de 2024 accueillis en France présentent un défi de sécurité de premier ordre.

La dimension de l'événement est en effet sans précédent pour la France. Ils se dérouleront pendant 57 journées consécutives dans des sites multiples répartis sur l'ensemble du territoire national avec une forte concentration dans les grandes agglomérations (notamment Paris centre et Nord-Est, Marseille, Lille). Environ 13 millions de billets seront vendus pour les compétitions en stade, auxquels s'ajouteront les visiteurs en *fanzones* et *live sites* (13 millions de personnes à Londres en 2012). Cette affluence fera peser une tension accrue sur les transports en commun (estimation de +2 millions de voyageurs par rapport aux trajets habituels). La seule cérémonie d'ouverture pourrait – sous réserve du format final qui sera retenu – concentrer à Paris une centaine de chefs d'États et plus de 100 000 invités et spectateurs payants qui s'ajouteront aux spectateurs non munis de billets spécifiques.

Les JOP 2024 se dérouleront dans un contexte de menace importante, notamment sur le plan du risque terroriste. La dimension, mais aussi la sensibilité (délégations officielles, personnalités d'envergure mondiale) et la visibilité de l'événement (rediffusion dans 200 pays, pour environ 5 milliards de téléspectateurs), rendent nécessaire la mise en place d'un dispositif de sécurité d'ampleur.

Un an avant les JOP 2024, la France accueillera la coupe du monde de rugby. Celle-ci se déroulera en 48 matchs sur une cinquantaine de jours, dans 9 villes, pour près de 3 millions de spectateurs en stade (dont environ 600 000 visiteurs étrangers).

Ces enjeux sont mobilisateurs pour l'offre industrielle et de services française, qui a structuré une réponse dédiée aux grands événements sportifs dans le cadre du contrat de filière.

D. Une industrie française de pointe, acteur de la souveraineté et de la croissance

1. Un secteur économique dynamique, pourvoyeur d'emplois et de recettes à l'exportation

La filière industrielle française de la sécurité compte près de 4 000 entreprises, emploie 130 000 personnes et réalise un chiffre d'affaires de près de 28 Md EUR[13]. C'est une filière dynamique, qui a connu un taux de croissance de 5-6 % sur les dernières années.

L'offre française est complète avec des entreprises présentes dans la cybersécurité, l'identité numérique, la protection des infrastructures et des réseaux, la sécurité du transport, le secours aux personnes, la lutte contre le terrorisme et la grande criminalité, la sécurité des territoires ou encore la gestion de crise**. Elle peut ainsi répondre, tant aux besoins de sécurité des entités d'État, que des entreprises ou des particuliers**.

Ses domaines d'excellence et la présence de leaders mondiaux parmi les grands groupes et les PME-ETI lui font réaliser près de 13 Md EUR de chiffre d'affaires à l'international. Les industriels auditionnés soulignent l'importance des marchés internationaux pour leur développement. Cependant, un solide marché domestique leur est essentiel. Il leur assure un socle économique, grâce à un accès au marché rendu plus facile par la bonne compréhension des besoins et de la régulation et la proximité des commanditaires avec les centres de décision et de production. En outre, les succès sur le marché domestique peuvent renforcer la crédibilité des industriels français vis-à-vis des acheteurs étrangers.

Les entreprises françaises sont favorables au concept de *privacy by design*. Il leur permet de développer des solutions technologiques éthiques qui protègent les données personnelles, ce qui constitue **un avantage comparatif pour la filière dans un contexte de forte concurrence internationale**. Les consommateurs sont de plus en plus sensibles à la question de la protection des données personnelles. Dans sa communication « *Façonner l'avenir numérique de l'Europe* », la Commission européenne estime que la confiance est un facteur de compétitivité pour les entreprises européennes.

(13) Données issues du Contrat stratégique de filière « industries de sécurité » du 29 janvier 2020.

La filière française est aussi marquée par une dynamique d'excellence et d'innovation, animée par une communauté d'acteurs diversifiés et de pointe. L'écosystème regroupe tout d'abord les entreprises de toutes tailles, dont des grands groupes leaders dans de multiples domaines (biométrie et identité numérique, paiements sécurisés, « secure elements », communications sécurisées). La filière comprend également des acteurs de la Recherche et Innovation, notamment des pôles de compétitivité (SAFE, SYSTEMATIC, SCS, TES, MINALOGIC, MER) et les organismes de recherche publique (CEA, INRIA, CNRS, universités). Au total, en 2020, la filière industrielle déclarait 1,7 Md EUR de dépenses de recherche-développement, soit 5 % de son chiffre d'affaires global.

La concurrence internationale invite à structurer toujours plus la filière et ses partenaires. Les travaux du Livre blanc de la sécurité intérieure de 2020 ont mis en avant le besoin de clarifier et de renforcer les partenariats public-privé et industrie-université. Cet axe de travail a été mis en évidence par les industriels entendus en audition et dans les contributions reçues.

Afin de coordonner son action, dans le double objectif de développer des synergies et de formuler des offres consolidées, **la filière française de sécurité intérieure se structure depuis près d'une décennie.** La coopération public-privé a pris la forme d'un comité stratégique de filière labellisé en 2018 par le conseil national de l'industrie et concrétisé par un contrat stratégique signé le 29 janvier 2020. Ce contrat porte cinq projets structurants mobilisateurs pour la filière et intéressant les pouvoirs publics : sécurisation des JOP 2024 et des grands événements, cybersécurité et sécurité de l'internet des objets, identité numérique, territoires de confiance et numérique de confiance.

2. Assurer la souveraineté technologique en matière de sécurité intérieure

Apparue dans les années 2000, la notion de souveraineté numérique s'entend comme la capacité de l'État à agir dans le cyberespace. En 2019, la commission d'enquête du Sénat sur la souveraineté numérique l'envisageait sous deux angles : d'une part, la cyberdéfense (*« faculté d'exercer une souveraineté dans l'espace numérique, qui repose sur une capacité autonome d'appréciation, de décision et d'action dans le cyberespace »*), d'autre part, la maîtrise de ses actifs (« *la capacité de garder ou restaurer la souveraineté de la France sur les outils numériques afin de pouvoir maîtriser nos données, nos réseaux et nos communications électroniques.* »)

La souveraineté, entendue comme la liberté d'action d'une Nation, se transforme dans le contexte de dématérialisation croissante des échanges que connaissent nos sociétés. Dans l'ensemble, l'enjeu de souveraineté numérique recouvre, d'une part, la capacité des États à agir dans le cyberespace et, d'autre part, les défis opposés à l'exercice de leurs fonctions traditionnelles par des acteurs privés transnationaux technologiquement en pointe.

Il est possible de structurer les objectifs de la souveraineté numérique autour de trois dimensions :

- Les enjeux de défense et de cybersécurité : l'autonomie française dans le cyberespace et les infrastructures essentielles, la lutte contre les cybermenaces.
- Les enjeux industriels : le soutien aux secteurs-clefs et la création d'un écosystème favorable aux acteurs privés.
- Les enjeux de régulation économique : l'adaptation de la réglementation aux défis du numérique.

La souveraineté numérique peut se décliner en trois cercles : les citoyens (protéger les données personnelles), les entreprises (sécuriser l'usage des données) et l'État (face aux concurrents publics et privés).

Si l'impératif de souveraineté numérique se traduit génériquement pour les grands domaines des nouvelles technologies (Big data, IA, cybersécurité, Cloud, identité numérique blockchain et quantique) et tous les secteurs sensibles (santé, transports, énergie, etc), **l'enjeu de souveraineté est plus marqué dans les usages régaliens des nouvelles technologies.**

Le recours à des technologies étrangères, en effet, n'est pas sans risques : refus d'export, contrôle extérieur, déni de service, écoute, détournement. En outre, l'application d'un cadre juridique extraeuropéen crée à la fois un risque pour la concurrence mais aussi pour la protection des données personnelles des citoyens européens. Les niveaux de protection des données ne sont pas équivalents entre l'Europe et les pays tiers.

Dans les dernières années, des marchés passés par les autorités publiques françaises avec des fournisseurs étrangers ont engendré des polémiques[14]. Des critiques ont été plus récemment formulées dans le débat public sur le choix de Microsoft, comme hébergeur de la plateforme de données de santé (« Health Data Hub »). Ces exemples témoignent de la sensibilité des questions relatives à la souveraineté numérique dans l'opinion publique. Elle constitue un nouvel enjeu pour les politiques publiques, mais aussi pour la société[15].

Or, l'environnement international est marqué par une accélération de l'innovation et une très forte concurrence entre États. Les acteurs français sont pris dans une course mondiale à l'innovation sur les nouvelles technologies. A titre d'exemple, environ 3 Md EUR ont été investis dans l'IA en Europe en 2016, contre quatre fois plus (12 Md) en Amérique du Nord et deux fois plus (6,5 Md) en Asie[16].

Le principal risque est une forme de renoncement, alors qu'il faudrait faire du sujet de la souveraineté numérique un enjeu stratégique européen, ainsi que le rappelait le commissaire au marché intérieur Thierry Breton[17] : « *Il faut assurer la souveraineté numérique de l'Europe* ».

Il est donc essentiel que la France assure et maintienne son autonomie en matière d'industries de sécurité. Les solutions, ou au moins les entreprises qui les développent, sont en outre souvent communes aux forces de sécurité intérieure et aux Armées. Le savoir-faire français mérite dès lors d'être soutenu afin de garantir, pour les fonctions régaliennes de l'État, une possibilité de recours à des technologies françaises. Les enjeux économiques, en termes d'investissement ou du fait des effets d'échelle permis par le recours aux données, peuvent conduire à envisager des partenariats au niveau européen.

La mobilisation française en faveur de sa souveraineté numérique peut retenir plusieurs priorités.

Elle devrait, en premier lieu, s'inscrire dans un équilibre entre le développement de solutions nationales parfois dépendantes d'approvisionnements internationaux et le recours à des solutions détenues par des acteurs déjà dominants. Dans certains cas, l'effort d'investissement à consentir pour développer les technologies sur lesquelles la France n'a pas la main serait tellement important qu'il pourrait nuire à la démarche d'ensemble pour un apport stratégique à relativiser. Il peut dès lors être raisonnable de renoncer à certains projets de développement ou de les reporter à des étapes ultérieures et dans un cadre partenarial (par exemple avec des partenaires européens) quand cette technologie n'est pas essentielle aux services de l'État les plus sensibles, aux opérateurs d'importance vitale (OIV), ou aux opérateurs de services essentiels (OSE) dans l'esprit de la directive *Network and Information Security* (NIS).

Afin d'assurer la souveraineté numérique française, il est indispensable de compléter l'offre française en matière d'infrastructures de base. Elle dispose déjà de certains atouts avec les entreprises de télécommunications, d'électronique grand public ou encore de composants électroniques. Ce socle doit être complété par une approche souveraine des data centers et du cloud. En 2021, la France accueillait 3,3 % des *data centers* mondiaux, contre par exemple 2,4 % pour les Pays-Bas, 4,7 % pour l'Allemagne, 5,6 % pour le Royaume-Uni, ou encore 38,6 % pour les États-Unis[18].

L'autre impératif est la sécurisation de certains approvisionnements. Il s'agit notamment des composants électroniques nécessaires aux équipements numériques, qui proviennent notamment de fournisseurs localisés en Asie. L'approvisionnement en données est aussi une priorité à retenir pour le développement de solutions. Il peut passer par un accès aux données tierces, notamment à l'échelle européenne, mais aussi par la participation à la constitution de bases de données de masse (par exemple dans une démarche d'open data). Celle-ci doit permettre aux acteurs non dominants du marché, notamment les entrants, qui ne bénéficient

(14) Prestation de Palantir à la DGSI pour le traitement de données hétérogènes de masse (l'offre nationale n'était pas encore arrivée à maturité mais les industriels français regrettent que le marché n'ait pas servi d'occasion de la faire aboutir) et achat de caméras piétons auprès de Motorola (selon la filière française, une offre nationale ou à tout le moins européenne était disponible).

(15) Bernard Benhamou, « *Souveraineté numérique : quelles stratégies pour la France et l'Europe ?* », Les cahiers français, mars-avril 2020.

(16) Livre blanc sur l'intelligence artificielle, Commission européenne, février 2020.

(17) Entretien accordé au journal Le Figaro, 1er juillet 2020.

(18) https://www.datacentermap.com

pas des effets d'échelle des grandes entreprises du numérique en matière d'accès aux données, de disposer de bases critiques pour développer des solutions. L'industrie française de sécurité pourrait bénéficier d'un meilleur accès à ces données. Cependant, l'ouverture doit être proportionnée à la sensibilité des données et ne peut dès lors faire l'objet d'une démarche d'ensemble indiscriminée.

L'assurance de la souveraineté numérique passe aussi par le développement de capacités nationales. Le chiffrement des données est par exemple, notamment dans les domaines sensibles comme la sécurité intérieure, une nécessité stratégique. L'investissement dans des domaines d'avenir, comme la *blockchain* ou l'informatique quantique, sont aussi des leviers d'une future souveraineté numérique sur des technologies sensibles.

Enfin, en matière de certification, les industriels français soulignent la dépendance européenne au *National Institute of Standards and Technology* (NIST) du ministère du commerce américain. C'est notamment le cas pour les algorithmes biométriques : le NIST est le seul organisme de certification reconnu internationalement. Sur les technologies dans leur ensemble, mais tout particulièrement dans les domaines sensibles, un effort de souveraineté normative doit être accompli afin de sécuriser l'innovation nationale et le développement des entreprises françaises à l'international.

3. Les entreprises françaises souhaitent la consolidation d'un environnement national et européen favorable à leur développement

Lors des auditions conduites et dans les contributions envoyées, les industriels français actifs dans les technologies de sécurité ont fait part de plusieurs difficultés entravant leur développement.

Le principal de ces obstacles relève d'un cadre juridique jugé trop contraignant ou instable pour sécuriser les programmes d'innovation. Les industriels redoutent notamment que la réglementation sur la protection des données contraigne trop les possibilités de les utiliser dans le développement des technologies. Ils s'interrogent par exemple sur l'équilibre à trouver dans le futur règlement de la Commission européenne sur l'intelligence artificielle. De trop grandes proscriptions sur les biais d'apprentissage et une protection excessive des bases d'apprentissage contraindraient, selon eux, leur capacité d'innovation. De même, le principe d'audit des algorithmes soulève des inquiétudes sur les secrets industriels.

Afin de pouvoir tester les innovations à l'échelle, les industriels français souhaitent un meilleur recours aux expérimentations en conditions réelles. Le besoin est tout particulièrement relevé en matière d'analyse d'image et de biométrie. L'apprentissage par intelligence artificielle est en effet dépendant de la qualité et de l'ampleur des bases de données offertes. Les industriels proposent de créer des standards concernant ces bases et de permettre des expérimentations algorithmiques afin de perfectionner les solutions développées (reconnaissance situationnelle, reconnaissance faciale).

Plusieurs industriels ont en outre appelé de leur vœu une évolution du cadre juridique de la vidéoprotection, afin d'y intégrer les technologies d'analyse automatisée (par ordinateur) des images.

Outre l'effort juridique à accomplir, les industriels français souhaitent un plus grand effort de soutien à l'investissement et à l'innovation. L'importance de l'économie numérique, notamment dans les domaines sensibles et les secteurs souverains, justifie la pleine mobilisation des leviers de la politique industrielle. L'investissement et la commande publics sont des leviers à mobiliser au maximum des capacités offertes, pour favoriser le développement d'une offre française.

Cette mobilisation peut passer par un partenariat public-privé plus étroit. Plusieurs propositions des entreprises françaises soulignent un besoin de renforcer les relations avec les autorités publiques. Cet effort peut se faire en prospective, dans l'identification des technologies essentielles et l'anticipation des domaines d'avenir. Dans le développement industriel, des partenariats renforcés, par exemple sous la forme d'incubation et d'un dialogue renforcé entre les FSI et les industriels, pourraient aussi avoir un effet-levier sur le développement de l'offre française.

Enfin, le secteur des industries de sécurité, amené à franchir un cap technologique dans les années à venir, doit faire l'objet d'une attention particulière de la politique d'investissement stratégique de l'État. L'actionnariat public peut en effet servir d'outil de souveraineté à long terme et être envisagé comme tel dès les phases d'accompagnement des entreprises innovantes.

Recommandation :

Favoriser le développement international des entreprises françaises en les encourageant à développer des solutions en *privacy-by-design* qui les distinguent de la concurrence.

Investir davantage dans les enjeux de normalisation et de certification à l'échelle internationale.

Compléter l'offre française en matière d'infrastructures de base et en sécurisant certains approvisionnements.

Faciliter le développement des technologies françaises en permettant aux entreprises de la filière de recourir à des expérimentations en situation réelle et en mobilisant l'investissement et la commande publics.

II. Améliorer l'aide à la décision et l'appui opérationnel des forces de sécurité et de secours grâce aux nouvelles technologies

Le champ des nouvelles technologies de sécurité est potentiellement très vaste. Les contributions des parties prenantes qui ont été consultées par la mission ont montré la diversité des technologies, des usages et des vecteurs. L'instabilité du champ, dans un contexte d'innovation rapide, caractérise aussi ce domaine.

Les forces de sécurité ont fait part de nombreux besoins, qu'il s'agisse des centres de commandement, de l'équipement de l'agent en mobilité, des outils de relation numérisée avec les usagers, de gestion de la donnée, de véhicules modernisés.

Face à l'ampleur des possibles et à l'impossible exhaustivité, la mission a recentré les besoins selon un triptyque : besoin des forces, enjeux pour les libertés, maturité de l'offre technique. Cette grille d'analyse a tenu compte des enjeux spécifiques aux grands événements sportifs que la France accueillera dans les années qui viennent, mais aussi des besoins plus structurels qui dépassent ces seules échéances.

La mission a aussi tenu compte des réflexions qui avaient déjà eu lieu dans d'autres cadres, afin de tenter d'identifier ce qui lui semblait prioritaire. Les grands enjeux qui sont apparus à la mission portent sur la question des données (Big data, personnelles, biométriques), de l'intelligence artificielle et de la mobilité opérationnelle.

Partant, les trois axes technologiques développés concernent les outils d'aide à la détection de situations de danger (dans les rassemblements, à l'entrée des sites exposés à des risques ou des menaces), les technologies reposant sur les données biométriques (notamment la reconnaissance faciale) et les équipements de mobilité (en particulier les drones).

Pour chacun de ces axes de besoin et chacune de ces technologies, les cas d'usages les plus essentiels au rendu d'un meilleur service de sécurité sont à prendre en compte, de même que le régime juridique sous-jacent.

A. Les technologies d'aide à l'identification de situations de danger

1. La détection de situations de danger pour les personnes par l'exploitation automatisée des données

Les nouvelles possibilités d'automatisation de l'analyse de données de natures différentes (texte, photo, vidéo, son, géopositionnement) ouvrent des capacités d'aide à l'identification de situations de danger. Le texte et l'image notamment peuvent apporter des informations opérationnelles utiles en temps réel pour les services de sécurité et de secours : les flux de communications ouverts entre des personnes peuvent renseigner sur une situation de danger à l'endroit où elles se trouvent. Il est envisageable de progresser dans l'exploitation de cette donnée disponible. L'ensemble des forces de sécurité reconnaît l'importance de développer une politique d'exploitation de la donnée opérationnelle pour les différentes missions de sécurité et de secours aux personnes.

Dans l'ensemble, ces techniques présentent plusieurs atouts pour les services de sécurité. Elles permettent de traiter plus massivement des données qui auraient pu échapper à une vigilance humaine des agents. Le traitement automatique aide les forces dans la prise de décision en émettant des signaux d'alertes sur certains événements, en allant parfois jusqu'à la leur caractérisation.

Elles peuvent apparaître comme porteuses de risques pour les libertés. Un usage non nécessaire et non proportionné peut en effet conduire à imposer une contrainte plus ou moins explicite sur la liberté d'expression, la liberté de circulation, l'anonymat dans l'espace public. Toutefois, un tel recueil et une telle exploitation de données ne reposent pas nécessairement sur l'intrusion dans la vie privée. Concrètement, il ne s'agit pas de connaître les situations individuelles, mais de savoir si un faisceau de communications publiques révèle une situation de risque localisée. Il s'agit davantage d'exploiter des extractions de données brutes ou situationnelles qui soient

anonymisées, afin d'alléger l'application de certaines règles relatives à la protection des données personnelles.

a) Permettre la détection de situations dangereuses et d'anomalies par l'analyse automatisée d'images

La multiplication des capteurs vidéo donne accès à des flux d'images en temps réel dans de multiples contextes. Il peut s'agir de la rue, des réseaux de transports, des grands établissements recevant du public (sport, culture). Les flux de personnes sont des situations de danger (bousculade sur un quai de métro) et les regroupements peuvent être la cible d'attaques à caractère terroriste.

