N° XXXX

—

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

SEIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 12 avril 2023

RAPPORT D'INFORMATION

DÉPOSÉ
en application de l'article 145 du Règlement

PAR LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE,

en conclusion des travaux d'une mission d'information [(1)]

sur les **enjeux** *de l'***utilisation** *d'***images** *de* **sécurité** *dans le* **domaine public** *dans une* **finalité** *de* **lutte** *contre l'***insécurité**

ET PRÉSENTÉ PAR

MM. PHILIPPE GOSSELIN ET PHILIPPE LATOMBE,

Députés

———

(1) La composition de cette mission figure au verso de la présente page.

La mission d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité est composée de MM. Philippe Gosselin et Philippe Latombe, rapporteurs.

SOMMAIRE

—

MESDAMES, MESSIEURS,

Le premier cadre juridique régissant la captation d'images sur le domaine public a été créé par la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. Depuis, la vidéoprotection s'est largement répandue. Initialement objet de méfiances, parfois source de fantasmes, l'utilisation de caméras fixes et mobiles suscite aujourd'hui une large adhésion de la population. Les forces de l'ordre la présentent comme un outil désormais incontournable afin d'accomplir leurs missions.

Opérationnellement, les forces de l'ordre s'appuient à la fois sur les caméras fixes installées par les municipalités et par les opérateurs de transport, ainsi que sur les caméras mobiles, qu'elles soient individuelles, embarquées ou aéroportées. À chaque vecteur de captation est associé un encadrement juridique spécifique, qui précise les finalités pour lesquelles il est utilisé, la durée de conservation des données ou le droit d'accès des personnels aux enregistrements. Produit d'une sédimentation législative et règlementaire de près de trente ans, il en découle un cadre juridique fragmenté, non seulement complexe mais aussi inadapté aux évolutions technologiques survenues au cours de la dernière décennie. La CNIL a rappelé le 19 juillet 2022 que la loi française n'autorisait pas l'usage par la puissance publique de caméras dites « augmentées » pour la détection et la poursuite d'infractions.

Un premier pas a été franchi avec l'adoption du projet de loi relatif aux jeux Olympiques et Paralympiques de 2024, mais le cadre proposé n'est qu'expérimental. Or il n'est plus possible de faire l'autruche. Dans ce domaine, ne pas encadrer, c'est déjà faire un choix : celui de fermer les yeux sur le caractère inéluctable de l'intelligence artificielle et d'être pris de court à l'avenir lorsqu'il s'agira d'en encadrer l'usage.

Se retrancher derrière le seul constat d'un risque pour les libertés fondamentales, c'est se priver d'outils qui ne sont pas intrinsèquement mauvais et qui peuvent grandement aider nos forces de l'ordre dans leurs missions quotidiennes. Les jeux Olympiques et Paralympiques ne sont que la dernière illustration des défis auxquels sont confrontés les pouvoirs publics pour garantir la sécurité sur le territoire français : prévention du terrorisme, maintien de l'ordre public dans des villes particulièrement denses, lutte contre une criminalité férue de nouvelles technologies.

Aucun compromis ne doit être fait concernant la protection des libertés fondamentales. Des institutions comme la CNIL et le Conseil d'État, qui sont garantes de l'équilibre entre préservation de l'ordre public et respect du droit à la

vie privée, devront être associées à chaque étape du processus de construction juridique.

Ne pas encourager le développement de solutions françaises et européennes, c'est courir le risque d'être dépendant plus tard des logiciels développés par des puissances étrangères. Or, en matière d'intelligence artificielle, perdre la maîtrise, c'est fragiliser notre souveraineté.

La réticence de la population française vis-à-vis du recours à des logiciels d'intelligence artificielle ne doit pas être sous-estimée : l'une des réponses à y apporter est de garantir que les logiciels utilisés répondent à des critères rigoureux en termes de protection des données à caractère personnel.

La mission a organisé 47 auditions à Paris et entendu plus de deux cents intervenants de tous horizons, qu'il s'agisse des membres des forces de l'ordre, des représentants des ministères, des experts scientifiques, des acteurs associatifs, ou encore entreprises. Ils ont rencontré des élus défendant des positions différentes sur ces sujets, à Nice, Nantes et Cannes. Ils se sont rendus sur les sites connaissant de forts enjeux opérationnels : la maison de la Sûreté de la SNCF, le centre de commandement de l'aéroport Roissy-Charles-de-Gaulle. Enfin, soucieux de voir ce qui existe à l'étranger, ils se sont déplacés à Monaco et en Israël.