Une analyse automatisée des images, dans ce cas, peut permettre de prendre des mesures de prévention : les modèles de simulation peuvent, par exemple, aider les gestionnaires de sites à apprécier la dynamique d'une foule dense et à détecter les facteurs de risque. Outre l'anticipation, la détection automatisée de situation permet de faire des remontées d'alerte dans un flux vidéo dense, afin de répondre à des situations d'urgence. La remontée d'un incident localisé peut ainsi alerter les forces de police et de secours en vue du déploiement des moyens humains. Plusieurs types de détection sont possibles : attroupements, circulation à contresens, courses/panique/vitesse, fumée dans une foule, présence d'une personne dans un lieu clos ou fermé.

Encadré : la vision par ordinateur

La vision par ordinateur est une branche de l'intelligence artificielle qui permet d'analyser, et de traiter les images prises par un système d'acquisition comme la vidéoprotection[19]. Elle est soumise aux règles relatives à la protection des données personnelles dès lors qu'elle implique la captation et l'utilisation de l'image de personnes qui se trouvent dans le champ des caméras[20]. La vision par ordinateur a, par exemple, été utilisée récemment pour détecter, dans les transports, le non-respect du port du masque sanitaire.

Les auditions conduites ont laissé entrevoir une incertitude sur le niveau normatif requis pour procéder à une expérimentation en situation réelle de l'analyse automatisée d'images à des fins de détection de situations dangereuses et d'anomalies dans les établissements accueillant du public.

Premièrement, il serait possible d'utiliser la détection automatisée en direct d'anomalies dans les établissements accueillant du public, après avoir réalisé une analyse d'impact relative à la protection des données et sous réserve d'un certain nombre de garanties. L'installation d'un système de vidéoprotection est soumise à une autorisation préfectorale sur le fondement de l'article L252-1 du CSI. Par ailleurs, l'article 35-3 c) du RGPD prévoit que les traitements qui engendrent une « *surveillance systématique à grande échelle d'une zone accessible au public* » sont soumis à une AIPD. Deux expérimentations ont déjà été réalisées par le SGDSN : la première en 2016 et la seconde en 2020[21].

Deuxièmement, il serait possible d'autoriser l'utilisation d'algorithmes de vision par ordinateur sur les images collectées aux fins de vidéoprotection dès lors que ces algorithmes anonymisent en temps réel les images et ne conservent aucune donnée permettant d'identifier directement ou indirectement une personne. Par exemple, un décret du 10 mars 2021 autorise le recours à la vidéo intelligente, afin de mesurer le taux de port du masque dans les transports, dans la mesure où les algorithmes anonymisent en temps réel les images et ne conservent pas de données à caractère personnel[22]. Il limite les droits d'accès, de rectification et d'opposition prévus par le RGPD sur la base de son article 23 qui prévoit que

(19) Source : DIJOP.
(20) Source : Datakalab.
(21) Source : SGDSN.
(22) Décret n°2021-269 du 10 mars 2021, relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports.

la législation nationale peut limiter la portée de certaines obligations et droits « *lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir la sécurité publique* »[23].

Il serait possible, dans le cadre des grands évènements, de recourir à droit constant à l'analyse automatisée d'images à des fins de détection automatisée d'anomalies en direct dans les établissements accueillant du public. La vision par ordinateur peut être utilisée dès lors que les algorithmes anonymisent en temps réel les images et ne conservent aucune donnée permettant d'identifier directement ou indirectement une personne. Un décret peut être pris sur la base de l'article 23 du RGPD, pour limiter les droits d'accès, de rectification et d'opposition.

Néanmoins, la CNIL considère pour le moment que les expérimentations en la matière ne peuvent pas se faire à droit constant. Elle estime que le principe même d'utilisation des algorithmes d'analyses d'images pour des finalités de prévention de l'ordre public par les forces de police nécessite une autorisation et un encadrement législatifs. En effet, ces dispositifs constituent un moyen de surveillance automatisé, en vue d'une intervention immédiate ou de l'enclenchement de procédures, administratives ou judiciaires, par les services de police. Ils modifient par principe la façon dont l'action des services de police influe sur l'exercice par les citoyens de leurs droits et libertés. Même limités à la protection de certains événements, de tels dispositifs pourraient se trouver régulièrement utilisés, ce qui semble nécessiter un encadrement législatif. De la même façon que l'usage, même temporaire, de drones pour des finalités de police administrative requérait, selon l'analyse du Conseil d'État, une intervention législative, il semble que l'utilisation de tels algorithmes ne pourrait être licite que si elle était prévue par la loi.

La CNIL précise qu'une demande d'avis au Conseil d'État sur ce point permettrait de clarifier le niveau de norme requis.

Si le Conseil d'État considère que les expérimentations en la matière ne peuvent pas se faire à droit constant, il sera nécessaire de prévoir des dispositions législatives afin de s'assurer de l'existence d'un cadre d'expérimentation et d'emploi à court terme, dans la perspective des jeux olympiques.

Recommandation :

Expertiser rapidement le niveau normatif nécessaire à l'expérimentation de la détection automatisée en direct d'anomalies dans les établissements accueillant du public en saisissant si nécessaire le Conseil d'État pour avis[24].

b) Renforcer l'exploitation opérationnelle de données à des fins d'identification de situations à risque

i. Les données textuelles

Les utilisateurs d'Internet produisent d'importantes données textuelles sur les réseaux sociaux, forums, espaces de commentaires de sites de presse… L'exploitation humaine dépasse les capacités cognitives, tandis que des outils d'IA permettent de les prendre en charge automatiquement.

Leur exploitation en temps réel permettrait de détecter des situations et événements associables à un danger : une remontée groupée de termes associés à une localisation peut constituer un signal pour les services de sécurité et de secours. Il peut s'agir d'un accident de la route, d'un incendie ou feu de forêt, d'une attaque de type terroriste. Les services de gestion de crise signalent que l'automatisation permettrait de mieux exploiter la donnée disponible, y compris en utilisant celle qui est habituellement moins prise en compte. D'un

(23) Article 23 du RGPD.

(24) Si un doute subsiste sur le niveau normatif requis, alors il est possible d'agir par voie législative. Le domaine législatif et le domaine règlementaire sont distincts. Mais, en pratique, les interventions de la loi dans le domaine réglementaire sont récurrentes. Selon une jurisprudence désormais constante, les incursions de la loi dans le domaine du règlement ne sont pas censurées par le Conseil constitutionnel (DC 1982 Blocage des prix et revenus : « *La Constitution n'a pas entendu frapper d'inconstitutionnalité une disposition de nature réglementaire dans la loi* »).

point de vue opérationnel, cette technique permet de capitaliser sur la donnée existante au plus proche des événements, de mesurer le degré d'urgence et de pouvoir répondre (envoi de moyens, communication) rapidement aux questions qui émergent des situations.

L'analyse automatisée des données textuelles de masse peut aussi aider à identifier le développement de *fake news*, qu'elles soient intentionnelles ou du fait de la simple rumeur qui émergerait d'une situation de panique. Les services publics seraient alors en mesure de proposer une communication juste afin d'alerter la population.

ii. Les autres données utiles

Les données textuelles constituent une matière importante laissant envisager un meilleur usage pour apporter une meilleure offre de sécurité et assurer le secours des personnes. Elles ne sont toutefois pas exclusives d'autres données.

Les images photo ou vidéo sont aussi des données utiles à des fins d'alerte, de détection de situation de danger. Y sont en outre associées des métadonnées non couvertes à ce stade par le cadre juridique(25).

Les données de géolocalisation sont également à prendre en compte. Leur partage et leur exploitation peuvent en effet renseigner de façon encore plus précise sur des événements : nombre de personnes, points névralgiques, déplacements des personnes. Dans un sens service-usagers, la société Facebook a lancé en 2011 un contrôle d'absence de danger (« *safety check* ») permettant aux usagers, géolocalisés dans une zone concernée par une catastrophe, de signaler leur situation.

La captation de sons peut aussi aider à identifier et caractériser des situations de risque : chocs, explosion, cris. Aujourd'hui, les opérateurs vidéo peuvent voir les scènes mais n'ont pas la capacité d'entendre. Cette restriction s'explique par des raisons techniques (les systèmes, notamment les plus anciens, n'étaient pas adaptés) mais aussi et surtout pour ne pas prendre un risque excessif pour les libertés. La captation de sons dans l'espace public fait courir le risque d'enregistrements extrêmement intrusifs, notamment des conversations entre les personnes. C'est une éventualité à exclure impérativement. Néanmoins, certaines « signatures sonores » peuvent être très caractéristiques et reconnues par un capteur de son sans enregistrement des autres bruits de l'entourage. Par exemple, un capteur pourrait n'être activé qu'à l'occurrence d'un son particulier (comme une alarme par un déclencheur de mouvement) qui aurait été associé à un risque (explosion, clameur forte et soudaine). Certaines collectivités ont montré un intérêt récent pour ces techniques, mais la CNIL s'est opposée à leur utilisation en l'absence d'une législation adaptée. En 2019, la ville de Saint-Étienne a envisagé de poser des dispositifs expérimentaux de captation et d'analyse de sons de la voie publique. La collectivité a dû y renoncer, faute de base légale suffisante. En effet, « *La CNIL [avait] estimé que l'atteinte susceptible d'être portée à la vie privée en raison de l'enregistrement constant et indifférencié sur la voie publique des voix et conversations privées, et notamment de données sensibles (opinions politiques, données concernant la santé, etc.), qui constituent des données à caractère personnel, nécessitait un encadrement juridique spécifique.* »(26) Les industriels relèvent aussi ce défaut de base légale(27).

iii. Vers un traitement des données hétérogènes de masse ?

L'analyse croisée des données peut fournir des éléments enrichis sur une situation de danger aux services en charge de la sécurité et des secours. De même, si une seule donnée, par exemple textuelle, peut ne pas être suffisamment significative, le croisement de plusieurs données hétérogènes, caractérisant un danger pour une localisation unique, peut constituer un motif d'alerte.

Les traitements de données hétérogènes de masse, lorsqu'ils recouvrent des données personnelles et sont utilisés pour des finalités qui représentent un risque particulier pour les droits et libertés des personnes physiques, sont soumis à des obligations spécifiques.

(25) Source : AN2V.
(26) Les polices municipales, Cour des comptes, octobre 2020.
(27) Source : AN2V.

D'une part, les traitements de données hétérogènes de masse sont soumis à la législation en vigueur au niveau national et européen en matière de protection des données personnelles.

Au niveau national, la loi « informatique et libertés » impose, dans son article 62, la réalisation d'une analyse d'impact relative à la protection des données (AIPD) pour les traitements de données à caractère personnel qui engendrent un risque élevé pour les droits et les libertés des personnes physiques, en application du RGPD[28].

Au niveau européen, le RGPD s'applique aux traitements de données personnelles sur le territoire des États-membres. La directive « police-justice »[29] concerne les traitements de données personnelles réalisés à des fins de prévention et de détection des infractions pénales. L'un et l'autre imposent de réaliser une AIPD, en cas de risque élevé pour les droits et les libertés des personnes physiques[30].

Encadré : les analyses d'impact relatives à la protection des données

Selon le RGPD, les AIPD sont obligatoires, lorsque le traitement présente un risque élevé pour les droits et libertés. Elles sont requises, en particulier, en cas de traitements à grande échelle de catégories particulières de données et en cas de surveillance systématique à grande échelle d'une zone accessible au public[31].

Le Comité européen à la protection des données (CEPD) a adopté des lignes directrices pour préciser le rôle et le contenu des AIPD[32]. Elles permettent de décrire le traitement, d'en évaluer la nécessité et la proportionnalité ainsi que d'anticiper les risques pour les droits et libertés. L'analyse d'impact intervient avant le début du traitement.

D'autre part, les traitements de données de masse sont soumis à des obligations supplémentaires, lorsqu'ils mobilisent des techniques d'intelligence artificielle.

Les traitements de données hétérogènes de masse qui sont associés à l'intelligence artificielle sont soumis à un cadre juridique particulier, lorsqu'ils poursuivent des finalités qui peuvent porter atteinte aux droits fondamentaux. Les techniques d'intelligence artificielle seront bientôt soumises à un encadrement spécifique. En effet, la Commission européenne a présenté en avril 2021 sa proposition de règlement visant à harmoniser les règles sur l'intelligence artificielle.

Mutatis mutandis, il est possible de regarder ce que la direction générale des finances publiques expérimente à des fins de contrôle, via les informations rendues disponibles sur les réseaux sociaux par les usagers : « *A titre expérimental et pour une durée de trois ans, pour les besoins de la recherche des manquements et infractions (…), l'administration fiscale et l'administration des douanes et droits indirects peuvent, chacune pour ce qui la concerne, collecter et exploiter au moyen de traitements informatisés et automatisés n'utilisant aucun système de reconnaissance faciale les contenus, librement accessibles sur les sites internet des opérateurs de plateforme en ligne (…), manifestement rendus publics par leurs utilisateurs.* »[33]. Ces dispositions sont assorties des garanties nécessaires au respect des droits individuels.

L'usage en matière de sécurité ne devrait pas avoir pour finalité le contrôle, mais bien l'aide à la détection de situations de danger pour les personnes.

(28) La loi ILF a été modifiée par la loi du 20 juin 2018 relative à la protection des données personnelles, par l'ordonnance n° 2018-1125 du 12 décembre 2018 et par la loi n° 2019-828 du 6 août 2019 de transformation de la fonction publique.

(29) Directive 2016/680 du Parlement européen et du Conseil du 26 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

(30) Article 35 (1) du RGPD et article 27 de la directive police-justice.

(31) Article 35 (1) et (7) du RGPD.

(32) Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 : https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

(33) Article 154 de la loi n°2019-1479 du 28 décembre 2019 de finances pour 2020.

iv. Quel traitement automatisé du Big Data au-delà de l'alerte sur les situations dangereuses ?

Si leur développement est poussé, les technologies de traitement de données massives permettent de modéliser certains phénomènes dans une **logique prédictive**. Ces schémas donnent aux forces la possibilité d'ajuster leurs dispositifs opérationnels selon les variations prévisibles ou de détecter des signes précurseurs d'un phénomène inhabituel afin de monter rapidement en capacité. Les forces de sécurité ont signalé leur intérêt pour de tels outils, qui ont déjà fait l'objet de modélisations (ex : projet NEXSIS en matière de secours par la sécurité civile). Le big data peut aussi servir d'outil d'analyse décisionnelle dans la planification des dispositifs de sécurité et de secours. L'analyse croisée de données nourrit aussi **le retour à postériori sur les opérations déjà conduites** (débriefing, évaluation). Il est même envisageable de réaliser des exploitations de données internes (données opérationnelles) et externes (source ouverte, données des partenaires) afin d'enrichir les analyses.

Recommandation :

Dans l'immédiat, ouvrir par voie législative un cadre d'usage expérimental de la captation automatique de données librement accessibles dans des sources ouvertes dans le but d'améliorer la détection précoce de situations de danger dans les domaines de la sécurité et du secours.

Concentrer les efforts sur les données textuelles avant d'envisager d'autres sources d'information et l'exploitation croisée des données.

Les finalités devraient se limiter à l'alerte et la détection de situations d'urgence et de danger.

Plus structurellement, ouvrir une réflexion au ministère de l'Intérieur, en vue de la consolidation d'une politique de la donnée (recueil, classification et exploitation de données à des fins d'alerte, d'analyse décisionnelle).

v. Quel cadre pour les données de recherche ?

Les services soulignent que les règles relatives aux traitements de données personnelles sont contraignantes pour les travaux de recherche et développement(34). Le député Eric Bothorel, dans son rapport sur la politique publique de la donnée, recommande de permettre à titre dérogatoire la réutilisation de données pour des finalités différentes de celles pour lesquelles elles ont été collectées, afin de constituer des jeux d'apprentissage en matière d'intelligence artificielle :

« Le pouvoir de dérogation devrait revenir à la CNIL en tant que garante de la protection desdites données, et lui permettre de déroger aux textes régissant les traitements source du jeu d'apprentissage, que ces textes aient été pris sur le fondement de la loi informatique et libertés ou sur le fondement d'autres textes sectoriels. La création de ce bac à sable au bénéfice de la CNIL implique une modification de la loi informatique et libertés. Une modalité de mise en œuvre serait de confier à la CNIL l'autorisation de la réutilisation des données à des fins d'apprentissage et, le cas échéant, leur conservation pour une durée supérieure à la durée prévue dans le traitement initial »(35).

La Commission européenne, quant à elle, propose dans son projet de règlement sur l'intelligence artificielle la création de « *bacs à sable réglementaires* » pour favoriser l'innovation dans le domaine de l'intelligence artificielle, en créant un environnement contrôlé d'expérimentation(36).

(34) Source : DGGN.
(35) Pour une politique publique de la donnée, des algorithmes et des codes sources, rapport de la mission du député Éric Bothorel, décembre 2020.
(36) Article 53 de la proposition de règlement 2021/0106 du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle.

Recommandation :

Favoriser les expérimentations dans le domaine de l'intelligence artificielle à partir de jeux de données réelles ré-employables. À titre dérogatoire, les données collectées pour une finalité première pourraient être réutilisées et conservées sur une durée plus longue en vue de la constitution de jeux d'apprentissage d'I.A. L'ouverture d'une telle possibilité implique de modifier la loi « informatique et libertés ».

2. La détection d'anomalies lors des contrôles d'accès à des sites regroupant du public

La détection précoce de situations de risque peut aussi se faire au moment des contrôles d'accès des personnes à certaines enceintes. Il s'agit de vérifier qu'aucun objet dangereux (armes, explosifs) n'y est introduit dans le cadre d'un rassemblement. Les techniques employées actuellement sont principalement les portiques de détection (notamment magnétiques pour les objets métalliques et rayons X pour la vérification des bagages) et/ou les palpations.

Les scanners corporels à ondes millimétriques, qui permettent d'obtenir des images « corps entier » des personnes, se sont développés plus récemment. Ils peuvent présenter des avantages en matière de fiabilité, car ils permettent d'identifier des objets dissimulés qui auraient pu échapper à d'autres moyens de contrôle. En outre, ils sont jugés moins intrusifs que les palpations, dès lors que les techniques actuelles permettent de ne pas restituer une image précise de la morphologie des personnes mais de transmettre des données schématiques pour localiser les éléments étrangers. Les principes de respect de la vie privée et de l'intimité des personnes doivent en effet être garantis.

Si le degré de précision de ces scanners peut intéresser les acteurs de la sécurité, ils présentent des inconvénients. Ce sont tout d'abord des dispositifs coûteux, surtout s'ils ont vocation à aider à contrôler les accès de sites à multiples entrées. En outre, le gain de temps qu'ils permettent dans le cadre d'un contrôle d'accès massif, comme pour un grand stade, est à expertiser précisément.

La question de l'usage courant des scanners corporels s'est posée pour les aéroports au tournant de l'année 2009-2010. La tentative d'attentat à l'explosif sur un vol Amsterdam – Détroit en 2009[37] a entraîné un mouvement de renforcement des contrôles d'accès des passagers. Plusieurs pays (Pays-Bas, Royaume-Uni, Canada) ont alors ouvert des programmes de test et de mise en service des scanners corporels dans les aéroports avec différentes garanties (droit d'option, respect de l'intimité).

Encadré : les expérimentations aéroportuaires en France

L'utilisation des scanners corporels n'est pas permise en France. Seules des expérimentations dans des aéroports ont eu lieu : Paris-Charles-de-Gaulle en 2010 et 2012, Nice en 2012. L'expérimentation de 2010, qui se limitait à des personnes volontaires, a permis au service technique de la direction générale de l'aviation civile, à la sécurité civile, à la police aux frontières et à Aéroports de Paris d'évaluer les aspects opérationnels (coût, impact sur la fluidité des flux de passagers, besoin en personnels, etc.) et la qualité de détection de ces appareils.

À l'issue, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure a ouvert un cadre d'expérimentation de 3 ans assorti de garanties. Le code de transports prévoit la possibilité d'expérimenter l'utilisation de dispositifs d'imagerie utilisant des ondes millimétriques durant une période de trois années. Les dispositions apportent des garanties à la prévention d'atteintes aux libertés individuelles en prévoyant que seules les personnes volontaires seront contrôlées par le biais d'un détecteur corporel avec possibilité de recourir à un autre dispositif de contrôle. L'analyse des images doit être conduite par des opérateurs ne connaissant pas l'identité de la personne et ne pouvant visualiser simultanément celle-ci et l'image produite par le détecteur corporel. Afin de garantir l'intimité de la vie privée de la personne contrôlée, l'image produite doit comporter un système brouillant l'image du visage. Enfin, l'enregistrement et la conservation des images sont interdits.

(37) Vol Amsterdam – Détroit de la NorthWest Airlines du 25 décembre 2009.

Dans l'optique des grands événements de 2023 et 2024, il serait utile de pouvoir tester la pertinence des scanners corporels en dehors du cadre aéroportuaire, et notamment sur des sites sportifs. La logique de flux peut en effet différer selon les contextes : les stades font face à une entrée concentrée et massive sur une courte durée quand d'autres sites connaissent un flux plus lissé.

À cette fin, il conviendrait de prévoir un texte législatif autorisant une utilisation limitée dans le temps à des fins expérimentales (validation du besoin et des possibilités techniques). Sous réserve de cette phase de test en conditions réelles et d'autres garanties (consentement et garanties comparables à celles prévues au code des transports[38]), un usage pérenne pourrait être envisagé.

Recommandation :

Prévoir des dispositions législatives autorisant au plus tard en 2022 un déploiement expérimental pluriannuel de dispositifs d'imagerie utilisant des ondes millimétriques (« scanners corporels ») pour l'accès aux enceintes sportives accueillant des grands événements. Ces dispositions préciseraient les garanties d'utilisation des scanners corporels, en reprenant *mutatis mutandis* celles figurant dans le code des transports pour les enceintes aéroportuaires.

B. Les technologies d'aide au suivi des personnes representant une menace pour la securité

1. Retour sur la biométrie

La biométrie est une technique de relevé et de mesure d'éléments de la personne humaine suffisamment uniques et permanents pour présenter un bon degré de fiabilité dans la reconnaissance d'un individu. En effet, elle part de caractéristiques physiques telles que les empreintes papillaires (digitales et palmaires), l'ADN, le visage, ou encore l'iris de l'œil. Les dernières recherches scientifiques tendent vers l'exploration d'autres caractéristiques biométriques telles que la voix, la démarche ou l'odeur corporelle.

En matière de biométrie, la reconnaissance de l'individu se fait par identification ou par authentification. La distinction entre les deux notions, importante pour le débat public, doit être clairement établie. **L'authentification** consiste à confronter des données biométriques enregistrées à celles présentées par un individu lors d'un contrôle (logique : 1 contre 1). **L'identification** consiste à repérer un individu dans un espace et une population donnée à partir de ce qui est déjà connu de lui biométriquement (logique : 1 contre N).

Toutefois, à ce stade, les biométries ne présentent pas toutes les mêmes possibilités, limites et contraintes d'utilisation. Le profil génétique individuel (ADN) et l'empreinte papillaire sont les plus précis, mais ils ne sont exploitables qu'avec le consentement de la personne et par un contact physique direct ou de forte proximité (le relevé et la prise d'empreintes). A l'inverse, le visage, par exemple, peut être recueilli à distance et sans le consentement des personnes, mais la qualité de la captation est beaucoup plus aléatoire et la comparaison *in fine* moins fiable en l'état des techniques.

Compte tenu de leur sensibilité particulière, les données biométriques ont un statut rigoureusement encadré par le droit. La sensibilité provient du très haut degré de correspondance entre les données biométriques (« traces ») et les personnes qui fait peser des risques, en termes de protection de la vie privée. En effet, ces données sont uniques et irrévocables ; elles appartiennent au patrimoine biologique de la personne et ne sont pas une construction sociale. Dès lors, elles sont classées dans la catégorie des données sensibles au sens du RGPD et de la loi « informatique et libertés ».

(38) Article L. 6342-4 du code des transports.

Encadré : le cadre juridique des données biométriques

L'usage de la biométrie à des fins d'authentification et d'identification est soumis à un cadre juridique strict au niveau européen et au niveau national.

Le traitement des données biométriques est encadré par le RGPD. Il interdit le traitement des données biométriques aux fins d'identifier une personne physique de manière unique, dans la mesure où ces données sont considérées comme sensibles(39). Certaines exemptions sont néanmoins prévues quand la personne concernée a consenti au traitement de ses données, lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée, ainsi que pour des motifs d'intérêt public(40). Par ailleurs, le RGPD impose la réalisation d'une analyse d'impact relative à la protection des données, lorsque le traitement poursuit une finalité qui représente un risque élevé pour les droits et libertés des personnes physiques(41).

Deuxièmement, le traitement des données biométriques est encadré par la directive police-justice. Elle autorise le traitement des données biométriques aux fins d'identifier une personne physique de manière unique seulement en cas de nécessité absolue et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée. Le traitement ne peut être autorisé que dans trois cas : lorsqu'il est autorisé par le droit de l'Union ou le droit d'un État membre, pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique et lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée(42).

La loi « informatique et libertés » reprend ces dispositions en précisant que des traitements régaliens peuvent être mis en place « en cas de nécessité absolue », sous réserve de l'adoption d'un décret ou d'une loi (43).

Dans le domaine de la sécurité, la biométrie peut être utilisée en criminalistique (enquête sur des infractions, identification d'un corps), dans le contrôle d'identités (procédure de délivrance de titres, détection de cas d'usurpation), ou encore dans le contrôle d'accès à des sites sensibles (par exemple les opérateurs d'importance vitale). La biométrie est un outil d'aide aux forces de sécurité intérieure dans leurs missions d'enquête, de surveillance et de contrôle, qui les confrontent fréquemment à la nécessité de reconnaître l'identité de personnes. C'est aussi un élément essentiel de prévention de la fraude à l'identité. Sous ses formes classiques (relevé d'empreintes digitales, d'ADN), elle s'est imposée comme un outil indispensable à la recherche des auteurs d'infractions et à la matérialisation de la preuve. Elle vient également conforter l'identité des personnes détentrices d'un titre d'identité ou de voyage, de manière à lutter contre l'usurpation d'identité.

Les services de police français sont limités à la signalisation biométrique de personnes ayant commis des actes délictueux ou criminels graves, ou à collecter des données biométriques pour l'identification des cadavres inconnus. Le recueil sans conservation peut également être fait sur des personnes s'étant trouvées sur une scène d'infraction afin d'exclure leurs traces dans la recherche d'individus impliqués. Dans le respect des personnes et des droits, afin de limiter les risques liés à l'usage de ces données sensibles, le système juridique français empêche d'interconnecter les bases de données biométriques collectées dans l'exercice des missions de sécurité intérieure et les différents fichiers (état-civil, titres d'identité ou de voyage).

2. La reconnaissance faciale

Les développements scientifiques et technologiques récents reposent la question de l'utilisation des données biométriques, notamment sous leurs formes les plus nouvelles, dans des missions de sécurité.

Si toutes les nouvelles biométries ne présentent pas un degré de maturité suffisant, la biométrie du visage, autrement appelée « reconnaissance faciale », a atteint un niveau de développement qui permet d'envisager une utilisation accrue. Si la reconnaissance faciale est possible de manière non automatisée (ex : recours aux physionomistes), les progrès techniques permettent

(39) Article 9 al. 1 du RGPD.
(40) Article 9 al. 2 du RGPD.
(41) Article 35 al. 1 du RGPD.
(42) Article 10 de la directive police-justice.
(43) Article 88 de la loi « informatique et libertés ».

maintenant, de façon automatisée, de collecter des données faciales, de les stocker et de les comparer avec un niveau de fiabilité intéressant.

Deux grands usages de la reconnaissance faciale sont possibles.

Elle peut tout d'abord être utilisée ***a posteriori*** pour la recherche d'un visage dans une banque de données stockées au préalable, dans le cadre d'une enquête par exemple.

L'autre usage possible est ***en temps réel*** : la personne est recherchée dans un flux *live* de vidéos. Cette reconnaissance faciale automatisée dans l'espace public peut prendre plusieurs formes. Il est d'abord, dans une forme restrictive, possible de rechercher dans un espace donné une personne prédéfinie. Dans une approche plus large, il est techniquement possible de localiser dans un espace et une foule définis les personnes recherchées pour des crimes ou délits ; le scan général des personnes présentes établit alors les concordances possibles avec les fichiers. Dans les deux cas, il n'est pas nécessaire d'identifier les personnes qui n'offrent pas de correspondance avec la base de recherche.

Bien qu'encore récente, la reconnaissance faciale est **une technologie qui tend à se répandre dans des usages quotidiens**. En France et dans de nombreux autres pays, la reconnaissance faciale est utilisée dans la sphère privée, comme pour le déverrouillage d'un téléphone portable ou l'accès à des sites privés (d'entreprise, par exemple). Il s'agit alors principalement d'authentification (l'identité de la personne est enregistrée préalablement dans un fichier ou dans une carte à puce afin de la reconnaître lors de son passage) sur la base du consentement de la personne concernée (l'enrôlement est consenti au préalable par la personne, voire se fait à son initiative). D'autres usages quotidiens en sont faits : à l'été 2020, les États-Unis ont connu une expérimentation de paiement par reconnaissance faciale(44).

D'une manière générale, la perception de cette technologie semble se banaliser dans une frange de la population française. Ainsi, un sondage de 2021, réalisé auprès d'un millier de Français, a relevé que 62 % des personnes interrogées approuvaient le recours à cette technologie pour l'expérience utilisateur, et 58 % à des fins d'authentification(45). Si son acceptation semble éminemment culturelle et générationnelle, la jeunesse ne l'adopte pas de façon indiscriminée : elle **la plébiscite pour les usages courants mais peut s'en méfier quand elle est utilisée à des fins de surveillance**(46).

Les répondants au sondage associent davantage la reconnaissance faciale à de la surveillance (51 %) qu'à de la sécurité (41 %)(47). Si la surveillance est un sous-ensemble nécessaire de la sécurité, elle est connotée négativement. De surcroît, la technologie est généralement associée à la surveillance de masse. C'est en effet une possibilité technique et un risque éthique, si l'usage qui en est fait n'est pas restreint aux principes de nécessité et de proportionnalité d'un État de droit entérinés par la législations européenne et nationale. Mais cette technologie peut aussi se limiter à des cas spécifiques. Il peut s'agir de la recherche d'une personne jugée dangereuse dans une zone où elle aurait été repérée, à des fins de prévention ou de poursuite. Elle peut dans d'autres cas contribuer à rechercher une personne disparue en danger. Compte tenu des technologies développées, de telles recherches pourraient aussi se faire par analyse automatisée de l'image sans reconnaissance faciale : si, par exemple, les vêtements portés par la personne recherchée sont connus, ils peuvent servir de base de requête. Cependant, le visage est une donnée plus fiable qui permet de sécuriser l'identification de la personne, quand les autres caractéristiques comme les vêtements portés à un instant sont instables et non pérennes. Face à des usages par les services de police qui peuvent s'apparenter à de la surveillance dans l'espace public, les pays occidentaux insistent sur la préservation des droits fondamentaux des personnes et en réservent donc l'usage à des hypothèses où d'importants intérêts publics sont en jeu (ex : lutte contre le terrorisme).

En France, en matière de sécurité intérieure, la reconnaissance faciale est possible à des fins judiciaires strictement encadrées. Le rapprochement en identification est ainsi permis dans le cadre du traitement des antécédents judiciaires (TAJ)(48) : une captation de visage peut être confrontée au fichier TAJ pour identifier éventuellement une personne qui y serait inscrite. Cet

(44) https://www.latimes.com/business/technology/story/2020-08-14/facial-recognition-payment-technology
(45) Sondage Odoxa de mai 2021 consulté par la mission.
(46) https://www.estrepublicain.fr/education/2020/11/30/reconnaissance-faciale-les-jeunes-francais-la-voient-d-un-mauvais-oeil
(47) Sondage Odoxa de mai 2021.
(48) Article R. 40-26 du code de procédure pénale.

usage est particulièrement restrictif. Il n'est actuellement pas possible d'utiliser la reconnaissance faciale dans d'autres cadres, soit dans d'autres fichiers pour lesquels cette utilisation n'est pas prévue par les textes (ex : le fichier des personnes recherchées), soit qu'il s'agisse d'en faire usage dans l'espace public en temps réel. La reconnaissance faciale en enquête *a posteriori* est aussi utilisée ailleurs en Europe. C'est, par exemple, un logiciel de reconnaissance faciale appliqué aux captations des caméras de vidéoprotection qui a permis d'identifier l'un des acteurs des attentats de l'aéroport de Zaventen en Belgique le 22 mars 2016.

L'emploi de la reconnaissance faciale (en temps réel ou *a posteriori*) devrait principalement aider à améliorer l'élucidation de faits constatés avec constitution d'éléments de preuve. Opérationnellement, elle permettrait des gains de temps-homme, une montée en capacité de traitement et davantage de précision. L'analyse automatisée des images en temps réel permet de recentrer les ressources humaines sur des missions de terrain. Elle peut aussi optimiser le visionnage des caméras de vidéoprotection dans la mesure où un opérateur est sujet à des baisses de concentration et d'attention. L'analyse automatisée *a posteriori* (tout comme en direct) rend possible un traitement d'images en grande quantité qui aurait été difficile ou impossible pour des opérateurs. Les gains opérationnels peuvent être considérables : une expérimentation conduite au Royaume-Uni a évalué que pour un même jeu de vidéos visionné *a posteriori*, il fallait environ dix jours de traitement humain contre une dizaine de minutes pour un logiciel. Enfin, les outils de requêtage permettent de lancer des recherches précises dans des flux ou des stocks de données-images volumineux.

3. Les usages de la reconnaissance faciale en matière d'authentification

La reconnaissance faciale peut renforcer les dispositifs d'authentification aux points d'accès à des sites sensibles. Elle fiabilise le processus de contrôle qui repose aujourd'hui essentiellement sur des cartes dont l'utilisation peut être usurpée.

La CNIL a eu récemment l'occasion d'admettre des expérimentations qui poursuivaient certaines finalités, comme le contrôle aux frontières dans les aéroports, et d'en interdire d'autres, par exemple, le contrôle de l'accès des élèves dans les établissements scolaires[49].

Encadré : l'authentification biométrique au sein des aéroports

Le Groupe Aéroports de Paris (ADP) mène actuellement une expérimentation d'authentification biométrique afin de fluidifier les flux de passagers à l'embarquement. Le recours à l'authentification biométrique a permis d'optimiser la qualité des contrôles et d'améliorer l'expérience usagers, tout en respectant les règles relatives à la protection des données, notamment le consentement des passagers et la durée de conservation des données. L'expérimentation a été réalisée sur douze vols internationaux et au sein de l'espace Schengen et présente un taux de succès de 98.7%[50]. Néanmoins, cette expérimentation repose sur une base biométrique centralisée sur laquelle la CNIL a émis un certain nombre de réserves[51].

Les grands événements sportifs de 2023-2024 présenteront des enjeux importants dans ce domaine. Sur les seuls jeux olympiques et paralympiques, près de 400 000 accréditations seront délivrées (100 000 l'avaient été pour l'Euro 2016 de football), dont 65 000 pour la famille olympique et 19 000 pour la famille paralympique. L'authentification « forte » des détenteurs d'accréditations de la famille olympique –athlètes, délégations sportives, officiels techniques, dignitaires… - par reconnaissance faciale « coopérative », avec le consentement des personnes pourrait être envisagée. Elle pourrait se concentrer sur les points d'accès des sites d'hébergement (village olympique) et de compétition. Le but recherché est la lutte contre les risques d'intrusions par usurpation d'identité ou de badges dans des enceintes réunissant un public sensible. Ces authentifications pourraient se faire sur le modèle du dispositif de contrôle aux frontières PARAFE, sans stockage centralisé de données à caractère personnel. Le cadre

(49) Reconnaissance faciale : pour un débat à la hauteur des enjeux, CNIL, novembre 2019.
(50) Ce point a été soulevé lors de la présentation de l'expérimentation d'authentification biométrique dans les locaux d'ADP lors de la visite du site.
(51) Ibidem.

juridique actuel le permet, en circonstanciant bien la finalité et à la suite d'une AIPD par le responsable de traitement.

D'autres usages pourraient faire l'objet d'expérimentations ciblées. Tout d'abord, une authentification forte pourrait être mise en place pour les détenteurs de droits d'accès, comme les billets ou les accréditations, afin de leur permettre d'accéder aux sites privés. Cette expérimentation peut se faire à droit constant sur le modèle de l'expérimentation réalisée à Roland-Garros, sous réserve d'une AIPD[52]. Ensuite, une authentification forte pourrait être mise en place pour les détenteurs de droits d'accès, afin de leur permettre d'accéder aux sites publics[53]. Cette expérimentation nécessite de prendre un décret en Conseil d'État et de définir les finalités du traitement.

Recommandation :

Envisager le déploiement de dispositifs d'authentification forte par reconnaissance faciale des accrédités de la famille olympique et paralympique aux points d'accès du village olympique et des sites de compétition afin de renforcer la prévention d'intrusions. Dans le respect des préconisations de la CNIL, aucune base biométrique centralisée ne serait constituée.

4. Faut-il prévoir un cadre d'usage expérimental de la reconnaissance faciale en temps réel dans l'espace public à des fins d'identification ?

a) L'usage expérimental : les possibles et les souhaitables

Plusieurs pays européens ont testé, pour leurs polices, la reconnaissance faciale en temps réel dans l'espace public afin d'en vérifier la pertinence et de s'assurer d'une maîtrise technique, opérationnelle et juridique.

En France, la ville de Nice a expérimenté la reconnaissance faciale en authentification et identification à la volée durant le carnaval de 2019, mais sur une base volontaire.

La police du Pays de Galles du Sud (*South Wales Police - SWP*) a testé la reconnaissance faciale en temps réel lors de grands événements, notamment sportifs et culturels, entre 2017 et 2020. Elle déclare avoir arrêté 61 personnes grâce à cette technique. Son utilisation expérimentale a cependant été interdite par un jugement en cour d'appel du Royaume-Uni en août 2020 au double motif que ladite police n'avait pas établi de doctrine d'emploi suffisamment claire et ne spécifiait pas qui figurait dans les listes de personnes recherchées. Si le jugement est propre au droit anglais et au contexte de l'expérimentation, sa logique laisse voir les principes retenus, qui intéressent tout usage possible. En matière de proportionnalité dans le cas d'espèce, la cour a jugé que les apports de la technologie étaient potentiellement importants pour un impact réduit sur la vie privée du plaignant. La cour a aussi jugé que la SWP n'avait pas suffisamment évalué les biais associés à cette technologie.

Au Royaume-Uni, la police métropolitaine de Londres a également déployé des dispositifs mobiles équipés de capteurs afin de réaliser des expérimentations entre 2016 et 2019 dans des zones sensibles de la capitale. L'expérimentation a été assortie de garanties (consentement, information, protection des données, finalités claires et restrictives, évaluation, association citoyenne). La police métropolitaine de Londres déclare un taux d'erreur inférieur à 0,1 % (soit environ une personne sur mille), qui reste significatif sur une population importante et montre les marges de progression technique qui restent à franchir. Un accompagnement humain adapté capable d'établir les levées de doute permet, outre la seule technique, de maîtriser en partie ces marges d'erreur.

Dans ce cas d'usage (temps réel dans l'espace public), l'un des principaux termes du débat porte sur les données d'entrée à insérer dans un système de reconnaissance faciale. Les expérimentations londoniennes et galloises reposaient sur des « watchlists » de personnes

(52) Les points de vigilance sont notamment le stockage des données biométriques et la mise en place de mesures alternatives.