Vos rapporteurs ont d'emblée exclu la vidéosurveillance des lieux privés du champ de leur mission, considérant que les enjeux n'étaient pas les mêmes. Le choix a également été fait d'écarter la vidéosurveillance des lieux de privation de liberté, où les problématiques sont différentes de celles qui se posent dans l'espace public. À l'inverse, ils se sont penchés sur l'usage de la vidéoprotection par les opérateurs de transport, considérant que leurs emprises appartiennent au domaine public.

Au terme de six mois de travaux, la mission d'information formule 41 recommandations. Celles-ci portent sur les dispositifs de captation existants, mais esquissent également des pistes relatives aux caméras « augmentées » et à la reconnaissance biométrique. L'objectif est d'anticiper les évolutions pour mettre l'intelligence artificielle au service de la sécurité.

Vos rapporteurs souhaitent que ces recommandations puissent aboutir au dépôt d'une proposition de loi dont le Parlement devra débattre : il est urgent que la représentation nationale se saisisse de ces enjeux, alors même que les institutions européennes examinent la proposition de règlement européen sur l'intelligence artificielle. Il ne s'agit pas de prévoir un cadre rigide susceptible de devenir rapidement obsolète, mais bien de fixer, de façon souple et claire, les grands principes qui concourront à renforcer la sécurité de nos concitoyens, dans le respect des libertés fondamentales.

I. LE DÉVELOPPEMENT DES DISPOSITIFS DE CAPTATION D'IMAGES DANS L'ESPACE PUBLIC : UNE COURSE DE VITESSE PARSEMÉE D'EMBÛCHES

La loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité a élaboré le premier cadre régissant la captation d'images de sécurité dans l'espace public. Près de trente ans plus tard, les évolutions politiques, sociales et technologiques ont abouti à généraliser le recours à la vidéo afin de lutter contre l'insécurité. L'usage de caméras fixes ou mobiles suscite aujourd'hui un intérêt croissant des pouvoirs publics locaux et nationaux, ainsi qu'un large consensus parmi la population (1).

Cette acculturation progressive de la société aux outils de captation d'images s'est accompagnée d'un empilement de dispositions législatives et règlementaires destinées à encadrer les pratiques en la matière. Sous le contrôle étroit de la jurisprudence constitutionnelle et européenne, un subtil équilibre entre préservation de l'ordre public et respect du droit à la vie privée se dessine, alors que le déploiement de ces dispositifs se heurte, en pratique, à certaines difficultés juridiques et opérationnelles.

A. LA COMPLEXIFICATION DU RÉGIME JURIDIQUE À L'ÉPREUVE DES ÉVOLUTIONS TECHNOLOGIQUES

La multiplication des règles relatives à l'ensemble des dispositifs de captations d'images de sécurité dans l'espace public, qu'il s'agisse des caméras fixes ou mobiles, souligne la nécessité de clarifier et d'unifier ce régime juridique dans le code de la sécurité intérieure. Si l'utilisation croissante de ces outils par les forces de sécurité bénéficie d'un fort soutien financier, elle demeure confrontée à des enjeux opérationnels qu'il convient de surmonter.

1. Une sédimentation législative et règlementaire à la fois complexe et inachevée

Depuis 1995, le cadre légal de la captation d'images à des fins de lutte contre l'insécurité a fait l'objet de nombreuses évolutions. Outre les lois du 18 mars 2003 (2) et du 14 mars 2011 (3), qui ont respectivement autorisé l'usage des dispositifs de lecture automatique de plaques d'immatriculation (LAPI) et étendu le champ de la vidéoprotection, les lois du 3 juin 2016 (4), du 25 mai 2021 (5) et du

(1) Selon un sondage réalisé par l'IFOP en septembre 2013, 83 % des personnes interrogées approuvaient le recours à la vidéoprotection.

(2) Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

(3) Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

(4) Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

(5) Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés.

24 janvier 2022 (1) ont précisé les règles relatives à l'usage des caméras mobiles par les forces de l'ordre, qu'il s'agisse des caméras piétons, embarquées ou aéroportées.

Il en résulte une forme de « sédimentation législative » qui complexifie le régime juridique de la captation d'images prévu par le code de sécurité intérieure (CSI) (2), alors même que des mesures règlementaires d'application se font toujours attendre. Vos rapporteurs estiment qu'un effort de rationalisation doit être mené afin d'améliorer dès que possible la lisibilité et la cohérence des règles en vigueur.

a. Les caméras de vidéoprotection et de lecture automatisée de plaques d'immatriculation (LAPI)

i. Les caméras de vidéoprotection

Les articles L. 251-1 à L. 255-1 du CSI fixent les règles générales applicables à la vidéoprotection. Les articles L. 223-1 à L. 223-9 du même code complètent ces dispositions, s'agissant spécifiquement de la vidéoprotection mise en œuvre dans le cadre de la lutte antiterroriste.