(53) Par exemple une zone d'habitation sécurisée dans le cadre d'un grand événement (G7-G20).

recherchées suivant des critères de gravité gradués. En France, l'utilisation de telles listes, issues des fichiers de police, suppose une autorisation par la loi ou un décret. Ainsi, l'expérimentation niçoise s'est fondée sur une « watchlist » dressée à partir de volontaires se mêlant ensuite à la foule elle-même volontaire pour participer. Le cadre légal allemand est comparable et l'expérimentation conduite par la police de Berlin dans une gare en 2017-2018 a également eu recours à des volontaires. La question d'une utilisation d'un ou de fichier(s) de police doit donc être traitée au préalable(54). En France, il s'agirait de fichiers de police, comme le FPR (fichier des personnes recherchées), qui serviraient de base à la constitution de listes de personnes particulièrement recherchées. L'utilisation de l'intégralité des fichiers poserait des questions de proportionnalité et de capacité technique des systèmes à les prendre en compte. De tels traitements posent des questions fondamentales de droit, qui doivent être regardées avec lucidité, sérénité et responsabilité.

Outre les aspects juridiques, la technique peut être un obstacle. En effet, la constitution des fichiers n'avait pas anticipé un recours à des systèmes d'analyse automatisée d'images. Celles-ci peuvent donc avoir un niveau de qualité et de précision insuffisant. Même si certains logiciels peuvent procéder à des redressements d'images, il serait probablement nécessaire de conduire un travail de mise en qualité afin que leur exploitation par de tels équipements soit optimisée(55). S'y ajouterait la nécessité de développer des compétences humaines pour la gestion des hits et la levée de doute.

L'emploi en situation réelle à des fins expérimentales répond à plusieurs objectifs. Il doit permettre de mesurer l'équilibre bénéfices / risques selon les cas d'usage de ces technologies, d'apprécier les efforts à accomplir en matière de maîtrise technique et humaine et de construire le cadre de contrôle et d'évaluation nécessaire. La base de licéité d'un tel usage est fondée sur la nécessité et la proportionnalité en fonction des finalités (judiciaire, prévention pour les cas les plus grave de terrorisme ou de la récidive d'actes criminels et délictuels graves) et les buts recherchés (protection de bâtiments sensibles, sécurisation d'évènements, identification de personnes recherchées, lutte contre l'hooliganisme).

La conduite d'une expérimentation sur la reconnaissance faciale en temps réel sur la voie publique pourrait en premier lieu aider à vérifier ses apports concrets pour les forces de sécurité avant de décider d'un usage pérenne et de son encadrement. L'intervention fondée sur une identification « fictive » (la personne était volontaire) ne laisse rien présager de l'efficacité de la technologie et de son utilisation dans un contexte réel avec des sujets non consentants.

Les premiers utilisateurs naturels des nouvelles technologies de sécurité sont les forces étatiques, compte tenu de leurs missions. Cependant, à terme et sous certaines conditions strictes, elles pourraient bénéficier à des acteurs non étatiques. Les collectivités locales ont ainsi montré leur intérêt pour l'expérimentation de la reconnaissance faciale. Elles font en effet face à des enjeux de sécurité importants et disposent de moyens techniques et financiers qui leur permettraient d'en conduire. De même, des opérateurs parapublics ou privés, comme dans le domaine des transports en commun, pourraient y trouver une utilité dans le contrôle des flux de voyageurs et la prévention.

En matière technique, si les développements les plus récents semblent satisfaisants, la marge de progression est réelle. En effet, en plus de la question morale de l'usage de la reconnaissance faciale dans l'espace public, qui a pu conduire à des moratoires (comme à San Francisco depuis 2019), se pose celle de la fiabilité des algorithmes et équipements. Les risques de faux positifs ou de biais (sexuels, ethniques) sont encore non négligeables car fondés sur l'ampleur des bases de données d'exercice. En effet, ces technologies sont fondées sur l'apprentissage : plus elles sont utilisées sur des données variées et réelles, plus elles apprennent, se précisent et se fiabilisent.

(54) Sur la question des fichiers à disposition des forces de sécurité, consulter le rapport des députés Didier Paris et Pierre Morel-A-L'Hussier : https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information

(55) La mise en qualité des données, notamment pour les fichiers relatifs aux étrangers et aux titres de séjour, est par ailleurs posée par l'évolution du cadre communautaire. L'adoption en 2019 des deux règlements portant « interopérabilité des systèmes s'information européens du domaine justice et affaires intérieures », avec pour horizon d'application 2022, implique en effet un emploi accru, systématisé et croisé des systèmes d'information dédiés à la gestion des ressortissants de pays-tiers et de personnes signalées. Ces évolutions impliquent notamment que les bases nationales et européennes soient alimentées en données de qualité et en partie biométriques.

La maîtrise technique recouvre différents aspects : les taux d'acquisition des visages par les capteurs, les taux de faux positifs et négatifs. Les expérimentations permettent aussi de mesurer les efforts nécessaires à un déploiement à grande échelle (charge informatique, coût des matériels, etc.). L'expérimentation peut enfin permettre d'approfondir certains paramètres, comme les capacités des différentes formes de capteurs (notamment fixes ou mobiles), le réglage et la formation des techniciens et des analystes vidéos (afin qu'ils soient en mesure de proposer des réglages paramétriques), le calibrage des moyens humains nécessaires à la levée de doute.

Les industriels du secteur font en outre valoir qu'expérimenter dépasse la question technique ; cela permet de s'approprier par la pratique l'environnement réglementaire et institutionnel d'une technologie.

La constitution et la consolidation d'un cadre de contrôle et d'évaluation doivent aussi profiter d'une période d'expérimentation. Celle-ci permettrait en effet de voir quel degré de transparence et d'information est nécessaire, qui sont les acteurs idoines du contrôle, quelles sont les modalités à retenir pour des vérifications et une évaluation effectives.

En accueillant les grands événements sportifs de 2023 (coupe de monde de rugby) et de 2024 (jeux olympiques et paralympiques), la France fera face à des besoins de sécurisation majeurs par la dimension des regroupements, les flux de voyageurs et la sensibilité des personnes engagées alors que le risque terroriste reste élevé. Ces événements ne doivent pas servir de cadre à une utilisation débridée de toutes formes de nouvelles technologies de sécurité. Il s'agit néanmoins de se donner les chances, si nécessaire, de manière ciblée et encadrée, de disposer d'outils de soutien opérationnel pour les forces de sécurité intérieure qui soient arrivés à un niveau de maturité suffisant pour être efficaces et conformes à nos standards éthiques.

Les méthodes de biométrie reposant sur la reconnaissance faciale peuvent être expérimentées afin d'assurer la sécurité des grands évènements de 2023 et 2024. La CNIL estime qu'il est possible d'organiser des expérimentations dans un cadre transparent(56). Elle rappelle que la reconnaissance faciale ne peut être utilisée que dans un impératif particulier de forte fiabilité de vérification de l'identification des personnes. Les règles relatives à la protection des données doivent être respectées, notamment en ce qui concerne le consentement des individus.

Le cadre juridique varie selon les finalités poursuivies par le traitement de données biométriques afin d'identifier une personne physique de manière unique :

- Les traitements régaliens ne peuvent être mis en place qu'en cas de nécessité absolue sous réserve de l'adoption d'un décret ou d'une loi (art. 88 de la loi « informatique et libertés »)(57).
- Les traitements réalisés à des fins de prévention et de détection des infractions pénales qui relèvent de la directive police-justice ne peuvent être mis en place qu'en cas de nécessité absolue quand le traitement est autorisé par le droit de l'État-membre(58).
- Les traitements de données biométriques aux fins d'identification d'une personne physique de manière unique qui sont réalisés sur la base du RGPD sont autorisés si la personne concernée a consenti au traitement de ses données(59). C'est sur cette base que la ville de Nice a pu expérimenter la reconnaissance faciale.

En outre, dépassant la perspective des seules années 2023-2024, les forces doivent penser à leurs besoins durables. Si cette technologie présente un équilibre bénéfices-risques satisfaisant et des apports opérationnels avérés, alors un usage pérennisé doit être envisagé. Il s'agit aussi de se projeter dans un monde vers lequel se tourne la société dans son ensemble et en particulier les adversaires et les homologues des forces. Ces nouvelles techniques devront sans aucun doute être maîtrisées dans un avenir proche pour assurer le niveau d'efficacité, d'autonomie et la capacité partenariale des forces de sécurité.

(56) Reconnaissance faciale : pour un débat à la hauteur des enjeux, CNIL, novembre 2019.
(57) Article 88 de la loi ILF.
(58) Article 10 de la directive police-justice.
(59) Article 9 al. 2 du RGPD.

Encadré : la proposition de règlement sur l'intelligence artificielle

La proposition présentée par la Commission européenne le 21 avril 2021 visant à harmoniser les règles relatives à l'intelligence artificielle encadre strictement le recours à l'identification biométrique.

La version initiale du texte **propose d'interdire l'usage de l'identification biométrique à distance dans les espaces publics par les forces de l'ordre en-dehors de cas spécifiques relevant de la sécurité des personnes ou du pays :** rechercher un enfant disparu, prévenir une menace terroriste spécifique et imminente, détecter, localiser, identifier ou poursuivre l'auteur ou le suspect d'une infraction pénale grave(60). Les systèmes d'identification biométrique à distance dans les espaces publics devraient être autorisés par une instance judiciaire ou un autre organisme indépendant et être soumis à des limitations de durée et de portée géographique.

Ces dispositions sont à l'état de propositions. Elles donnent cependant des indications sur les contours possibles d'un futur encadrement européen applicable à la législation nationale de la reconnaissance faciale en temps réel dans l'espace public.

b) La nécessaire mise au débat public

Les régulateurs, les institutions et associations de défense des droits mettent en garde contre le risque induit pour les libertés individuelles et les données personnelles par les nouvelles technologies de sécurité, dont la reconnaissance faciale.

Dans une approche philosophique, les institutions et associations de défense des droits questionnent l'orientation de la société dans son ensemble vers un usage accru des technologies de sécurité plus performantes et interconnectables. Ainsi, dans sa contribution à la mission, la Commission nationale consultative des droits de l'Homme (CNCDH) rappelle que *« (…) les droits de l'Homme ne peuvent être seulement assimilés à des 'garanties mises en place pour encadrer strictement l'usage' de dispositifs techniques de sécurité (…) »* et *« (…) souligne l'effet cumulatif des dispositifs de surveillance de l'espace public, jusqu'à la surveillance d'internet. Il est essentiel de ne pas s'en tenir simplement à une approche segmentée des technologies de sécurité, qui consisterait à envisager leur impact sur les droits fondamentaux de manière isolée. La mobilisation croissante, présente et à venir, de ces outils aura vraisemblablement une incidence sur la société et la conception de l'on se fait de la liberté. »*

Collectivement, le Comité européen de la protection des données et le Contrôleur européen de la protection des données ont confirmé dans un avis du 21 juin 2021 leur opposition à *« l'identification biométrique à distance des personnes dans les espaces accessibles au public »* et demandé *« une interdiction générale de l'utilisation de l'IA pour la reconnaissance automatisée des caractéristiques humaines dans des espaces accessibles au public »*.

La Défenseure des droits estime que les dispositifs biométriques d'identification en temps réel dans l'espace public sont les plus intrusifs. Il lui apparait difficile de concevoir comment l'utilisation de ces systèmes pourrait être considérée comme nécessaire et proportionnée compte tenu des risques de détournement d'usage et de biais qu'ils représentent(61).

Il est impératif de faire droit à ces préoccupations car elles recouvrent une aspiration consubstantielle aux démocraties modernes que sont les libertés publiques et les libertés individuelles (qui couvrent le droit à la vie privée et l'anonymat dans l'espace public). Mais ces droits ne peuvent se suffire en eux-mêmes, dans l'absolu. L'appréciation de l'intérêt général et de la fonction de l'État implique de les mettre en équilibre avec d'autres objectifs proportionnés, comme la sécurité partagée des individus et de la collectivité.

La sensibilité particulière de la reconnaissance faciale en temps réel dans l'espace public implique de débattre collectivement de l'usage qu'il est souhaitable d'en faire généralement, et tout particulièrement en matière de sécurité.

(60) Article 5 (1) (d) de la proposition de règlement 2021/0106 du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle.

(61) Technologies biométriques : l'impératif respect des droits fondamentaux, Défenseure des droits, juillet 2021.

Ainsi, la CNIL française, dans une publication de 2019[62], appelait à ouvrir un débat démocratique informé et sincère. Compte tenu des enjeux en question, cette démarche est essentielle et indispensable.

Le respect des droits implique que l'expérimentation soit conçue avec honnêteté. Les expérimentations sont souvent perçues comme une première étape, sans possibilité réelle de retour en arrière (« effet-cliquet »), et non comme le moyen de vérifier la maîtrise de la technologie, son cadre d'emploi et de contrôle et les améliorations à apporter pour un éventuel usage à l'avenir. Certains contributeurs à la mission ont soulevé, par exemple, que le déploiement de la vidéo-protection n'avait pas fait l'objet d'une évaluation approfondie sur les effets, en termes de prévention de la délinquance et d'aide aux enquêtes. La technologie est considérée avoir été progressivement installée, généralisée et tacitement acceptée, sans que soit porté un regard critique approfondi sur ses avantages opérationnels. **Afin que l'expérimentation ne soit pas un levier d'acceptabilité qui n'aille pas au fond de la vérification de la nécessité et de la proportionnalité d'emploi, elle doit être sincère et complète**. Il en va de son crédit et du crédit de la parole publique. Il est proposé de revenir à son acception première, qui est de tester un dispositif et d'en apprécier la pertinence, les avantages, les inconvénients et le devenir. Pour cela, il est indispensable d'ouvrir un débat sincère, informé et constructif.

Recommandation :

Premièrement, engager à court terme (2021) un programme d'expérimentations ciblées de la reconnaissance faciale en temps réel dans l'espace public, à droit constant, en partenariat avec les grandes collectivités et les grands opérateurs sur le modèle de l'expérimentation du Carnaval de Nice conduite en 2019. Viser en priorité les sites les plus pertinents en vue des échéances de 2023 et 2024 (grands rassemblements, enceintes sportives, nœuds et flux de transports).

Deuxièmement, en parallèle (2021-2022), envisager une évolution législative pour ouvrir un cadre d'emploi en situation réelle pour une durée limitée. Un projet ou une proposition de loi permettrait d'ouvrir un débat parlementaire sur la reconnaissance faciale en temps réel dans l'espace public. Cette expérimentation devrait se limiter pour le moment à la lutte contre le terrorisme.

Si elle avait lieu, une telle période expérimentale dans des conditions réelles devrait être sincère, transparente et strictement encadrée (finalité, durée, contrôle, évaluation) ; elle ne devrait pas seulement viser l'appréciation des apports opérationnels réels et la maîtrise technique, mais aussi le perfectionnement des moyens humains nécessaires et des garanties supplémentaires qu'il est souhaitable de mettre en place ; elle devrait plus largement contribuer à nourrir un débat public sur les usages liés à cette technologie et ce qu'il est souhaitable d'adopter et de renoncer à employer.

La supervision et l'évaluation de l'expérimentation devraient être assurées par une instance indépendante et collégiale - comprenant notamment des universitaires et des acteurs académiques - dont les conclusions seraient publiques.

Des instances citoyennes pourraient être constituées dans les localités d'expérimentation à des fins d'information, de restitution de comptes et de débat public.

Si une telle expérimentation était retenue, elle pourrait viser une arrivée à maturité en 2023-2024 afin que les emplois utiles et admis soient possibles pour la sécurisation des grands événements sportifs. Cependant, la sensibilité du sujet oblige à ne pas enfermer le sujet dans un calendrier trop contraint. Il apparaît indispensable de privilégier la réflexion et le débat, sur la base d'éléments matériels issus d'expérimentations, avant d'envisager tout usage pérenne.

Ce dispositif d'expérimentation de la reconnaissance faciale en matière de sécurité et le débat qui l'accompagnerait ne feraient pas préjudice à un débat citoyen plus large sur l'emploi des nouvelles technologies en général dans la société (cf. 3e partie du rapport).

(62) Reconnaissance faciale : pour un débat à la hauteur des enjeux, CNIL, novembre 2019.

C. Les équipements de projection et de mobilité

1. L'usage des drones et la lutte anti-drones

Les drones sont des aéronefs n'embarquant pas d'équipage et qui sont pilotés automatiquement ou télécommandés. On distingue les drones à usage civil des drones à usage militaire ou pour des missions de sécurité et secours. Ces aéronefs se répartissent en une gamme très variée de tailles, de capacités (portage, visionnage…), d'autonomie. L'usage des drones civils s'est largement répandu dans la sphère domestique ou plus largement privée (médias, événementiel). Les forces armées, de sécurité et de secours se sont aussi converties à l'usage de cette nouvelle catégorie d'aéronefs(63). Le cadre juridique d'emploi reste cependant incertain et fluctue en fonction des finalités. Les opportunités opérationnelles offertes par les drones (maniabilité, accès à des zones difficiles) font qu'il est nécessaire de réfléchir à un cadre d'emploi pérenne.

a) L'utilisation des drones à des fins de sécurité et de secours

i. Une grande diversité d'usages

Les drones sont principalement associés au portage de caméras et à la captation d'images. Ce dispositif est, par exemple, utile pour les rassemblements (manifestations, événements populaires) car il permet d'évaluer une situation, de mesurer le volume d'une foule, d'en comprendre les flux. Les forces de sécurité peuvent aussi utiliser des drones-éclaireurs afin de connaître un terrain d'intervention avant un engagement.

Le recueil d'images (photos ou vidéos) n'est cependant qu'un des usages possibles. Un drone peut répondre à de multiples autres besoins opérationnels : il peut transporter une lampe afin d'éclairer une opération, un haut-parleur afin d'informer une population, une charge d'eau dans un incendie, des équipements de survie pour une personne blessée difficilement accessible (accident de montagne par exemple), un capteur thermique pour chercher une personne égarée ou un fugitif, des dispositifs de communication radio de secours. Les forces de sécurité et de secours ont partagé avec la mission de nombreux cas d'usage concrets dans des événements récents : tempête Alex, ouragan Irma.

L'usage des drones couvre un large spectre de missions de sécurité, dont de nombreuses missions d'assistance et de secours : recherche de personnes et secours, recherche de malfaiteurs, surveillance d'espace (zone protégée, parcs nationaux, littoraux fragiles), lutte contre la délinquance environnementale (dépôts d'ordure sauvages, pollution fluviale, surveillance des cours d'eau), surveillance de zone frontalière, sécurisation de site sensible (OIV par exemple), garantie du droit à manifester (par identification des individus à risques et casseurs), communication préventive et anti fake news, cartographie de crise, aide à la régulation de flux routiers ou piétons aux abords de grands rassemblements, levée de doute en cas d'incidents.

Le drone doit donc s'envisager au travers de la « charge utile » et de la mission qui lui est assignée(64).

L'arrêté du 3 décembre 2020 encadre l'utilisation de l'espace aérien par les aéronefs sans équipage à bord qui exécutent des activités militaires, de douane, de police, de recherche et sauvetage, de lutte contre l'incendie, de contrôle des frontières ou des activités analogues sous le contrôle de l'État(65). Il impose une déclaration préalable auprès du préfet territorialement compétent aux autorités publiques qui utilisent un drone sans captation d'images(66).

ii. La particularité des drones capteurs d'images

La captation d'images par drones n'en demeure pas moins un usage important pour les forces de sécurité et une source de difficulté dans l'emploi en raison de l'encadrement juridique du recueil et de l'exploitation des données. Celle-ci relève des règles relatives au traitement des données personnelles. En effet, les drones capteurs d'images peuvent

(63) La direction de la police nationale et la direction de la gendarmerie nationale emploient respectivement 262 et 300 drones (source : avis 3404 sur le projet de loi de finances pour 2021 par M. le député Stéphane Mazars).
(64) Source : DGGN.
(65) Article 1 de l'arrêté du 3 décembre 2020.
(66) Article 3 de l'arrêté du 3 décembre 2020.

permettre l'identification de personnes dans l'espace public ou encore la prise de vues dans les espaces privés d'habitation.

Le 18 mai 2020, une ordonnance du Conseil d'État a enjoint à l'État de cesser d'utiliser des drones pour la surveillance à Paris du respect des règles de sécurité sanitaire applicables à la période de déconfinement jusqu'à l'intervention d'un texte réglementaire[67]. Celui-ci devait être pris, après avis de la CNIL, pour autoriser, dans le respect des dispositions de la loi « informatique et libertés » applicables aux traitements relevant du champ d'application de la directive « police-justice », la création d'un traitement de données à caractère personnel. Les drones utilisés devaient être équipés de dispositifs de nature à rendre impossible, pour quelque usage que ce fût, l'identification des personnes filmées.