« Vidéoprotection » et « vidéosurveillance »

Depuis la loi du 14 mars 2011, le terme de « vidéoprotection » correspond aux dispositifs fixes de captation d'images utilisés dans l'espace public. Il se distingue de la « vidéosurveillance », qui concerne les dispositifs installés dans les lieux non-ouverts au public. Bien que cette évolution sémantique, déjà ancienne, ne soit pas exempte d'arrière-pensées idéologiques (3), le présent rapport utilise ces termes conformément à leur acception juridique actuelle.

L'article L. 251-2 du CSI énumère les onze finalités pour lesquelles un dispositif de vidéoprotection peut être installé par une autorité publique, après autorisation préfectorale.

(1) Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure.

(2) Créé par l'ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure.

(3) Dans son étude intitulée « Les caméras au village *» publiée le 19 novembre 2021, le laboratoire d'innovation numérique de la Commission nationale de l'informatique et des libertés (CNIL) considère explicitement que «[…]* le choix de ce terme, qui se veut plus rassurant, répond à une logique de communication *» (p. 9).*

Finalités pour lesquelles la vidéoprotection peut être mise en œuvre selon l'article L. 251-2 du code de la sécurité intérieure

1° La protection des bâtiments et installations publics et de leurs abords ;

2° La sauvegarde des installations utiles à la défense nationale ;

3° La régulation des flux de transport ;

4° La constatation des infractions aux règles de la circulation ;

5° La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières prévues par le dernier alinéa de l'article 414 du code des douanes et des délits prévus à l'article 415 du même code portant sur des fonds provenant de ces mêmes infractions ;

6° La prévention d'actes de terrorisme, dans les conditions prévues aux articles L. 223-1 à L. 223-9 du code de la sécurité intérieure ;

7° La prévention des risques naturels ou technologiques ;

8° Le secours aux personnes et la défense contre l'incendie ;

9° La sécurité des installations accueillant du public dans les parcs d'attractions ;

10° Le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile ;

11° La prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets.

Depuis 1995, le Conseil constitutionnel a développé une jurisprudence relativement favorable au déploiement de la vidéoprotection. Les dispositions législatives soumises à son examen sont systématiquement appréhendées à travers la conciliation entre, d'une part, l'objectif à valeur constitutionnelle de prévention des atteintes à l'ordre public et, d'autre part, l'exercice du droit au respect de la vie privée découlant notamment de l'article 2 de la Déclaration des droits de l'Homme et du Citoyen de 1789 (1).

L'appréciation souveraine de cet équilibre par le Conseil constitutionnel implique un encadrement strict des modalités de recours et d'utilisation des caméras de vidéoprotection par les pouvoirs publics, tout en leur offrant une souplesse suffisante pour garantir l'opérationnalité de ces dispositifs.

Ainsi, un système de vidéoprotection ne saurait visualiser les images de l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées (2). Le public est informé de la mise en œuvre d'un tel système par

(1) Décisions n° 94-352 DC du 18 janvier 1995, n° 2003-467 DC du 13 mars 2003 et n° 2021-817 DC du 20 mai 2021.

(2) Article L. 251-3 du CSI.

l'apposition de panonceaux ou d'affiches et dispose d'un droit d'accès aux enregistrements qui le concernent (1).

L'installation des caméras, qu'elles soient fixes ou déplaçables, est soumise à une autorisation préfectorale, d'une durée de cinq ans, prise après avis de la commission départementale de vidéoprotection (2). L'autorisation peut prescrire que les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales, des douanes, des services d'incendie et de secours, des services de police municipale ainsi que les agents individuellement désignés et dûment habilités sont destinataires des images et enregistrements (3). Elle précise aussi les modalités de transmission des images et d'accès aux enregistrements, ainsi que la durée de conservation des images, dans la limite d'un mois (4) à compter de cette transmission ou de cet accès – sans préjudice des nécessités de leur conservation pour les besoins d'une procédure pénale.

Selon les chiffres communiqués à vos rapporteurs par la délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité (DPSIS) du ministère de l'Intérieur et des outre-mer, seules 26 816 des 42 387 demandes d'installation de caméras de vidéoprotection ont bénéficié d'une autorisation préfectorale en 2022, soit un taux d'acceptation de 63 % (5). **Ce résultat traduit la rigueur avec laquelle les services préfectoraux instruisent les dossiers qui leur sont soumis** (6), conformément aux dispositions légales et règlementaires prévues par le CSI.

Interrogé sur la lenteur supposée de la procédure d'autorisation (7), le Gouvernement a indiqué en mars 2022 ne pas souhaiter confier aux forces de l'ordre ou aux communes l'initiative d'installer des dispositifs de vidéoprotection sans l'intervention de l'autorité préfectorale (8).

Dans un objectif de réactivité, l'article L. 252-6 du CSI permet au préfet d'autoriser provisoirement une collectivité locale à mettre en œuvre un système de vidéoprotection en cas de tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens. Cette autorisation vaut pour une période

(1) Articles L. 251-3, L. 253-5 et R. 253-3 du CSI.

(2) L'article L. 251-4 du CSI précise que cette commission est présidée par un magistrat honoraire ou, à défaut, une personnalité qualifiée, nommée par le premier président de la cour d'appel. Elle est chargée de donner un avis au préfet sur les demandes d'autorisation de systèmes de vidéoprotection et d'exercer un contrôle sur les conditions de fonctionnement des systèmes autorisés.

(3) Article L. 252-3 du CSI.

(4) L'article L. 252-4 du CSI prévoit que l'autorisation préfectorale peut également fixer un délai minimal de conservation des images.

(5) En 2021, sur 45 511 demandes enregistrées en préfecture, 26 317 ont obtenu une autorisation, soit moins de 58 %.

(6) L'article R. 252-3 du CSI détaille le contenu du dossier administratif et technique joint à la demande d'autorisation.

(7) Le délai d'instruction s'élève en moyenne à deux mois.

(8) Réponse ministérielle du 1er mars 2022 à la question écrite n° 34027 du député Jean-Noël Barrot.

maximale de quatre mois [1]. Dans les mêmes conditions, le préfet peut également prescrire, sans l'avis préalable de la commission départementale de vidéoprotection, la mise en œuvre d'un système de vidéoprotection pour la seule durée de la manifestation [2]. En outre, l'article R. 252-3 du CSI a instauré la notion de périmètre vidéoprotégé. Au lieu d'autoriser l'installation d'une ou plusieurs caméras précisément situées, le préfet définit une zone « vidéoprotégée » par des caméras dont le nombre, l'implantation et les éventuels déplacements sont susceptibles d'évoluer au gré des besoins de l'autorité responsable.

Sur le fondement de l'article L. 253-2 du CSI, les caméras installées peuvent faire l'objet de contrôles par la commission départementale de vidéoprotection et la Commission nationale de l'informatique et des libertés (CNIL) [3]. Chaque dispositif doit satisfaire à certaines normes techniques définies par l'arrêté ministériel du 3 août 2007 afin de permettre l'exploitation des images par les forces de sécurité. L'article R. 252-13 du CSI rappelle les exigences de disponibilité, de confidentialité et d'intégrité des enregistrements, ainsi que la traçabilité des consultations des images.

En outre, l'article L. 254-1 du CSI réprime pénalement le non-respect de l'ensemble des règles précitées. Le fait d'installer un système de vidéoprotection ou de le maintenir sans autorisation, de procéder à des enregistrements sans autorisation, de ne pas les détruire dans le délai prévu, de les falsifier, d'entraver l'action de la commission départementale ou de la CNIL, de faire accéder des personnes non habilitées aux images ou d'utiliser ces images à d'autres fins que celles pour lesquelles elles sont autorisées est puni de trois ans d'emprisonnement et de 45 000 euros d'amende [4].

ii. Les lecteurs automatisés de plaques d'immatriculation (LAPI)

Autorisés par la loi n° 2003-239 du 18 mars 2003, les lecteurs automatisés de plaques d'immatriculation (LAPI) sont des systèmes intégrés à des caméras ayant pour objet de capturer et de traiter l'image des plaques d'immatriculation des véhicules [5] dans le but d'en extraire les informations correspondantes. Il s'agit principalement de dispositifs fixes installés sur la voie publique, placés sur des poteaux de signalisation ou des murs.

Traitements automatisés de données signalétiques des véhicules, les LAPI sont régis par les articles L. 233-1 à L. 233-2 du CSI. L'article L. 233-1 prévoit que les services de police et de gendarmerie nationales et des douanes peuvent installer

---

(1) La commission départementale de vidéoprotection en est informée aux fins de statuer sur son maintien.

(2) Article L. 252-7 du CSI.

(3) Selon les informations communiquées à vos rapporteurs, la CNIL reçoit chaque année 7 000 plaintes relatives au fonctionnement des dispositifs de vidéoprotection. Elle mène annuellement près de 600 contrôles sur le terrain.

(4) Sans préjudice des dispositions de l'article 226-1 du code pénal et des articles L. 1121-1, L. 1221-9, L. 1222-4 et L. 2323-47 du code du travail.