Dans son avis du 20 septembre 2020, le Conseil d'État a souligné que les captations d'images par les autorités publiques à l'aide de dispositifs aéroportés, si elles donnent lieu à un visionnage des images filmées en temps réel sans conservation ou à un enregistrement, ne peuvent être autorisées que par la loi[68].

La CNIL a précisé dans sa délibération du 12 janvier 2021 que toute opération portant sur l'image de personnes pouvant être reconnues constitue un traitement de données à caractère personnel. Le système de floutage ne soustrait pas les images à la règlementation applicable en matière de la protection des données à caractère personnel[69].

L'article 47 de la loi pour une sécurité globale préservant les libertés prévoyait de créer un régime juridique permettant le traitement d'images au moyen de caméras installées sur des drones. Plusieurs garanties ont été apportées : interdiction du recours permanent aux drones, interdiction de filmer l'intérieur des domiciles, interdiction du recours à la reconnaissance faciale, interdiction de la captation des sons et obligation d'information du public.

Néanmoins, par sa décision du 20 mai 2021, le Conseil constitutionnel a déclaré non conformes à la Constitution les dispositions de la loi pour une sécurité globale préservant les libertés relatives au cadre juridique de la captation et l'enregistrement d'images par des caméras à bord des drones[70].

Encadré : la décision du conseil constitutionnel du 20 mai 2021

L'article 47 de la loi pour une sécurité globale préservant les libertés qui est relatif au cadre juridique de la captation et l'enregistrement d'images par des caméras à bord des drones a été censuré par le Conseil constitutionnel. Le législateur peut autoriser la captation, l'enregistrement et la transmission d'images par drones. Néanmoins la mise en œuvre de tels systèmes doit être assortie de garanties particulières de nature à sauvegarder le droit au respect de la vie privée.

En matière de police judiciaire, on peut recourir à ce dispositif pour toute infraction, y compris pour une contravention. En matière de police administrative, on peut y recourir, pour la prévention des atteintes à la sécurité des personnes et des biens, pour la sécurité des rassemblements de personnes sur la voie publique ou dans les lieux ouverts au public, pour la prévention d'actes de terrorisme, la protection des bâtiments et installations publics exposés à des risques d'intrusion ou de dégradation, la régulation des flux de transport, la surveillance des frontières et le secours aux personnes.

Le Conseil constitutionnel a relevé que le législateur n'a fixé aucune limite maximale à la durée de l'autorisation pour recourir à un tel moyen de surveillance, ni aucune limite au périmètre dans lequel la surveillance peut être mise en œuvre. Le législateur n'a défini aucun principe de contingentement du nombre de drones pouvant être utilisés, le cas échéant simultanément, par les différents services de l'État et ceux de la police municipale. Le Conseil constitutionnel a par conséquent censuré les dispositions.

(67) Ordonnance du Conseil d'État n°440442 du 18 mai 2020.
(68) Avis du Conseil d'État n°401214 du 20 septembre 2020.
(69) Délibération de la CNIL SAN-2021-003 du 12 janvier 2021.
(70) Décision du Conseil constitutionnel n°2021-817 du 20 mai 2021.

Les apports opérationnels représentés par les drones capteurs d'images, tels qu'en font part les forces de sécurité et de secours, invitent à établir un cadre d'emploi incluant les garanties nécessaires à la préservation des droits. En outre, l'ensemble des usages de drones, y compris lorsqu'il ne s'agit pas de capter des images, risque de souffrir d'une confusion autour de ces équipements. Au-delà des drones, la réflexion pourrait s'engager sur l'ensemble des aéronefs capteurs d'images (avions, hélicoptères, ballons).

Recommandation :

Afin de tenir compte de la décision du conseil constitutionnel du 20 mai 2021, clarifier par la loi le cadre juridique d'emploi par les forces de sécurité et de secours d'aéronefs dotés de dispositifs de captation automatisée d'image.

b) La lutte anti-drones

Si les drones peuvent être employés dans le cadre de missions de sécurité et de secours, ils représentent aussi une menace. Ces dernières années ont vu se multiplier les incidents de sécurité, accidentels ou intentionnels, liés à des drones d'usage civil.

Un travail conduit en 2016 par le SGDSN a permis de catégoriser les différents risques associés aux drones :
- Captation indue d'informations par des drones équipés de micros.
- Utilisation criminelle (dépôt d'objets dans les maisons d'arrêt, transport de stupéfiants).
- Action terroriste (largage d'une charge explosive sur un rassemblement, une tribune officielle, un site stratégique).
- Atteinte à la crédibilité des pouvoirs publics, des institutions ou des entreprises dans le cadre d'actions de communication.

La loi n° 1428-2016 du 24 octobre 2016 relative au renforcement de la sécurité de l'usage des drones civils approfondit la réglementation française. Elle pose ainsi de nouvelles obligations aux usagers de drones civils de plus de 800 g (enregistrement, formation, signalements). Cette loi prévoit aussi le développement d'Infodrones par le ministère de l'Intérieur, afin d'exploiter les données d'enregistrement en vue de l'identification de drones en infraction ou malveillants.

Les moyens opérationnels de lutte anti-drones sont divers et encore en développement, en raison du caractère récent du sujet et de l'identification des menaces associées ainsi que de la dynamique d'innovation que connaissent les drones. Ils devraient par conséquent faire l'objet d'un intérêt approfondi en recherche-développement et innovation. Plusieurs méthodes sont aujourd'hui identifiées : la détection des drones, l'analyse des spectres électromagnétiques, l'interception des signaux vidéos, les brouilleurs mobiles.

La perspective des grands événements sportifs de 2023 et 2024 invite à accroître l'effort sur la détection et la neutralisation de drones malveillants. Des expérimentations pourraient consister en la mise en œuvre d'un système de surveillance et de tracking des drones sur la voie publique[71]. En l'absence de base légale, depuis la censure constitutionnelle de l'article 47 de la loi « sécurité globale » autorisant le traitement d'images au moyen de caméras embarquées sur des drones, les expérimentations en cours ont été interrompues. En effet, les télépilotes opérant les drones qui simulent l'action malveillante pour tester les systèmes de détection ont besoin du retour vidéo du drone pour son pilotage. Elles pourraient reprendre si le législateur l'autorise.

Recommandation :

Suivant les options retenues sur le cadre d'emploi des drones capteurs d'images, envisager des expérimentations en matière de lutte anti-drones, en y associant des financements dédiés dans le cadre de la préparation des jeux olympiques et paralympiques.

(71) Source : SGDSN.

2. Les « caméras embarquées »

Les véhicules de transport des forces de sécurité et de secours peuvent aussi être dotés de dispositifs de captation d'images. Ces recueils peuvent être utiles dans une exploitation en temps réel, afin d'assurer une liaison avec les centres de commandement ou dans une revue *a posteriori* (pour un retour d'expérience, dans le cadre d'une enquête administrative ou judiciaire).

Comme les dispositifs similaires intégrés à des aéronefs, ils présentent des risques pour les droits et libertés car les images captées peuvent inclure des personnes ou des lieux privés. Les caméras portées par les agents, dites « caméras-piétons », ont été dotées d'une cadre juridique d'emploi, afin d'assurer un équilibre entre les finalités de sécurité et la garantie des droits.

Les dispositions relatives aux caméras embarquées, prévues dans la loi pour une sécurité globale préservant les libertés, ont été censurées le 20 mai 2021 par le conseil constitutionnel, au motif que les garanties apportées n'étaient pas suffisamment fortes pour l'intégrité des droits et libertés des personnes.

Encadré : la décision du conseil constitutionnel du 20 mai 2021

L'article 48 de la loi pour une sécurité globale préservant les libertés qui visait à autoriser les services de police à procéder à la captation, à l'enregistrement et à la transmission d'images au moyen de caméras embarquées équipant tout moyen de transport, à l'exception des drones, a été censuré par le Conseil constitutionnel.

D'une part, le Conseil souligne que les caméras embarquées peuvent capter, enregistrer et transmettre des images sur la voie publique ou dans des lieux ouverts au public, y compris de l'intérieur des immeubles, ainsi que de leurs entrées. D'autre part, il rappelle que l'information spécifique du public, prévue par le législateur, n'est pas donnée lorsque les circonstances l'interdisent ou lorsqu'elle est en contradiction avec les objectifs poursuivis.

Enfin, le Conseil considère que le législateur n'a fixé aucune limite maximale à la durée nécessaire à la réalisation de l'intervention, ni aucune borne au périmètre dans lequel cette surveillance peut avoir lieu. La décision de recourir à des caméras embarquées relève des seuls agents des forces de sécurité intérieure et des services de secours. Elle n'est soumise à aucune autorisation, ni même à l'information d'une autre autorité. Pour ces raisons, le Conseil constitutionnel a censuré ces dispositions.

Les caméras embarquées sont des outils opérationnels qui peuvent être utiles aux forces de sécurité et de secours. Les liaisons avec les centres de commandement peuvent donner à voir en temps réel l'état d'une situation locale et l'éventuel besoin d'adapter une posture opérationnelle et les moyens engagés. A l'instar des caméras-piétons, elles peuvent en outre avoir un effet de prévention en suscitant un apaisement des situations de tension. Enfin, elles ont un usage *a posteriori* en constituant des banques de données exploitables, notamment dans le cadre d'enquêtes sur des faits et des interventions. Afin d'en favoriser l'utilisation tout en tenant compte des impératifs de préservation des droits et libertés des personnes par des garanties suffisantes, tel que le rappelle le conseil constitutionnel dans sa décision du 20 mai dernier, il serait nécessaire d'adapter par la loi le cadre juridique d'emploi.

Recommandation :

Afin de tenir compte de la décision du conseil constitutionnel du 21 mai 2021, clarifier par la loi le cadre juridique d'utilisation des dispositifs de captation d'image intégrés aux véhicules des forces de sécurité et de secours (dits « caméras embarquées »).

III. Donner des garanties pour construire une relation de confiance à long terme avec les Français autour des nouvelles technologies dans le domaine de la sécurité

A. Construire un socle de principes communs autour des technologies de sécurité

Les forces de sécurité intérieure doivent pouvoir employer les technologies de sécurité dans un cadre respectueux des libertés publiques et individuelles afin de bénéficier d'un appui technique (opérationnel, dans l'aide à la décision, etc.) pour réaliser leurs missions en pleine légitimité. La définition d'un socle de principes communs vise à encadrer l'usage des technologies par les forces de sécurité intérieure afin de préserver les libertés. D'une part, ces principes permettent d'éviter un usage disproportionné des technologies de sécurité. D'autre part, ces principes rendent possible l'expérimentation des technologies dans un cadre clair et suffisamment flexible.

1. Garder la main sur la technologie

Dans un contexte d'automatisation croissante des tâches, notamment à l'aide de l'IA, les forces de sécurité intérieure doivent pouvoir garder la main sur les technologies, c'est-à-dire avoir la maîtrise des solutions technologiques qu'elles emploient. Cela passe par la formulation de critères dans le choix des technologies qui sont employées mais aussi par un encadrement technique.

a) Les choix technologiques

Tout d'abord, il est préférable que les forces de sécurité intérieure ne recourent à des technologies de sécurité que lorsque celles-ci ont atteint un stade de maturité suffisant. La maturité des technologies peut notamment être éprouvée au travers d'expérimentations. Les technologies qui n'ont pas atteint un niveau de maturité technologique suffisant ne doivent pas être déployées à grande échelle, notamment dans le cadre des grands évènements.

Ensuite, il est souhaitable que les forces de sécurité intérieure privilégient des solutions souveraines pour les usages les plus critiques et dans le respect du droit de la commande publique. Le recours à des solutions étrangères peut représenter un risque opérationnel pour les forces de sécurité. En outre, la pleine maîtrise des outils permet de garantir les droits des personnes en évitant une extra-territorialisation des flux (ex : *backdoors*, transferts de données).

Enfin, les forces de sécurité intérieure devraient adopter une approche par les risques lorsqu'elles emploient des technologies de sécurité. Les technologies les plus intrusives ne doivent être employées que pour le haut du spectre des missions de sécurité (terrorisme, criminalité organisée, personnes dangereuses). Les garanties à apporter sont d'autant plus importantes que les usages présentent des risques pour les droits et les libertés. A titre d'exemple, l'identification biométrique, en temps réel, dans l'espace public, par les forces de sécurité, ne devrait être utilisée que pour des finalités strictement définies et pour les cas les plus graves. La conformité des usages au droit européen sera à confirmer en fonction des suites de la proposition de règlement sur l'intelligence artificielle portée par la Commission.

b) Le cadre technique

Le recours aux technologies de sécurité doit être encadré sur le plan technique afin que les forces de sécurité intérieure gardent la maîtrise des technologies qui sont employées.

D'une part, les technologies de sécurité doivent bien prendre en compte la cybersécurité. Les défauts en matière cyber peuvent affecter durablement la confiance de la population et constituer un motif de rejet des technologies de sécurité[72]. Comme le souligne le rapport du *National Intelligence Council*, la croissance exponentielle des appareils connectés augmente considérablement le risque d'attaques cyber[73]. Dès lors, l'État doit être exemplaire en matière de cybersécurité. Il peut réaliser systématiquement des analyses de risques cyber

(72) Source : ANSSI.
(73) https://www.dni.gov/index.php/gt2040-home/gt2040-structural-forces/technology

en amont de l'intégration des technologies, mais aussi intégrer des clauses types dans les marchés publics qui permettent d'acquérir ou de déployer de nouvelles technologies. Un niveau élevé de cybersécurité doit être maintenu tout au long du cycle de vie des technologies.

D'autre part, les technologies entièrement automatisées sont à proscrire pour des raisons de sécurité. Techniquement, cette automatisation quasi-complète pourrait être possible, si le paramétrage et son évolution bénéficient de technologies auto-apprenantes. Le renoncement à cette perspective est donc à nommer explicitement. Il est nécessaire de maintenir une intervention humaine en décision. Si les technologies d'IA, par exemple, peuvent contribuer au processus décisionnel en sélectionnant, recommandant, comparant, challengeant, l'agent doit rester maître de la décision finale emportant une intervention. Les technologies doivent intervenir au stade de la levée de doute, de l'aide à la décision ou à la planification, mais ne doivent pas se substituer à l'acte décisionnel pris par un agent.

Recommandation :

Enrichir les doctrines d'emploi avec les principes suivants : niveau de maturité technologique suffisant, solutions souveraines pour les usages les plus critiques, approche par risque, prise en compte des enjeux de cybersécurité et intervention humaine obligatoire dans le processus décisionnel dans les cas où la technologie est partiellement ou entièrement automatisée.

2. Protéger les données

Le droit à la vie privée et le droit à la protection des données personnelles sont consacrés dans le droit national et au niveau conventionnel. La vie privée est un droit protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen (DDHC). La protection des données personnelles est consacrée par l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Les principes de nécessité et de proportionnalité guident l'action des forces de sécurité intérieure lorsqu'elles emploient des technologies de sécurité. Elles mettent en place des garanties afin de préserver les droits et libertés.

a) Les droits

Le droit à la vie privée est pleinement reconnu au niveau national et européen. L'article 9 du code civil précise que « *toute personne a droit au respect de sa vie privée* ». La Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'Union ont consacré le droit à la vie privée[74]. S'il ne figure pas dans le droit constitutionnel écrit[75], le Conseil constitutionnel a reconnu que le droit à la vie privée est protégé par l'article 2 de la DDHC[76].

Le droit à la protection des données personnelles est venu renforcer le droit à la vie privée. La loi Informatique et libertés de 1978 a créé la commission nationale de l'informatique et des libertés (CNIL). Le RGPD et la directive police-justice ont posé un cadre juridique spécifique pour la protection des données personnelles. Les informations qui sont considérées comme des données personnelles sont soumises aux règles relatives à la protection des données. Le droit à la protection des données personnelles n'est pas absolu mais doit, au contraire, être mis en balance avec d'autres intérêts, tels que ceux poursuivis par les technologies de sécurité.

(74) Article 8 de la CEDH et article 7 de la CDFUE.
(75) Vincent Mazeaud, « La constitutionnalisation du droit au respect de la vie privée », Les nouveaux cahiers du Conseil constitutionnel n°48, juin 2015.
(76) Décision du Conseil constitutionnel n° 99-416 du 23 juillet 1999.

b) Les principes

Les principes de proportionnalité et de nécessité guident la décision des forces de sécurité intérieure dans l'emploi des technologies de sécurité. **Selon la CNIL, ils imposent des analyses au cas par cas appliquées *in concreto* à des cas d'usages bien déterminés**.

Le principe de nécessité permet d'apprécier les finalités qui sont envisagées par les forces de sécurité. Le besoin des forces doit être réel, effectif et actuel. Il ne suffit pas qu'une technologie soit potentiellement utile, au contraire elle doit dégager des bénéfices concrets précisément délimités et qui ont été évalués. L'objectif poursuivi ne peut raisonnablement pas être atteint par des moyens moins intrusifs.

Le principe de proportionnalité permet d'apprécier l'adéquation entre les moyens utilisés et les objectifs poursuivis par les forces de sécurité. Sur le fondement de ce principe, le recours à certaines technologies, particulièrement intrusives, peut être interdit si elles sont employées pour réaliser des objectifs qui ne justifient pas cette atteinte. Ainsi, l'utilisation d'une technologie de reconnaissance faciale automatique sur une caméra de vidéoprotection, afin de repérer la commission d'une simple contravention, semble disproportionnée. Un autre effet possible de l'application du principe de proportionnalité est de n'accepter le recours à une technologie qu'à la condition que des garanties soient créées.

c) Les garanties

Les textes relatifs à la protection des données personnelles prévoient un certain nombre de garanties que doivent respecter, dans la mesure du possible, les forces de sécurité intérieure lorsqu'elles emploient des technologies qui traitent des données à caractère personnel[(77)]. Les finalités doivent être limitées, c'est-à-dire déterminées, explicites et légitimes. Les données qui sont traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard de ces finalités. La durée de conservation des données personnelles n'excède pas ce qui est nécessaire. Les modalités de contrôle sont essentielles. Plus elles sont nombreuses, diverses et fréquentes en amont et en aval, plus la probabilité d'atteindre le juste équilibre entre liberté et sécurité est importante. Enfin, si l'information du public sur les conditions de mise en œuvre du traitement de données dont les personnes font l'objet, peut légitimement être écartée, lorsque cette information fait obstacle ou nuit à la finalité même du traitement en cause[(78)], elle n'en reste pas moins obligatoire à chaque fois que cela est permis par les circonstances de l'espèce.

Les textes relatifs à la protection des données personnelles prévoient un certain nombre de garanties techniques qui peuvent venir faciliter le travail des forces. L'anonymisation des données consiste à casser tout lien entre des données et les personnes concernées à l'origine par ces données. Un ensemble de données est à priori anonyme quand il n'est possible, ni d'individualiser, ni de corréler, ni d'inférer ces données[(79)]. L'anonymisation est un problème complexe, qui nécessite, en général, une analyse au cas par cas, afin de déterminer précisément les techniques d'anonymisation. Certains types de données sont très difficiles à anonymiser correctement. De plus, certaines finalités ne sont pas conciliables avec l'anonymisation et doivent donc être opérées sur des données à caractère personnel, ce qui fait tomber les traitements associés dans le champ d'application du cadre juridique relatif à la protection des données personnelles. Néanmoins, des travaux pourraient être initiés pour anonymiser des jeux de données quand cela est possible, afin de les sortir du champ d'application du RGPD.

(77) Article 5 du RGPD et article 4 de la directive police-justice.
(78) Article 12 à 15 du RGPD et article 13 de la directive police-justice.
(79) Avis du G29 05/2014 sur les techniques d'anonymisation : https://www.cnil.fr/fr/le-g29-publie-un-avis-sur-les-techniques-danonymisation

Recommandation :

Il est difficile d'établir la proportionnalité et la nécessité des atteintes au droit à la vie privée lorsque des acteurs publics ou privés utilisent des technologies qui exploitent des données personnelles. Le champ juridique est récent et les innovations techniques le challengent régulièrement. Il apparaît indispensable que le ministère de l'Intérieur se dote d'une politique de la donnée qui concilie la protection des données personnelles et l'emploi de technologies de sécurité.

3. Expérimenter les technologies de sécurité

L'expérimentation recouvre deux réalités différentes. La plupart des expérimentations se font à droit constant et ne permettent pas de déroger au cadre juridique existant. A l'inverse, certaines expérimentations permettent de suspendre l'application d'une norme législative ou réglementaire quand une loi ou un décret d'expérimentation ouvre un cadre d'expérimentation.