(5) Ces dispositifs permettent également de photographier le véhicule et ses occupants.

ces dispositifs en tous points appropriés du territoire, en particulier dans les zones frontalières, portuaires ou aéroportuaires ainsi que sur les grands axes de transit national ou international, selon plusieurs finalités limitatives :

– prévenir et réprimer le terrorisme ;

– faciliter la constatation des infractions criminelles ou liées à la criminalité organisée ;

– faciliter la constatation des infractions de vol et de recel de véhicules volés ;

– faciliter la constatation des infractions de contrebande.

Leur emploi est également autorisé par le préfet à l'occasion d'événements particuliers ou de grands rassemblements de personnes en vue de préserver l'ordre public. Une commune n'est pas autorisée à recourir aux LAPI quand bien même les données collectées seraient destinées à être mises à la disposition de la gendarmerie nationale à des fins d'aide à l'identification des auteurs d'infractions (1).

L'article L. 233-2 du CSI précise que les traitements comportent une consultation du traitement automatisé des données contenues dans le fichier des objets et des véhicules signalés (FOVeS) ainsi que dans le système d'information Schengen (SIS) (2). Les données collectées sont conservées pour une durée maximale de quinze jours, au-delà de laquelle elles sont effacées dès lors qu'elles n'ont donné lieu à aucun rapprochement positif avec les fichiers précités (3). Les données qui font l'objet d'un rapprochement positif avec ces mêmes traitements sont conservées pour une durée d'un mois, sans préjudice des nécessités de leur conservation pour les besoins d'une procédure pénale ou douanière.

b. Les caméras piétons, embarquées et aéroportées

Le titre IV du livre II du CSI encadre l'utilisation des caméras mobiles par les forces de l'ordre. Leur usage s'est fortement développé au cours de la dernière décennie, en l'absence de tout cadre légal jusqu'à la loi du 3 juin 2016 s'agissant des caméras piétons et à la loi du 24 janvier 2022 en ce qui concerne les caméras embarquées et aéroportées (4).

(1) Conseil d'État, Commune de Gujan-Mestras, *27 juin 2016.*

(2) Le SIS est une base de données commune dans laquelle les pays membres et associés à l'espace Schengen renseignent l'identité de personnes signalées.

(3) Durant cette période de quinze jours, la consultation des données n'ayant pas fait l'objet d'un rapprochement positif avec ces traitements est interdite, sans préjudice des nécessités de leur consultation pour les besoins d'une procédure pénale ou douanière.

(4) La loi du 24 janvier 2022 a tiré les conséquences de la censure par le Conseil constitutionnel des dispositions prévues par la loi du 25 mai 2021 relatives aux caméras embarquées et aéroportées.

i. Les caméras piétons

À l'issue d'une expérimentation jugée satisfaisante dans plusieurs zones de sécurité prioritaire depuis mai 2013 (1), la loi du 3 juin 2016 a fixé les règles applicables aux caméras piétons portées par les policiers et les gendarmes lors de leurs interventions. Ces dispositions ont été complétées par la loi du 25 mai 2021 (2) et par la loi du 24 janvier 2022, celle-ci se bornant à tirer les conséquences d'une réserve d'interprétation précédemment posée par le Conseil constitutionnel (3). En outre, la loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités a ouvert la possibilité aux agents assermentés des entreprises de transport d'expérimenter l'usage des caméras piétons, jusqu'au 1er juillet 2024 (4).

Le dispositif a été précisé au niveau règlementaire par les décrets n° 2022-605 du 21 avril 2022 et n° 2022-1395 du 2 novembre 2022 relatifs à la mise en œuvre de traitements de données à caractère personnel provenant des caméras piétons des gendarmes et des agents de la police nationale et de police municipale. Ces dispositions font également l'objet d'une doctrine d'emploi commune à la police et à la gendarmerie publiée le 28 octobre 2022.

L'article L. 241-1 du CSI précise que les agents de police et les gendarmes sont autorisés à procéder à l'enregistrement audiovisuel de leurs interventions dans des conditions et selon des finalités limitativement énumérées.

Premièrement, si la décision d'enregistrement appartient uniquement à l'agent, elle demeure conditionnée à l'existence potentielle ou avérée d'un incident, eu égard aux circonstances de l'intervention ou au comportement des personnes concernées par celle-ci. L'enregistrement, non-permanent, se matérialise par un signal visuel spécifique. Son déclenchement fait l'objet d'une information des personnes filmées, sauf si les circonstances l'interdisent.