L'expérimentation est essentielle pour déterminer si les outils et les technologies envisagés présentent un avantage réel aux forces de sécurité. Elle permet aussi de vérifier les niveaux de compétences, les processus de contrôle, la conformité au cadre juridique. Une expérimentation est réussie lorsqu'elle suit une méthodologie précise. Cette méthode peut déclinée de façon opérationnelle pour préparer les grands évènements.

a) La méthodologie

Les technologies de sécurité sont expérimentées par les forces de sécurité intérieure pour plusieurs raisons. Tout d'abord, une expérimentation permet de tester la nécessité d'emploi et le niveau de maturité d'une technologie. Ensuite, une expérimentation vient valider des cas d'usage et permet de trouver un cadre d'emploi pertinent. Enfin, les résultats des expérimentations permettent d'écarter le recours à certaines technologies ou fournissent au contraire des arguments objectifs et scientifiques pour retenir l'emploi d'autres technologies de sécurité.

Les expérimentations présentent néanmoins un certain nombre d'écueils qui doivent être anticipés par les forces de sécurité intérieure. D'une part, il faut tenir compte des résultats des expérimentations, ce qui n'est pas toujours le cas, celles-ci étant souvent reconduites sans tenir compte des évaluations qui ont été réalisées. D'autre part, le passage à l'échelle doit être anticipé par les forces de sécurité intérieure. Trop d'expérimentations ne font l'objet d'aucune généralisation. La démarche doit être sincèrement expérimentale, ce qui implique de limiter dans le temps et dans l'espace les dispositifs, d'identifier exactement les objectifs poursuivis et de définir précisément les modalités d'évaluation[80].

Les expérimentations qui ont lieu à droit constant peuvent être soumises à une autorisation de la CNIL. Ces autorisations sont obtenues dans des délais qui sont souvent incompatibles avec le déploiement rapide des solutions industrielles (un an, dans certains cas, pour obtenir une autorisation). Si cet allongement des délais est compréhensible, vu l'augmentation croissante des missions de la CNIL, il est particulièrement problématique, pour certains acteurs, comme les opérateurs d'importance vitale (OIV) ou les opérateurs de services essentiels (OSE) qui participent aux missions de sécurité. Il serait souhaitable que la CNIL mette en place une procédure permettant de prioriser les demandes d'autorisations pour des expérimentations, en tenant compte de l'origine de la demande, de l'urgence et des enjeux. Par ailleurs, il serait souhaitable que des prestataires extérieurs puissent accompagner juridiquement les entreprises et les opérateurs qui souhaitent entamer une démarche d'expérimentation afin de pouvoir faciliter leurs démarches. Ces prestataires pourraient être agréés par la CNIL, dans une logique de tiers de confiance.

Les expérimentations qui permettent de déroger au cadre juridique sont autorisées par le parlement ou par le pouvoir réglementaire en adoptant une loi ou en prenant un décret d'expérimentation. L'article 37-1 de la constitution encadre rigoureusement les

(80) Source : CNIL.

possibilités d'expérimentations, qui dérogent au principe d'unité du droit sur le territoire de la République. En effet, il implique de prendre une loi ou un décret comportant des dispositions à caractère expérimental, dans des délais qui sont difficilement compatibles avec le calendrier de déploiement des solutions industrielles. Afin d'accélérer et de densifier cette procédure, plusieurs mesures sont possibles : (*i*) identifier un interlocuteur unique qui centralise les demandes d'adaptation des normes réglementaires et législatives ; (*ii*) accompagner juridiquement en amont les acteurs pour identifier les besoins ; (*iii*) fixer un calendrier en amont pour prendre une loi ou décret d'expérimentation.

Recommandation :

Faciliter le recours aux expérimentations des technologies de sécurité en prenant les mesures législatives et réglementaires nécessaires, en clarifiant les processus, en définissant une méthode partagée et en renforçant l'accompagnement des acteurs.

b) Le lancement d'expérimentations en amont des grands évènements

Si le gouvernement souhaite lancer des expérimentations en amont des grands évènements de 2023 et de 2024, la première étape est de déterminer quelles sont les expérimentations qui peuvent se faire à droit constant et quelles sont les expérimentations qui nécessitent de prendre une loi ou un décret d'expérimentation.

Les expérimentations qui peuvent se faire à droit constant d'ici les grands évènements concernent l'authentification forte des détenteurs de droit d'accès aux sites privés[81] et l'identification biométrique en temps réel sur le modèle de l'expérimentation du Carnaval de Nice (avec consentement).

Les expérimentations, qui nécessitent de prendre en amont un décret ou une loi, concernent l'authentification forte pour les détenteurs de droit d'accès aux sites publics[82], la détection de drones malveillants[83], les dispositifs d'imagerie utilisant des ondes millimétriques DE pour l'accès aux enceintes sportives[84]. S'y ajouterait, selon le déroulé du débat public, l'identification biométrique en temps réel dans l'espace public par reconnaissance faciale dans les finalités retenues (lutte anti-terroriste)[85]. Si le gouvernement souhaite lancer rapidement ces expérimentations, il doit agir par voie réglementaire et législative d'ici la fin de l'année 2021.

Pour certaines expérimentations, comme la détection automatisée d'anomalies en direct dans les établissements accueillant du public, la nécessité d'adapter le droit, et, le cas échéant, le niveau normatif requis sont à déterminer rapidement en sollicitant si nécessaire l'avis du Conseil d'État.

La deuxième étape consiste à ouvrir les crédits nécessaires pour financer les expérimentations avant les grands évènements de 2023 et 2024. Afin d'assurer la sécurisation des jeux olympiques, il faut moderniser l'équipement des forces de sécurité intérieure. L'État s'est engagé auprès des industriels à solliciter un budget consacré à la sécurité des jeux olympiques et des grands évènements sportifs internationaux, qui soit rattaché au ministère de l'Intérieur, pour financer l'expérimentation de technologies de sécurité et leur déploiement opérationnel. Le montant des besoins est estimé à environ 200 millions sur trois ans dont une vingtaine de millions pour l'année 2021 qui ne pourront pas être financés en gestion et sous plafond existant.

Les étapes suivantes interviendront en 2022, avec la restitution des expérimentations et avant leur généralisation, pour les grands évènements sportifs en 2023 et 2024.

(81) Une telle expérimentation a déjà été menée à Roland-Garros.
(82) Sous réserve d'un décret en Conseil d'État.
(83) Les expérimentations en cours ont été interrompues en l'absence de base légale depuis la censure de l'article 47 de la loi sécurité globale autorisant le traitement d'images au moyen de caméras embarquées sur des drones.
(84) Sous réserve d'une disposition législative.
(85) Sous réserve d'une disposition législative.

Recommandation :

Déterminer quelles sont les expérimentations qui peuvent être menées à droit constant et quelles sont les expérimentations qui nécessitent de prendre en amont des dispositions législatives ou réglementaires, les dispositions législatives pouvant être introduites par voie d'amendement d'ici la fin 2021.

Ouvrir les crédits nécessaires au financement des expérimentations, en attribuant dans un premier temps 50 millions d'euros au secrétariat général du ministère de l'Intérieur pour l'année 2022. Porter une attention particulière au pilotage, qui pourrait être confié à la délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité (DPSIS).

B. Mobiliser la société civile

Les contestations sociales qui ont eu lieu durant l'examen de la loi sécurité globale montrent la sensibilité de l'opinion publique sur l'emploi des nouvelles technologies à des fins de sécurité. Alors que le traitement massif de données personnelles par de grands groupes privés extraeuropéens suscite relativement peu de polémiques dans le débat public, l'emploi des technologies par les forces de sécurité intérieure est régulièrement critiqué par une partie de l'opinion publique.

La question de l'acceptabilité sociale des nouvelles technologies est devenue un enjeu majeur pour les forces de sécurité intérieure. Si plusieurs facteurs expliquent aujourd'hui le manque d'acceptabilité des technologies de sécurité, ce sujet dépasse largement le domaine de la sécurité publique. La montée en compétence de la société sur les sujets technologiques et la capacité à remobiliser le corps social pour définir collectivement les usages de demain sont des garanties indispensables à l'emploi des technologies au XXIème siècle.

1. L'acceptabilité des nouvelles technologies de sécurité

a) *L'acceptabilité des technologies est un défi majeur dans le champ de la sécurité mais aussi pour l'ensemble du secteur public*

Aujourd'hui, on constate une accentuation de la défiance envers les technologies, lorsqu'elles sont employées dans le champ de la sécurité. Une frange de la société civile est clairement hostile à l'emploi des technologies par les forces de sécurité intérieure. Parmi elles, les associations protectrices des droits de l'Homme critiquent l'augmentation croissante des atteintes à la vie privée, ainsi que le recours accru aux technologies à des fins de surveillance des populations. A titre d'exemple, les technologies biométriques sont considérées par la Ligue des droits de l'Homme comme des techniques qui participent à la réduction de l'identité[86]. L'EDRI demande un moratoire sur la reconnaissance faciale au niveau européen[87].

Néanmoins, la défiance vis-à-vis des nouvelles technologies n'est pas uniquement présente dans le champ de la sécurité mais concerne l'ensemble du secteur public. Cette contestation prend différentes formes, en fonction des politiques publiques et des outils qui sont mobilisés. Il est intéressant de remarquer que l'application *Stop Covid* proposée par le gouvernement pour répondre à la crise sanitaire a connu des oppositions similaires à celles que peuvent provoquer les technologies de sécurité. Une partie de la population était inquiète de la capacité à être géolocalisée à tout moment. Les préoccupations qui émanent de la société civile sur l'emploi des nouvelles technologies dépassent largement le domaine de la sécurité.

(86) Source : LDH.
(87) https://www.politico.eu/article/activists-urge-eu-to-ban-live-facial-recognition-in-public-spaces/

b) Plusieurs facteurs peuvent venir expliquer les difficultés à accepter l'emploi des nouvelles technologies dans le domaine de la sécurité

Le manque d'information du public peut expliquer l'absence d'appropriation des enjeux liés aux nouvelles technologies, mais aussi leur mauvaise compréhension dans l'opinion publique. Le sondage Odoxa, conduit pour Saegus sur la reconnaissance faciale en mai 2021, montre que les Français se sentent de plus en plus mal informés sur l'utilisation de leurs données par des technologies de reconnaissance faciale (75% aujourd'hui contre 72% en 2020), alors même que le sujet est de plus en plus évoqué dans le débat public et dans l'actualité. La dégradation de la qualité du débat public empêche les Français de s'approprier les enjeux liés aux technologies dans le domaine de la sécurité. Les réseaux sociaux, en mettant en avant les opinions clivantes, accentuent la polarisation du débat public(88) et installent les internautes dans des bulles de confort où ne leur est proposé qu'un contenu en accord avec leur opinion (« *enfermement algorithmique* »). Ils facilitent, en outre, la diffusion de fausses informations. La désinformation, c'est-à-dire le détournement volontaire d'information pour induire, cacher ou travestir des faits, et la mésinformation, c'est-à-dire la diffusion d'informations erronées de manière involontaire, sont des pratiques de plus en plus courantes qui nuisent à la qualité du débat public(89).

La réticence au partage de données peut aussi expliquer en partie les difficultés du public à accepter l'emploi de nouvelles technologies particulièrement intrusives. Aujourd'hui, plus des deux tiers des Français affirment être attentifs au traitement de leurs données personnelles, lorsqu'ils utilisent internet(90). Ils témoignent d'un intérêt croissant pour la protection des données personnelles, et peuvent se montrer ainsi plus réticents au partage de leurs données.

La défiance institutionnelle est un dernier facteur qui peut venir expliquer les réticences des citoyens par rapport à l'emploi de nouvelles technologies dans le domaine de la sécurité. Les contestations que nous connaissons aujourd'hui, et qui peuvent être assimilées à une remise en cause de l'autorité, ne sont pas uniquement présentes dans le domaine de la sécurité, comme en témoigne la crise des gilets jaunes ou plus récemment les contestations sur le port du masque dans l'espace public et sur l'instauration du passe sanitaire. Néanmoins, elles doivent nécessairement être prises en compte. En effet, imposer les technologies de sécurité ne fera que tendre une situation déjà complexe.

Au contraire, c'est en assurant une meilleure compréhension des enjeux, et en permettant une définition collective des usages, que nous pourrons résorber la défiance vis-à-vis des technologies, à la fois dans le champ de la sécurité mais aussi dans le reste du secteur public.

2. S'approprier les nouvelles technologies

a) Politique massive d'information et de sensibilisation du grand public

Afin d'assurer la montée en compétence du grand public sur les sujets technologiques, une politique massive d'information et de sensibilisation peut permettre, d'une part d'informer le grand public sur les usages qui sont faits du numérique et, d'autre part de le sensibiliser aux risques qui existent dans l'espace numérique et aux moyens pour s'en prémunir : protection des données personnelles, lutte contre la désinformation, résilience contre les risques cyber.

(88) Source : CNNum.
(89) Task force Reconnaissance faciale, Jeunes IHEDN, juin 2021.
(90) https://www.ifop.com/publication/les-francais-et-la-souverainete-numerique/

Recommandation :

Mener au niveau national une large campagne de sensibilisation aux nouvelles technologies. Au sein du ministère de l'Intérieur, une campagne de sensibilisation peut être lancée auprès du grand public sur l'action des forces de sécurité intérieure. Cette campagne évoquerait en particulier les besoins des forces et les raisons pour lesquelles ils recourent aux technologies.

b) Formation aux nouvelles technologies

La formation aux technologies passe par l'acquisition de nouvelles compétences dans toutes les tranches de la population. D'une part, la formation initiale permet de sensibiliser la population au numérique dès le plus jeune âge, mais aussi de former une partie de la jeunesse aux métiers du numérique. Si la formation aux sciences du numérique, l'éducation aux médias et la maîtrise des outils sont intégrés dans les programmes scolaires(91), certains publics comme les femmes ou les habitants des quartiers prioritaires restent sous-représentés dans les métiers du numérique(92). D'autre part, la formation continue permet d'acquérir des compétences numériques tout au long du cycle de vie professionnelle. La formation aux nouvelles technologies représente un double défi en termes de massification et d'individualisation des contenus de formation : 50% des métiers ont vocation à voir leurs contenus profondément évoluer, mais il faut dans le même temps tenir compte des besoins de chaque salarié(93).

L'emploi des technologies de sécurité implique une politique de formation adéquate au ministère de l'Intérieur. Le recrutement et la formation doit s'adapter à l'évolution des missions en diversifiant les viviers de candidats et les modalités de recrutement. Le numérique doit être davantage intégré aux cursus et aux plans de formation(94), qui sont l'occasion de sensibiliser les forces aux aspects techniques, mais aussi au droit et à l'éthique en matière de sécurité et d'emploi des technologies. Le recours à des contractuels pour des missions de haut niveau peut être renforcé dans le domaine des nouvelles technologies si la compétence est insuffisante en interne. Comme le souligne le Livre blanc de la sécurité intérieure de 2020, cela nécessiterait de travailler à l'attractivité de l'administration pour les hauts profils numériques. L'articulation de l'approche scientifique universitaire avec les pratiques et l'activité de terrain des forces de sécurité constitue un enjeu majeur. Il est indispensable de développer des partenariats avec les universités, mais aussi de recruter des chercheurs lorsqu'ils disposent de compétences rares ou spécifiques essentielles aux missions du ministère.

Recommandation :

Concernant la formation initiale le service national universel doit être l'occasion de valider les compétences numériques de la population et de renforcer le lien entre les forces de sécurité intérieure et la nation.

Concernant la formation continue la politique des ressources humaines doit permettre de recruter au sein du ministère de l'Intérieur des compétences mixtes, à la fois techniques et juridiques.

(91) Rapport d'information de la sénatrice Catherine Morin-Desailly, juin 2018.
(92) « Faire du numérique un accélérateur de diversité », CNNum, septembre 2020.
(93) Rapport d'information de la sénatrice Catherine Morin-Desailly, juin 2018.
(94) Par exemple en intégrant le numérique au cursus de formation des commissaires de police ou en massifiant les formations suivies sur les nouvelles technologies. Le MOOC de l'Institut Montaigne sur l'intelligence artificielle est déjà suivi par près de 80 000 gendarmes.

c) Ouverture des données et des codes sources

L'ouverture des données et des codes sources par les administrations publiques garantit la mise à disposition des données et des codes sources publics dans des formats ouverts et exploitables. Elle s'inscrit directement dans l'application de l'article 15 de la DDHC : « *La société a le droit de demander compte à tout agent public de son administration* ».

L'ouverture des données et des codes sources est un gage de transparence et d'efficacité pour l'action publique. D'une part, l'ouverture des données publiques et des codes sources est un gage de transparence de la décision publique, dans la mesure où les citoyens disposent des informations fondant la décision de l'administration et des traductions informatiques des algorithmes de décisions. En ce sens, elle renforce la confiance des citoyens et leur adhésion. La mission menée par le député Eric Bothorel recommande, par exemple l'ouverture de certaines briques du code source de l'identité numérique régalienne, qui pourrait renforcer la confiance dans le dispositif, en explicitant la manière dont sont utilisées les données(95). D'autre part, l'ouverture des données publiques et des codes sources améliore le pilotage des politiques publiques, dans la mesure elle renforce le contrôle de gestion et d'évaluation des politiques publiques, le partage d'informations entre les administrations publiques et le pilotage de l'action publique par la donnée. Comme le souligne la mission Bothorel : *« L'ouverture des données épidémiologiques dans le cadre de l'épidémie de Covid19 a mis en évidence l'importance de la collecte de données dans le pilotage de la crise. Par ailleurs, la recherche de transparence de l'action publique et la pédagogie nécessaire pour susciter l'adhésion aux décisions prises ont joué un rôle dans la place centrale réservée aux données »*.

L'ouverture des données publiques et des codes sources se heurte néanmoins à des contraintes fortes dans les domaines régaliens. D'une part, l'ouverture des données et des codes sources publics peut présenter des risques en matière de protection des données personnelles, de sécurité informatique, mais aussi de captation de la valeur de la donnée par des acteurs privés(96). D'autre part, il existe plusieurs exceptions à la communicabilité et à la réutilisation des documents administratifs : la défense nationale, la sûreté de l'État, la sécurité publique et la sécurité des personnes(97). La Commission d'accès aux documents administratifs (CADA) ne refuse pas systématiquement la communication de documents dans le domaine de la sécurité publique, mais uniquement des documents « *dont la divulgation serait de nature à lui porter atteinte* »(98). Il faut déterminer les conditions de l'articulation de l'ouverture des données publiques avec les nécessités de sécurité publique.

Le ministère de l'Intérieur conduit une politique d'ouverture des données publiques, qu'il souhaite amplifier en 2021. Le ministère de l'Intérieur s'est pleinement impliqué dans la politique d'*open data* lancée par le Gouvernement depuis 2011. Cet engagement lui permet actuellement d'afficher un socle volumineux de données ouvertes avec 613 jeux de données, au 1er juillet 2021, qui couvrent l'ensemble de ses domaines d'intervention : l'exercice démocratique, les libertés publiques, la sécurité intérieure et la protection des populations(99). Ces données sont éditées sous des formats réutilisables et publiées sur data.gouv.fr. À l'issue du Comité interministériel de la transformation publique (CITP) du 27 avril 2021, le Premier ministre a annoncé le lancement d'une politique publique de la donnée ambitieuse en s'appuyant sur une gouvernance renforcée. La circulaire du 27 avril 2021, relative à la politique de la donnée, invite les administrations à réunir les conditions de mise en œuvre d'une meilleure ouverture des données publiques, afin de les rendre exploitables par des tiers. Elle crée un réseau d'administrateurs ministériels des données (AMD), en charge d'élaborer la stratégie d'exploitation et d'ouverture des données publiques.

(95) Pour une politique publique de la donnée, des algorithmes et des codes sources, rapport de la mission du député Eric Bothorel, décembre 2020.
(96) Ibidem.
(97) Article L311-5 du CRPA.
(98) Bertrand Warusfel, « *Enjeux et limites de l'ouverture des données en matière de sécurité et de défense* », Revue française d'administration publique, 2018/3 (N° 167).
(99) Source : DNUM.