Deuxièmement, les finalités du dispositif sont circonscrites à la prévention des incidents au cours des interventions, au constat des infractions et à la poursuite de leurs auteurs par la collecte de preuves, ainsi qu'à la formation et la pédagogie des agents.

Conformément à l'article R. 241-2 du CSI, les traitements de données issues des caméras piétons font apparaître les informations suivantes :

– les images et les sons captés ;

– le jour et les plages horaires d'enregistrement ;

---

(1) Des usages expérimentaux et très localisés avaient également eu lieu en 2008 et 2009.

(2) Le port des caméras piétons par les gardes champêtres sera expérimenté jusqu'en novembre 2024.

(3) Décision n° 2021-817 DC du 20 mai 2021.

(4) L'article 8 du projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, adopté par l'Assemblée nationale le 11 avril 2023, repousse au 1er octobre 2024 le terme de cette expérimentation.

– l’identification de l’agent porteur de la caméra lors de l’enregistrement des données ;

– le lieu où ont été collectées les données ;

– l’identifiant de la caméra ;

– l’identification des personnels utilisateurs du logiciel d’exploitation des fichiers vidéo ;

– le motif d’export du fichier vidéo, le nom de l’agent et du service demandeurs, et le numéro de procédure.

En cas de menace sur la sécurité des personnes, les images captées et enregistrées au moyen de caméras individuelles peuvent être transmises en temps réel au poste de commandement du service concerné et aux personnels impliqués dans la conduite et l’exécution de l’intervention (1).

Lorsque cette consultation est nécessaire pour faciliter la recherche d’auteurs d’infractions, la prévention d’atteintes imminentes à l’ordre public, le secours aux personnes ou l’établissement fidèle des faits lors des comptes rendus d’interventions, les personnels auxquels les caméras individuelles sont fournies peuvent avoir accès directement aux enregistrements auxquels ils procèdent dans le cadre d’une procédure judiciaire ou d’une intervention. Les caméras sont équipées de dispositifs techniques permettant de garantir l’intégrité des enregistrements jusqu’à leur effacement et la traçabilité des consultations lorsqu’il y est procédé dans le cadre de l’intervention. Les enregistrements audiovisuels sont conservés dans la limite d’un mois, à l’exception des cas où ils sont consultés dans le cadre d’une procédure judiciaire, administrative ou disciplinaire.

Les articles L. 241-2 et L. 241-3 du CSI déclinent l’ensemble de ces règles à l’usage des caméras piétons par les agents de police municipale (2) et par les sapeurs-pompiers et les marins-pompiers des services d’incendie et de secours (3).

ii. Les caméras embarquées

À la suite de la censure par le Conseil constitutionnel des dispositions encadrant le recours aux caméras embarquées dans les véhicules des forces de l’ordre (4), la loi du 24 janvier 2022 a défini le régime juridique auquel elles sont assujetties. Inspirées partiellement des règles relatives aux caméras piétons, les

(1) Article R. 241-3 du CSI.

(2) Le port des caméras piétons par les agents de police municipale est subordonné à l’autorisation du préfet, sur demande du maire.

(3) Contrairement à la durée de conservation maximale d’un mois concernant les enregistrements réalisés par les gendarmes et les policiers nationaux et municipaux, cette durée s’établit à six mois s’agissant des sapeurs-pompiers et marins-pompiers.

(4) Décision n° 2021-817 DC du 20 mai 2021.

dispositions des articles L. 243-1 à L. 243-5 du CSI précisent les conditions d'utilisation des caméras embarquées.

Ainsi, les agents de la police nationale, les agents des douanes, les militaires de la gendarmerie nationale, les sapeurs-pompiers professionnels et volontaires des services d'incendie et de secours ainsi que les personnels des services de l'État et les militaires des unités investis à titre permanent de missions de sécurité civile peuvent procéder, au moyen de caméras embarquées dans leurs véhicules, embarcations et autres moyens de transport fournis par le service, à un enregistrement de leurs interventions dans des lieux publics lorsque se produit ou est susceptible de se produire un incident, eu égard aux circonstances ou au comportement des personnes concernées.

Les règles relatives à l'information du public et à la transmission en temps réel des images au poste de commandement sont similaires à celles prévues pour l'usage des caméras piétons (1). En revanche, l'article L. 243-3 du CSI prévoit spécifiquement que les caméras embarquées ne peuvent ni comporter de traitements automatisés de reconnaissance faciale, ni procéder à aucun rapprochement, interconnexion ou mise en relation automatisée avec d'autres traitements de données à caractère personnel. Dans sa décision n° 2021-834 DC du 20 janvier 2022 sur la loi relative à la responsabilité pénale et la sécurité intérieure, le Conseil constitutionnel a considéré que le législateur n'avait pas méconnu le droit au respect de la vie privée. Mais il assortit la constitutionnalité du dispositif d'une réserve d'interprétation limitant potentiellement l'intérêt futur de ces dispositifs :

« *Toutefois, ces dispositions ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées comme autorisant les services compétents à procéder à l'analyse des images au moyen d'autres systèmes automatisés de reconnaissance faciale qui ne seraient pas installés sur les caméras* » (2).

Par ailleurs, la durée maximale de conservation des images s'élève à sept jours, hors procédure judiciaire, administrative ou disciplinaire.

Conformément à la jurisprudence constitutionnelle, les contraintes relatives aux modalités d'enregistrement apparaissent particulièrement strictes. L'article L. 243-4 du CSI prévoit que les caméras sont employées de telle sorte qu'elles ne visent pas à recueillir les images de l'intérieur des domiciles ni, de façon spécifique, celles de leurs entrées. Lorsque l'emploi de ces caméras conduit à visualiser de tels lieux, l'enregistrement est immédiatement interrompu. Toutefois, lorsqu'une telle interruption n'a pu avoir lieu compte tenu des circonstances de

(1) Le public est informé, par une signalétique spécifique apposée sur le moyen de transport, que celui-ci est équipé d'une caméra. Toutefois, cette obligation ne s'applique pas aux véhicules ne comportant pas d'équipements ou de dispositifs de signalisation spécifiques et affectés à des missions impliquant l'absence d'identification du service concerné.

(2) Paragraphe n° 54.

l'intervention, les images enregistrées sont supprimées dans un délai de quarante-huit heures à compter de la fin du déploiement du dispositif.

Près de quinze mois après l'entrée en vigueur de la loi, le décret d'application prévu par l'article L. 243-5 du CSI est toujours en cours d'élaboration, retardant ainsi le déploiement effectif des caméras embarquées. **Si vos rapporteurs ne sous-estiment pas le travail règlementaire qui incombe aux services du ministère de l'Intérieur, ils considèrent en l'espèce que les délais de publication du décret ne sont pas satisfaisants.** Cette situation suscite une impatience légitime, voire une frustration compréhensible, de la part des représentants des forces de l'ordre auditionnés dans le cadre des travaux de la mission d'information, indépendamment des enjeux opérationnels qui entourent la mise en œuvre du dispositif.

iii. Les caméras aéroportées

L'usage de drones équipés de caméras dans le cadre de missions de police administrative ou de police judiciaire s'est développé à la fin des années 2010. En l'absence de tout cadre légal ou règlementaire approprié, le recours à des caméras aéroportées par les forces de sécurité intérieure – notamment au cours de la crise sanitaire du premier semestre 2020 (1) – s'est heurté à la jurisprudence du Conseil d'État statuant en référé (2) et à la position de la CNIL.

En effet, dans sa délibération du 12 janvier 2021, la formation restreinte de la CNIL a rappelé à l'ordre le ministère de l'Intérieur pour avoir méconnu plusieurs dispositions du règlement général sur la protection des données (RGPD) (3) du fait de l'usage de drones équipés d'un dispositif de captation d'images. Considérés comme des traitements de données à caractère personnel assujettis aux règles du RGPD, ces dispositifs requièrent l'élaboration préalable d'un cadre normatif aux fins d'autoriser la mise en œuvre de traitements de telles données.

Dans l'attente d'une telle évolution juridique, la CNIL a ainsi enjoint le ministère de l'Intérieur de ne plus recourir à la captation de données à caractère personnel à partir de drones.

La première tentative d'encadrement législatif des caméras aéroportées a été intégralement censurée par le Conseil constitutionnel, celui-ci considérant, à l'occasion de l'examen de la loi du 25 mai 2021, que les finalités et les modalités de l'usage des drones étaient insuffisamment précises (4). Tirant les enseignements

---

(1) Dans ses réponses au questionnaire transmis par la CNIL, le ministère de l'Intérieur reconnaissait en mai 2020 l'usage fréquent de caméras aéroportées afin de vérifier le respect des mesures de confinement, de surveiller le déroulement de manifestations, d'effectuer des missions de police judiciaire ou de surveiller des rodéos urbains.

(2) Conseil d'État, n° 440442 et n° 440445, 18 mai 2020 et n° 446155, 22 décembre 2020.

(3) Règlement (UE) 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, et abrogeant la directive 95/46/CE.

(4) Décision n° 2021-817 DC du 20 mai 2021.

de la censure constitutionnelle, la loi du 24 janvier 2022 a établi un cadre strict autorisant, d'une part, le recours aux caméras aéroportées en matière de police administrative et de sécurité civile et, d'autre part, à des fins de police judiciaire (1).