Recommandation :

Organiser la feuille de route du ministère de l'Intérieur sur l'ouverture des données publiques, en déterminant les conditions de son articulation avec les nécessités de sécurité publique. La feuille de route devra répondre aux priorités identifiées par la circulaire du Premier ministre à savoir le développement de compétences liées aux données, tant parmi les cadres dirigeants de la fonction publique que par l'ensemble des agents, et la définition des objectifs relatifs au pilotage, à l'ouverture, à la circulation et au partage des données et des codes sources, afin de les rendre exploitables par les chercheurs, les entreprises et les citoyens. Elle pourra déterminer la liste des données et des codes sources publics qui peuvent être rendus accessibles au public.

3. Définir collectivement les usages

Les technologies de sécurité présentent une sensibilité tout à fait particulière, en raison de leur impact sur les droits et libertés. Elles doivent donc faire l'objet d'un débat informé, lucide et raisonnable. Cependant, leur émergence s'inscrit dans une révolution technique plus large qui a des répercussions multiples sur la société dans son ensemble. Il est dès lors nécessaire d'ouvrir un large débat public sur les grandes innovations technologiques.

a) Comment organiser le débat public ?

Le mode participatif vise à impliquer directement les citoyens dans la conception, la mise en œuvre et l'évaluation des politiques publiques. D'une part, il permet de répondre à la demande démocratique des citoyens qui souhaitent s'impliquer davantage dans la conception des politiques publiques. D'autre part, il permet de renforcer l'acceptabilité des décisions publiques, en concertant en amont des représentants de la société civile. Le mode participatif est très institutionnalisé en France, contrairement aux États-Unis où il est davantage mobilisé comme un contre-pouvoir. Des dispositifs participatifs ont été rendus obligatoires au niveau local et au niveau national, par exemple en matière environnementale. Le mode participatif connait aujourd'hui un nouvel essor, avec la mobilisation croissante des outils numériques mais aussi la création des conventions citoyennes et l'instauration du tirage au sort.

Néanmoins la multiplication des dispositifs participatifs est insuffisante pour remobiliser les citoyens. Les résultats des élections régionales et départementales, au cours desquelles une abstention massive a été constatée (66, 73%), peuvent être interprétés comme le signe d'une désaffectation croissante des Français vis-à-vis de la démocratie représentative. On constate que la démocratie participative reproduit peu ou prou les mêmes problématiques. Le Cevipof a notamment constaté que les participants au Grand débat national ont une moyenne d'âge de 60 ans et sont à 65% des diplômés de l'enseignement supérieur(100). Les citoyens ne disposent pas du même intérêt pour le débat public, ni des mêmes ressources communicationnelles(101).

La participation des citoyens doit être structurée par les corps intermédiaires et objectivée par la communauté scientifique. Les corps intermédiaires, en tant que représentants de la société civile, peuvent venir jouer le rôle de facilitateur auprès des citoyens qui souhaitent participer au débat public. Les représentants de la communauté scientifique exposent des arguments objectifs afin d'éclairer le débat public. La classe politique tranche en fonction des arguments qui lui sont présentés afin de définir les usages des technologies de sécurité qui sont acceptables dans une société démocratique, et ceux qui doivent être écartés.

b) Associer les citoyens à la définition des usages

Les ateliers collaboratifs, qui ont pour objectif de comprendre les contraintes et les attentes du public sur un dispositif, peuvent être menés dans le cadre des expérimentations sur les technologies. Les ateliers collaboratifs permettent de prendre en compte le regard et les attentes des usagers. Ils sont précédés d'une étude quantitative ou qualitative qui pose les

(100) https://www.sciencespo.fr/cevipof/fr/content/lobservatoire-des-debat-0.html
(101) Source : CNNum.

enjeux et alimente les débats et peuvent éventuellement aboutir sur une évaluation ou un questionnaire qui mesure le ressenti des usagers. Un laboratoire d'usage peut, par exemple, venir jouer le rôle d'un tiers de confiance dans les expérimentations sur les technologies.

Les consultations en ligne peuvent permettre de recueillir l'avis du public sur les textes qui portent sur les technologies tout en mobilisant peu de moyens. La captation d'un large public donne une légitimité plus importante à la décision publique mais elle écarte les personnes éloignées du numérique et peut être phagocytée par des groupes d'intérêts qui sont amenés à s'emparer du sujet. La consultation peut être un facteur de succès pour le ministère qui porte le projet si elle s'inscrit dans le calendrier du gouvernement et est portée politiquement.

Encadré : la consultation sur le projet de loi pour une République numérique

La consultation, initiée en 2015 par le secrétariat d'État au numérique, a été lancée pour alimenter le projet de loi pour une République numérique. Les citoyens pouvaient voter sur les articles de l'avant-projet de loi ou déposer des contributions, en vue de les modifier ou proposer de nouveaux articles. Cette discussion publique, ouverte et interactive en ligne a conduit à la présentation de cinq nouveaux articles et de 90 modifications issues de la consultation, avant l'envoi du texte au Conseil d'État et son adoption en Conseil des ministres.

Le lancement d'un débat public sur les nouvelles technologies est l'occasion de créer, avec les citoyens, un cadre de réflexion et de dialogue sur les grandes innovations numériques. Les citoyens sont formés sur le sujet par des experts et fournissent un avis éclairé construit collectivement, qui vient appuyer la décision publique et limite les contestations. Cette forme de mobilisation peut être retenue si le gouvernement décide de lancer un débat approfondi sur l'usage des nouvelles technologies, qui comme l'I.A. posent des choix de société. Les lois de bioéthiques offrent un modèle intéressant qui, sans être intégralement reproductible, peut servir d'inspiration à des lois « *techno-éthiques* ». Elles constitueraient le cadre de révision des emplois des grandes innovations numériques.

Encadré : les États généraux de la bioéthique

La France est pionnière en matière de législation dans le domaine de la bioéthique depuis 1988. La loi de 2011 a prévu que tout projet de réforme sur les problèmes éthiques et les questions de société qui sont soulevés par les progrès de la connaissance dans les domaines de la biologie, de la médecine et de la santé doit être précédé d'un débat public sous forme d'états généraux organisés à l'initiative du Comité consultatif national d'éthique (CCNE)[102].

Les États généraux qui se sont tenus en 2018 ont notamment mobilisé des espaces de réflexion éthique régionaux, un site participatif, des comités d'éthique institutionnels et des experts, un comité citoyen et un médiateur auprès duquel les citoyens pouvaient déposer des réclamations[103].

c) Conduire une réflexion sur le long terme sur le modèle des lois de bioéthiques

Les corps intermédiaires peuvent conduire une réflexion de long terme sur les nouvelles technologies en structurant la participation citoyenne. Le Conseil économique social et environnemental (CESE) a, par exemple, en tant que représentant des corps intermédiaires, la possibilité de mobiliser directement les citoyens au travers du tirage au sort et par la voie de la pétition. Sa prochaine mandature pourrait en partie être consacrée au suivi des nouvelles technologies.

(102) Article L1412-1-1 du code de la santé publique.
(103) Les États généraux de la bioéthique 2018, Comité consultatif national d'éthique.

Encadré : la modernisation du Conseil économique, social et environnemental

La loi organique du 15 janvier 2021 a réformé le fonctionnement du Conseil économique, social et environnemental. Depuis plusieurs années, celui-ci nourrit ses travaux avec des dispositifs de participation citoyenne. Il a organisé la Convention citoyenne pour le Climat. Désormais il pourra être saisi, soit par le gouvernent, soit par 150 000 citoyens. Il enrichit ses avis, en associant directement les citoyens par la voie de la pétition et du tirage au sort. Le CESE pourrait intégrer prochainement la dimension numérique à ses travaux, lors de la conférence des enjeux, mais aussi créer une commission temporaire pour suivre l'évolution des technologies qui ont dans le domaine de la sécurité un impact sur les libertés publiques[104].

La communauté scientifique peut dresser un état de l'art régulier des grandes avancées scientifiques et formuler des recommandations pour éclairer le débat public. Associant les experts et la société civile organisée, les conférences de consensus ont beaucoup été utilisées dans le domaine de la santé, principalement par la Haute Autorité de Santé. Elles permettent de faire dialoguer les experts, les acteurs publics et le grand public autour d'enjeux considérés comme décisifs sur le plan scientifique. En s'appuyant sur les connaissances scientifiques et en permettant un débat structuré, une telle méthode doit aboutir à la construction d'un socle de consensus susceptible de poser les bases d'une évolution de la politique publique. Le numérique se caractérise par des avancées technologiques très rapides et une littérature universitaire abondante. Cela justifie une synthèse des informations disponibles et une prise de position de la communauté scientifique. Différentes instances, comme le Comité national pilote d'éthique du numérique (CNPEN) mais aussi le Conseil national du numérique (CNNum), peuvent venir jouer ce rôle d'animation et de structuration du débat scientifique sur les grandes innovations techniques.

Recommandation :

Associer les citoyens à la conception et à la mise en œuvre des politiques publiques dans le domaine de la sécurité en recourant à des ateliers participatifs lors des expérimentations et en organisant des consultations publiques en amont de la présentation des projets de texte.

Lancer un débat public sur les grandes innovations technologiques sur le modèle des lois bioéthiques afin d'apprécier les conséquences des évolutions techniques sur les libertés en mobilisant les corps intermédiaires et la communauté scientifique.

C. Superviser l'action des forces de sécurité

La mise en place de dispositifs d'évaluation et de contrôle constitue une garantie importante pour les forces de sécurité intérieure, lorsqu'elles emploient des technologies de sécurité. C'est à la fois un gage d'efficacité et d'acceptabilité. L'évaluation vise à mesurer l'efficacité des technologies qui sont employées et, plus largement l'action des forces de sécurité. Le contrôle permet de vérifier à chaque étape de la procédure, si l'action des forces de sécurité est légale. Néanmoins, les moyens d'évaluation et de contrôle ne doivent pas faire obstacle à l'action des forces de sécurité intérieure. Des évaluations et des contrôles trop nombreux, avec des délais importants, constitueraient une contrainte qui briderait l'action des forces de sécurité. Il faut déterminer les conditions de leur articulation avec les nécessités de sécurité publique.

(104) Source : CESE.

1. Les évaluations

a) *Les évaluations techniques et opérationnelles*

Les forces de sécurité auto-évaluent l'efficacité technique et opérationnelle des dispositifs qu'elles emploient. Les expérimentations leur permettent notamment d'éprouver l'efficacité technique des technologies, et d'en évaluer l'intérêt par rapport à leur coût[105]. Elles sont essentielles pour déterminer si les technologies présentent un avantage réel aux forces, mais aussi pour vérifier les capacités, l'endurance des technologies et les possibilités pour des opérations d'ampleur. Elles font l'objet d'une évaluation pour décider de leur usage pérenne.

Les forces de sécurité sont amenées à prendre en compte la prévention des risques. D'une part, elles doivent intégrer des exigences en matière de cybersécurité. L'ANSSI recommande notamment de réaliser des analyses de risques cyber, en amont de l'intégration des nouvelles technologies[106]. D'autre part, les forces de sécurité doivent intégrer de nouvelles exigences en matière d'auditabilité des algorithmes.

Encadré : l'audit des algorithmes

Le député Cédric Villani, dans son rapport sur l'intelligence artificielle, préconise d'accroître l'auditabilité des systèmes d'I.A. : « *À long terme, l'explicabilité de ces technologies est l'une des conditions de leur acceptabilité sociale. S'agissant de certains sujets, c'est même une question de principe : on ne peut admettre, en tant que société, que certaines décisions importantes puissent être prises sans explication* »[107].

La question de l'audit des algorithmes implique de nombreux acteurs. La CNIL est compétente pour opérer des contrôles sur les traitements de données à caractère personnel, y compris les éventuels algorithmes qu'ils pourraient contenir[108]. Mais des organismes privés peuvent aussi intervenir dans ce domaine, afin d'auditer ou certifier des algorithmes dans une optique de gestion de la qualité. Ainsi, le Laboratoire national de métrologie et d'essais (LNE) travaille sur un référentiel de certification[109], et l'AFNOR travaille à la réalisation de normes dans ce domaine, qui pourraient ensuite servir de base à des certifications attribuées après une phase d'audit.

Le projet de règlement sur l'intelligence artificielle de la Commission européenne prévoit une évaluation de la conformité des systèmes d'IA à haut risque. Il confie la mission de réguler les systèmes d'IA à des entités publiques. Dans certains cas, les systèmes d'IA devront faire l'objet d'une évaluation des risques réalisée par un tiers indépendant, qui devra donc auditer leur fonctionnement.

Pour Sébastien Louradour, *Fellow* au World Economic Forum : « *Il s'agit davantage de certifier la qualité des processus plutôt que la performance des algorithmes dans le règlement IA.* » La Commission européenne ne détaille aucun seuil de performance à respecter, mais requière en revanche l'obligation de fournir une documentation portant sur les processus mis en œuvre[110]. Il faut expliquer la méthodologie, pas le fonctionnement technique de l'algorithme[111].

Recommandation :

Intégrer la prévention des risques dans les évaluations techniques et opérationnelles qui sont réalisées par les forces de sécurité intérieure.

(105) https://www.gendarmerie.interieur.gouv.fr/crgn/publications/revue-de-la-gendarmerie-nationale/revue-n-267
(106) Source : ANSSI.
(107) Donner un sens à l'intelligence artificielle, rapport de la mission du député Cédric Villani, mars 2018.
(108) Source : CNIL.
(109) https://www.lne.fr/fr/actualites/ia-appel-public-commentaires-referentiel-certification
(110) Source : Sébastien Louradour Fellow, Artificial Intelligence and Machine Learning au World Economic Forum.
(111) Source : Pr. Erwan Le Pennec, professeur Ecole Polytechnique.

b) L'évaluation des politiques publiques

L'action des forces de sécurité intérieure pourrait être mieux évaluée en amont et en aval, notamment lorsqu'elles mobilisent des technologies de sécurité qui touchent à certains droits fondamentaux. L'évaluation en amont des besoins des forces par le biais des études d'impact et des avis qui sont rendus sur les textes est essentielle, de même que l'évaluation en aval de l'action des forces par les inspections.

En amont, les besoins des forces de sécurité intérieure pourraient être mieux évalués, en renforçant les études d'impact et les avis qui sont rendus sur les textes. Les propositions de loi ne sont pas suffisamment évaluées, en l'absence de dispositions contraignantes : elles ne font pas l'objet d'une étude d'impact, et ne sont pas systématiquement soumises pour avis au Conseil d'État et à la CNIL(112). Malgré l'existence de dispositions contraignantes, les projets de loi restent insuffisamment évalués. Ils sont accompagnés d'une étude d'impact, sont transmis au Conseil d'État et dans certains cas à la CNIL lorsque les dispositions sont relatives à la protection des données personnelles(113). Mais dans les faits, la qualité des études d'impact est très hétérogène et le temps consacré à l'examen des textes est insuffisant pour que le Parlement contre-expertise les études d'impact du gouvernement(114).

Recommandation :

Il est nécessaire de mieux évaluer en amont les besoins des forces de sécurité en renforçant les études d'impact et les avis qui sont rendus sur les textes. Cela implique de prévoir des délais suffisants pour l'examen des textes dans le respect des prérogatives du Parlement. Il est possible de solliciter en pratique de manière systématique l'avis du Conseil d'État sur les propositions de loi conformément à l'article 39 de la constitution. Il est souhaitable d'étendre le champ des études d'impact aux propositions de loi. Cette possibilité n'existant pas d'un point de vue légal, il serait intéressant de solliciter à droit constant l'avis du CESE ou d'organismes consultatifs indépendants afin qu'ils participent à un type nouveau d'évaluation préalable de la proposition de loi(115). Une autre option serait de permettre au rapporteur du texte parlementaire de commander des évaluations ex ante à des universités ou organismes publics de recherche afin de compléter le rapport accompagnant le projet de texte(116).

En aval, les inspections pourraient être plus sollicitées afin d'évaluer plus spécifiquement l'emploi des nouvelles technologies par les forces de sécurité intérieure. Le déploiement des technologies de sécurité entraîne un volume de dépense important alors que les résultats sont dans certains cas difficiles à évaluer. La Cour des comptes, dans son rapport sur les polices municipales, recommande d'évaluer l'efficacité de la vidéoprotection dans la prévention de la délinquance et l'élucidation des délits, avec le concours de chercheurs et d'experts reconnus.

(112) Article 39 de la constitution : le Président de l'Assemblée et le Président du Sénat peuvent solliciter l'avis du Conseil d'état sur les propositions de loi. Article 8 de la loi ILF : La CNIL peut être consultée par le Président de l'Assemblée, par le Président du Sénat ou par les commissions compétentes sur les propositions de loi relatives à la protection de données personnelles.
(113) Article 8 de la loi organique du 15 avril 2009, article 39 de la constitution et article 8 de la loi ILF.
(114) Étude d'impact, mieux évaluer pour légiférer, CESE, septembre 2019.
(115) Ibidem.
(116) Ibidem.

Encadré : l'absence d'évaluation des dispositifs de vidéoprotection

La Cour des comptes, dans son rapport de 2020 sur les polices municipales, revient sur le développement des caméras de surveillance sur la voie publique[117]. Elle rappelle l'évolution croissante du nombre de centres de supervision urbain, et du nombre de communes dotées de dispositifs de vidéoprotection. Elle souligne que la vidéoprotection et les caméras piétons sont des dispositifs coûteux pour lesquels les communes disposent d'aides de l'État, de la région et du département. Elle constate enfin que l'efficacité de la vidéoprotection n'est pas suffisamment mesurée : « *Au vu des constats locaux résultant de l'analyse de l'échantillon de la présente enquête, aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation* ». En ce sens, elle recommande d'engager une évaluation de l'efficacité de la vidéoprotection sur la voie publique, notamment dans l'élucidation des crimes et des délits avec le concours de chercheurs et d'experts (SGMI, DCS, DACG). L'ampleur des sommes engagées impose une appréciation objective de l'efficacité de la vidéoprotection.

Recommandation :

Solliciter, de manière plus systématique les inspections afin d'évaluer le recours aux technologies de sécurité. Des chercheurs et des experts pourront être associés au processus d'évaluation.

2. Les procédures et les autorités de contrôle

a) Renforcer les procédures administratives

La première solution consiste à moderniser le cadre applicable à la vidéoprotection tout en en élargissant le périmètre. L'installation d'un système de vidéoprotection est soumise à la réalisation d'une analyse d'impact relative à la protection des données auprès de la CNIL[118] et à l'autorisation du préfet[119]. Les commissions départementales de vidéoprotection rendent un avis au préfet avant la mise en place d'un système de vidéoprotection. Elles sont instituées par arrêté et sont composées de quatre membres : un magistrat, un maire, un représentant de la chambre de commerce et une personnalité qualifiée[120]. La commission nationale de la vidéoprotection rend des avis sur toute question relative à la vidéoprotection, et sur les projets d'actes réglementaires et législatifs[121]. Les municipalités peuvent disposer d'un comité d'éthique sur la vidéoprotection, comme c'est le cas à Paris[122]. La commission nationale de vidéoprotection et les commissions départementales pourraient être renforcées et voir leur périmètre élargi à d'autres technologies de recueil d'images pérennes.

La seconde solution consiste à contrôler *a posteriori* l'emploi des technologies, en nommant un référent membre du conseil d'État sur le modèle des fichiers GIPASP et PASP. Le GIPASP et le PASP sont deux fichiers relatifs à la prévention des atteintes à la sécurité publique qui sont tenus respectivement par la gendarmerie et la police nationales. Un référent national est chargé de veiller à l'application des dispositions concernant les mineurs. Il formule chaque année des recommandations, qui font l'objet d'un rapport public. L'intervention du référent national est prévue aux articles R236-15 et R236-26 du CSI. Une équipe de référents-adjoints lui apporte son concours. Le référent national et ses adjoints exercent leurs missions sans préjudice de la CNIL, qui peut être saisie par la procédure d'accès indirecte aux données personnelles. Sur le modèle du référant PASP/ GIPASP, un référent membre du Conseil d'État pourrait être nommé pour contrôler a posteriori l'emploi des technologies de sécurité.

La troisième solution consiste à renforcer le droit d'accès indirect (DAI), qui permet aux

(117) Les polices municipales, Cour des comptes, octobre 2020.
(118) Article L252-1 du CSI.
(119) Article 35-3 c) du RGPD.
(120) Article R251-8 du CSI.
(121) Article R251-1 à -5 du CSI.
(122) Charte d'éthique de la vidéoprotection à Paris

citoyens de saisir la CNIL pour accéder aux informations qui les concernent dans plusieurs fichiers intéressant la sûreté de l'État, la défense et la sécurité publique[123]. Ce droit s'exerce par le truchement d'un commissaire de la CNIL, par ailleurs magistrat, qui est chargé d'entrer en contact avec les organismes qui gèrent les fichiers pour ensuite communiquer les informations à la personne concernée. Le droit d'accès indirect pourrait être renforcé, en donnant plus de moyens juridiques et techniques au commissaire de la CNIL[124].

La quatrième solution est de créer l'équivalent du Forensic Science Regulator, Biometrics and Surveillance Camera Commissioner qui existe au Royaume-Uni. Rattaché au ministère de l'Intérieur, il est notamment chargé d'assurer le respect par les forces de sécurité des règles relatives à la collecte et la conservation de l'ADN, des empreintes digitales et des caméras de surveillance. Son rôle est prévu par le *Protection of Freedom Act* de 2012[125]. Ses missions portent à la fois sur les données biométriques mais aussi sur les dispositifs de vidéoprotection. Une seule personne assure désormais ces deux missions qui ont été confiées à Fraser Sampson en 2021[126]. Une telle autorité pourrait être mise en place en France, tout en prenant en compte le fait qu'il existe des différences significatives entre les deux pays en termes de déploiement et de régulation des technologies de sécurité.

Encadré : la reconnaissance faciale dans l'espace public au Royaume-Uni

Contrairement à la France, les outils de reconnaissance faciale ont été utilisés au Royaume-Uni à grande échelle, sur la base de vraies bases de données biométriques, pour des usages dans l'espace public [127]. En 2019, des passants ont été filmés à leur insu dans le quartier de King's Cross par un promoteur immobilier qui communiquait ces informations à la police, afin d'identifier des personnes recherchées. L'autorité britannique de protection des données enquête en ce moment sur ce cas d'espèce. Plus généralement, l'opinion publique britannique semble rétive à l'utilisation de la reconnaissance faciale : 55 % des citoyens interrogés souhaitent des restrictions sur l'utilisation de ces technologies par les forces de police selon une étude réalisée par l'Ada Lovelace Institute. Un conseil délibératif citoyen a depuis été créé.

Recommandation :

A court terme, renforcer les procédures qui encadrent l'emploi des technologies de sécurité par les forces et les élargir, quand cela est possible, à d'autres technologies de sécurité. A plus long terme, envisager la mise en place d'un *Forensic Science Regulator*, *Biometrics and Surveillance Camera Commissioner* sur le modèle britannique.

b) Augmenter les moyens des autorités de contrôle

Il s'agit, d'une part, de renforcer les moyens qui sont alloués à la CNIL, afin qu'elle puisse réaliser ses missions à périmètre constant. Les effectifs de la CNIL sont aujourd'hui en deçà de ce qui serait nécessaire, pour absorber l'ensemble des missions qui lui ont été confiées par le législateur national et européen. Avec 245 ETP en 2021, la taille de ses effectifs est inférieure à celle de ses homologues européens. L'autorité allemande de protection dispose de 1 000 personnes à périmètre constant[128]. Le ratio entre le nombre d'agents de la CNIL et le nombre d'habitants est le 3eme ratio le plus bas d'Europe[129]. Les besoins en ressources humaines de la

(123) Selon la nature des fichiers de police, de gendarmerie ou de renseignement, la procédure n'est pas la même. Par exemple, pour le fichier TAJ les personnes disposent sur le fondement du décret n°2018-687 du 1er août 2018, d'un droit d'accès et de rectification direct : elles doivent adresser leur demande au ministère de l'Intérieur et non plus à la CNIL. Plus d'info : https://www.cnil.fr/fr/le-droit-dacces-aux-fichiers-de-police-de-gendarmerie-et-de-renseignement

(124) Source : Renaissance numérique.

(125) Section 20 et section 34 du *Protection of Freedom Act*.

(126) https://videosurveillance.blog.gov.uk/2021/03/18/appointment-of-professor-fraser-sampson-the-new-biometrics-and-surveillance-camera-commissioner/

(127) Encadrement des technologies de reconnaissance faciale : Une approche comparée de la France et du Royaume-Uni, Renaissance numérique, juin 2020.

(128) Source : CNIL.

(129) Ibidem.

CNIL doivent être évalués, afin qu'elle puisse effectuer ses missions, notamment en matière d'accompagnement des entreprises et de *compliance*. Il serait également souhaitable qu'elle traite plus rapidement les demandes d'autorisation des acteurs publics, lorsqu'ils souhaitent réaliser une expérimentation, notamment lorsqu'il s'agit d'opérateurs d'importance vitale ou d'opérateurs de services essentiels qui participent aux missions de sécurité. Enfin, la CNIL pourrait envisager de renforcer la procédure de droit d'accès indirect.

Il s'agit, d'autre part, de renforcer l'efficacité de la chaîne pénale, en créant un parquet spécialisé. La chaîne pénale et la formation des magistrats sont inadaptées pour appréhender certains enjeux soulevés par les technologies de sécurité. Les limites actuelles auxquelles les magistrats sont confrontés pour lutter contre la cybercriminalité ressemblent à celles qui existaient en matière économique et financière, avant la création du Parquet National Financier : aggravation et complexification de la délinquance, absence d'interlocuteur précisément déterminé au niveau national et international, formation insuffisante des magistrats, insuffisance des moyens humains et techniques(130). La spécialisation des magistrats, et de l'ensemble de la chaîne pénale, permettrait au système judiciaire de traiter plus efficacement les infractions complexes commises dans le domaine cyber. Alors qu'un nouveau pôle national de lutte contre la haine en ligne a été créé au tribunal judiciaire de Paris en application de la loi Avia, le gouvernement pourrait étudier la création d'un parquet national cyber élargi disposant de ressources et des expertises suffisantes pour instruire les dossiers liés aux affaires de cyber délinquance les plus complexes(131).

Recommandation :

Évaluer les besoins en ressources humaines de la CNIL afin qu'elle puisse accompagner les entreprises et les administrations dans leurs démarches d'expérimentation, en priorisant si nécessaire les demandes d'autorisation à caractère prioritaire (ex : État, OIV, opérateurs de services essentiels). Étudier la création d'un parquet national cyber élargi, disposant de ressources et des expertises suffisantes pour instruire les affaires de cyber délinquance les plus complexes.

(130) Source : Me A. Basdevant.
(131) Avis du CNSP sur la sécurité numérique, avril 2021.

Liste des sigles

ADP	Aéroports de Paris
AFNOR	Association française de normalisation
AIPD	Analyse d'impact relative à la protection des données
AMD	Administrateur ministériel des données
ANR	Agence nationale de la recherche
ANSSI	Agence nationale de la sécurité des systèmes d'information
API	*Application Programming Interface*
CADA	Commission d'accès aux documents administratifs
CCNE	Comité consultatif national d'éthique
CDFUE	Charte des droits fondamentaux de l'Union européenne
CEA	Commissariat à l'énergie atomique et aux énergies alternatives
CEDH	Convention de sauvegarde des droits de l'Homme et des libertés fondamentales
CEPD	Comité européen de la protection des données - *European Data Protection Board*
CEPD	Contrôleur européen de protection des données - *European Data Protection Supervisor*
CESE	Conseil économique, social et environnemental
CITP	Comité intermistériel de la transformation publique
CNCDH	Commission nationale consultative des droits de l'Homme
CNIA	Coordinateur national pour l'intelligence artificielle
CNIL	Commission nationale de l'informatique et des libertés
CNNum	Conseil national du numérique
CNPEN	Comité national pilote d'éthique du numérique
CNRLT	Coordination nationale du renseignement et de la lutte contre le terrorisme
CNRS	Centre national de la recherche scientifique
CNSJ	Coordination nationale pour la sécurité des jeux
CNSP	Commission supérieure du numérique et des postes
CRPA	Code des relations entre le public et l'administration
CSI	Code de la sécurité intérieure
CSF-IS	Comité stratégique de filière « industries de sécurité »
DAI	Droit d'accès indirect
DDHC	Déclaration des droits de l'homme et du citoyen
DGGN	Direction générale de la gendarmerie nationale
DGPN	Direction générale de la police nationale
DGSCGC	Direction de la sécurité civile et de la gestion des crises
DGSI	Direction générale de la sécurité intérieure
DIJOP	Délégation interministérielle aux jeux olympiques et paralympiques
DINUM	Direction interministérielle du numérique
Directive NIS	Directive *Network and Information Security*

DITP	Direction interministérielle de la transformation publique
DLPAJ	Direction des libertés publiques et des affaires juridiques
DNUM	Direction du numérique
DPSIS	Délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité
DUDH	Déclaration universelle des droits de l'homme
EDRI	*European Digital Rights*
FEM	Forum économique mondial - *World Economic Forum*
FPR	Fichier des personnes recherchées
GIPASP	Fichier de Gestion de l'information et prévention des atteintes à la sécurité publique
HAS	Haute autorité de santé
HDH	*Health Data Hub*
IA	Intelligence artificielle
IFL	Loi Informatique, Fichiers et Libertés
IGN	Institut national de l'information géographique et forestière
IHEDN	Institut des hautes études de défense nationale
INRIA	Institut national de recherche en sciences et technologies du numérique
JOP	Jeux olympiques et paralympiques
LDH	Ligue des droits de l'Homme
LNE	Laboratoire national de métrologie et d'essais
MOOC	*Massive Open Online Course*
NIST	*National Institute of Standards and Technology*
OIV	Opérateurs d'importance vitale
OSE	Opérateurs de services essentiels
PARAFE	Passage automatisé rapide aux frontières extérieures
PASP	Fichier de prévention des atteintes à la sécurité publique
PLF	Projet de loi de finances
RATP	Régie autonome des transports parisiens
RGPD	Règlement général sur la protection des données
RPUE	Représentation permanente de la France auprès de l'Union européenne
RRF	Programme réseau radio du futur
SGDSN	Secrétariat général de la défense et de la sécurité nationale
SNCF	Société nationale des chemins de fer français
STSI2	Services des technologies et des systèmes d'information de la sécurité intérieure
SWP	*South Wales Police*
TAJ	Fichier de traitement d'antécédents judiciaires

Annexes

ANNEXE 1 : LETTRE DE MISSION

Le Premier Ministre

-543/21 SG

Paris, le 23 AVR. 2021

Monsieur le député,

Démocratisées dans leur usage du quotidien, les nouvelles technologies (intelligence artificielle, analyse automatisée des données, des images et des vidéos, drones, etc…) offrent de nombreuses perspectives aux acteurs publics, à explorer notamment dans le champ des missions de sécurité. Cependant, leur utilisation soulève alors des enjeux de libertés individuelles et publiques et peut susciter des craintes.

À l'aube de grands évènements organisés par la France, comme la coupe du monde de rugby en 2023 ou les jeux Olympiques et Paralympiques en 2024, et alors que la France possède des fleurons industriels reconnus sur le secteur des technologies de sécurité, je souhaite vous confier le soin d'identifier le moyen de faire bénéficier l'État de ces nouvelles capacités, tout en veillant aux garanties à mettre en place pour encadrer strictement leur usage.

Dans cet objectif, vous examinerez en premier lieu quelles pourraient être les opportunités et vous détaillerez les objectifs concrets et opérationnels de l'utilisation de ces nouvelles technologies et les gains réellement attendus.

Vous définirez les grands principes qui devraient accompagner un recours accru à ces nouvelles technologies de sécurité. Afin d'en limiter le caractère intrusif et préserver les libertés individuelles et publiques, la mission pourra ainsi réfléchir à un cadre d'emploi cohérent pour ces technologies.

La mission éclairera également la réflexion sur la façon dont les usages pourraient être définis collectivement avec la société civile, ab initio, afin d'adopter une approche la plus inclusive possible qui répondrait à des besoins plébiscités par les citoyens. Elle proposera également des pistes pour une réflexion apaisée dans la durée sur la possibilité de favoriser l'usage transparent de ces technologies, permettant d'en questionner régulièrement le recours au fur et à mesure que la technologie elle-même et ses usages se développeront. Enfin, elle indiquera si les moyens de contrôle actuels lui paraissent suffisants, ou s'il conviendrait d'en mettre en place de nouveaux pour accompagner le développement des usages, en tenant compte du paysage institutionnel existant (conseil national du numérique, comité pilote d'éthique du numérique et de l'intelligence artificielle, etc.).

…/…

Monsieur Jean-Michel MIS
Député
Assemblée nationale
126, rue de l'Université
75007 PARIS

Au-delà de ces questions centrales et essentielles à un usage responsable et acceptable par la société des technologies de sécurité, je vous serais reconnaissant de bien vouloir m'éclairer sur deux thématiques spécifiques :

- la question de la responsabilité en cas de défaillance, notamment en cas de décision liée à une indication erronée de la technologie (erreur sur la personne identifiée, par exemple) ;

- la question de la souveraineté technologique française et européenne.

Enfin, à l'heure où la Commission européenne se saisit également d'une partie du sujet, il sera utile de disposer d'un point de situation sur les réflexions de quelques pays européens et des cadres qu'ils ont pu déjà adopter pour accompagner le recours à ces technologies sur leur territoire. Cet éclairage sera idéalement accompagné en miroir d'un point de situation sur les cadres et usages en vigueur dans des pays d'Amérique et d'Asie qui ont déjà fait le choix d'un recours très large aux nouvelles technologies.

Pour conduire cette mission, vous pourrez bénéficier du concours d'un haut fonctionnaire de l'inspection générale de l'administration.

Vous veillerez à élaborer vos recommandations dans le respect des règles d'indépendance, d'impartialité et d'objectivité qui s'imposent au titre de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique et à m'informer des éventuelles mesures prises à cet effet.

Un décret vous nommera, en application de l'article L.O. 144 du code électoral, parlementaire en mission auprès de M. Gérald Darmanin, ministre de l'intérieur.

Je souhaite disposer de votre rapport pour le 30 juin 2021.

Je vous prie de croire, Monsieur le Député, à l'assurance de mes sentiments les meilleurs.

Jean CASTEX

ANNEXE 2 : PERSONNES AUDITIONNEES

Maryse Artiguelong, Ligue des droits de l'Homme ● Stéphane Avigni, EuroDisney ● Didier Baichère, député ● Adrien Basdevant, avocat ● Alain Bauer, criminologue ● Thierry Beaudet, Conseil économique, social et environnemental ● Bilel Benbouzid, universitaire ● Côme Berbain, RATP ● Gérard Blondin, EuroDisney ● Marc Boget, ministère de l'intérieur ● Vincent Bouatou, Idemia ● Stéphane Bouillon, Secrétariat général de la défense et de la sécurité nationale ● Michel Cadic, ministère de l'intérieur ● Michel Cadot, délégation interministérielle aux jeux olympiques et paralympiques ● Thomas Campeaux, ministère de l'intérieur ● Didier Cannesson, Idemia ● Jean-Marie Cavada, IDFRights ● Adeline Champagnat, ministère de l'intérieur ● Agathe Cury, cabinet du ministre de l'Intérieur ● Olivier de Mazières, ministère de l'intérieur ● Christophe Delaye, délégation interministérielle aux jeux olympiques et paralympiques ● Thibault Deloye, délégation interministérielle aux jeux olympiques et paralympiques ● Laurent Denizot, Egidium technologies ● direction technique de la DGSI ● Pauline Dubarry, représentation permanente de la France auprès de l'UE ● Morgane Duval, Foot Unis ● David Foltz, ministère de l'intérieur ● Grégory Frély, cabinet du Premier ministre ● Jean-Gabriel Ganascia, universitaire ● Nicolas Goniak, représentation permanente de la France auprès de l'UE ● Stéphane Gouaud, RATP ● Stéphane Grasset, Atos ● Bénédicte Guitard, IDF-mobilités ● Benjamin Jean, Inno3 ● Yoann Kassianides, Alliance pour la confiance numérique ● Ziad Khoury, ministère de l'intérieur ● Philippe Laborie, Aéroports de Paris ● Guillaume Lambert, ministère de l'intérieur ● François-Xavier Lauch, cabinet du ministre de l'Intérieur ● Julien Laurent, RATP ● Erwan Le Pennec, universitaire ● Dominique Legrand, AN2V ● Jérôme Létier, ministère de l'intérieur ● Pierre Lieutaud, ministère de l'intérieur ● London Metropolitan Police ● Eric Marion, EuroDisney ● Fabrice Mattatia, ministère de l'intérieur ● Nicolas Nordman, Ville de Paris ● Laurent Nunez, coordination nationale du renseignement et de la lutte contre le terrorisme ● Yann Padova, avocat ● Aurélien Palix, ministère de l'économie ● Laurent Pellegrin, Idemia ● Bruno Poirier-Coutansais, ministère de l'intérieur ● Laurent Probst, IDF-mobilités ● Pierre Rabadan, Ville de Paris ● Yannick Ragonneau, One Point ● Franck Robine, cabinet du Premier ministre ● Christian Rodriguez, ministère de l'intérieur ● Elisabeth Rolin, ministère de l'intérieur ● Jacques Roujansky, CSF-IS ● Jérôme Séguy, Aéroports de Paris ● Elizabeth Sellos-Cartel, ministère de l'intérieur ● Sébastien Soriano, Institut national de l'information géographique et forestière ● Françoise Soulié, Hub IA ● Patrice Spinosi, avocat ● Olivier Tesquet, journaliste ● Alain Thirion, ministère de l'intérieur ● David Tortel, cabinet du ministre de l'Intérieur ● Frédéric Veaux, ministère de l'intérieur ● Renaud Vedel, coordinateur national pour l'IA ● Julien Vignon, ministère de l'économie ● Christian Vigouroux, comité d'éthique de la vidéo protection de Paris ● Mathieu Weill, ministère de l'économie

ANNEXE 3 : CONTRIBUTEURS

Agence nationale de la sécurité des systèmes d'information ● AN2V ● Alliance Police Nationale ● Alliance pour la confiance numérique ● Alternative Police-CFDT Interco ● Axon ● Commission nationale consultative des droits de l'Homme ● Commission nationale de l'informatique et des libertés ● Commission supérieure du numérique et des postes ● Comité stratégique de filière « industries de sécurité » ● Conseil national du numérique ● Cybercercle ● Datakalab ● Délégation interministérielle aux jeux olympiques et paralympiques ● Direction du numérique du ministère de l'intérieur ● Direction générale des entreprises du ministère de l'économie, des finances et de la relance ● Direction générale de la gendarmerie nationale ● Direction générale de la police nationale ● Direction générale de la sécurité civile et de la gestion des crises ● Fédération des Industries Électriques, Électroniques et de Communication ● Fédération Française de la Cybersécurité ● Fédération Française des Métiers de l'Incendie ● France 2023 Rugby ● IN Groupe ● Institut national de recherche en sciences et technologies du numérique ● M. Adrien Basdevant, avocat ● M. Claude Kirchner, Directeur du Comité national pilote d'éthique du numérique ● M. Daniel Le Coguic, Atos ● M. Didier Baichère, député ● Mme Françoise Soulié, Conseiller scientifique HUB IA ● M. Gérard Lacroix, GICAT ● M. Gilbert Réveillon, président du groupe d'expertise TIC et Économie Numérique au Comité National des Conseillers du Commerce Extérieur de la France et membres du réseau des CCEF ● M. Hervé Debar, Professeur, Télécom Sud-Paris, Institut Mines-Télécom ● M. Jean-Gabriel Ganascia, informaticien et philosophe ● M. Jean-Marie Cavada, président d'IDFrights ● Mme Laurane Raimondo, chercheure associée, Centre Lyonnais d'Études de Sécurité Internationale et de Défense ● M. Lilian Bossuet, Université Jean-Monnet ● M. Lionel Le Cleï, Thales ● Mme Manon Vermenouze, Shark Robotics ● Mme Mouna Mouncif-Moungache, Université Jean-Monnet ● M. Richard Lizurey, consultant ● M. Robin Rivaton, investisseur et essayiste ● M. Sébastien Louradour, Expert Technique International, Forum Économique Mondial ● M. Sébastien Soriano, directeur général de l'Institut national de l'information géographique et forestière ● M. Stéphane Grasset, Atos ● M. Thierry Berthier, Conseiller scientifique de la Fédération professionnelle européenne Drones4Sec ● M. Victor Vuillard, société Parrot ● M. Yannick Ragonneau, Atos ● Palantir France ● Renaissance numérique ● Secrétariat général de la défense et de la sécurité nationale ● Serenicity ● Syndicat des cadres de la sécurité intérieur ● Syndicat National des Personnels de Police Scientifique ● Thales ● Two-i