S'agissant des drones utilisés dans le cadre de missions de police judiciaire, les articles 230-47 à 230-53 du code de procédure pénale fixent les règles applicables aux conditions de recours et d'utilisation des caméras aéroportées. L'article 230-47 énumère trois cas de figure :

– la réalisation d'une enquête ou d'une instruction portant sur un délit ou un crime puni d'au moins trois ans d'emprisonnement ;

– la réalisation d'une enquête ou d'une instruction de recherche des causes de la mort ou de la disparition d'un individu ;

– la recherche d'une personne en fuite.

Le recours aux dispositifs aéroportés est autorisé pour une durée maximale d'un mois, renouvelable une fois, dans le cadre d'une enquête préliminaire. En ce qui concerne l'instruction, il est autorisé pour une durée maximale de quatre mois, renouvelable sans que la durée totale des opérations ne puisse excéder deux ans. (2)

L'autorisation du procureur de la République ou du juge d'instruction précise l'objet, les lieux concernés et la durée du recours à ces dispositifs. Le déroulement des opérations est placé sous l'autorité et le contrôle du magistrat qui les a autorisées et qui peut ordonner leur interruption à tout moment (3). L'officier de police judiciaire compétent décrit les données enregistrées utiles à la manifestation de la vérité. Les enregistrements sont placés sous scellés fermés et il est procédé à la destruction de ces données à l'expiration du délai de prescription de l'action publique et à la diligence du procureur qui en dresse le procès-verbal (4). Dans le cadre de leurs missions de police judiciaire, les forces de sécurité peuvent recourir aux drones, sans qu'il ne leur soit interdit de filmer l'intérieur d'un lieu privé, contrairement à l'usage prévu en matière de police administrative.

Cependant, ces évolutions législatives sont restées lettres mortes à ce jour. Auditionnée le 25 janvier 2023, la direction des affaires criminelles et des grâces (DACG) du ministère de la Justice considère que cette base légale est insuffisante pour autoriser l'usage de drones en matière judiciaire : selon le Gouvernement, un décret est en effet indispensable afin de satisfaire les exigences fixées notamment par les articles 97 à 107 de la loi du 6 janvier 1978 dite « Informatique et Libertés », en ce qui concerne les modalités de conservation des données.

---

(1) À la suite d'un avis non-publié rendu par le Conseil d'État le 12 octobre 2021 se prononçant en faveur d'une reconnaissance explicite dans le code de procédure pénale d'un régime légal permettant le recours aux drones à des fins de police judiciaire.

(2) Article 230-48 du code de procédure pénale (CPP).

(3) Articles 230-49 et 230-50 du CPP.

(4) Articles 230-52 et 230-53 du CPP.

S’agissant des drones utilisés dans le cadre des missions de police administrative et de sécurité civile, les articles L. 242-1 à L. 242-8 du CSI précisent les règles applicables à leur usage par les agents de police nationale, les gendarmes et les personnes intervenant dans le cadre de la sécurité civile (1).

Sur le fondement de l’article L. 242-2 de ce code, les images captées peuvent être transmises et visionnées en temps réel ou différé par le personnel du poste de commandement impliqué dans sa conduite et son exécution, pendant une durée strictement nécessaire. Le personnel doit garantir techniquement l’intégrité des enregistrements et la traçabilité des consultations. Sauf si les circonstances l’interdisent ou que cette information entre en contradiction avec les objectifs poursuivis, le public doit être informé par tout moyen approprié de l’emploi de dispositifs aéroportés et de l’autorité responsable de leur mise en œuvre. Le ministère de l’Intérieur doit veiller à une information générale du public (2).

Plusieurs principes limitent le recours aux caméras aéroportées : celui-ci doit être strictement nécessaire, adapté aux circonstances et temporaire. Il peut donner lieu à la collecte et au traitement strictement nécessaires de données à caractère personnel dans le respect de la loi « Informatique et Libertés » et des règles du RGPD. La captation du son, le traitement automatisé de reconnaissance faciale et le rapprochement automatisé avec d’autres traitements de données à caractère personnel sont expressément exclus (3).

L’autorité responsable tient un registre qui précise la finalité des traitements, la durée des enregistrements ainsi que les personnes ayant accès aux images. Ils sont conservés sous la responsabilité du chef de service les ayant mis en œuvre pendant une durée maximale de sept jours à compter du déploiement du dispositif, sans que nul ne puisse y avoir accès sauf dans le cadre d’une procédure judiciaire, administrative ou disciplinaire (4).

En ce qui concerne les seules missions de police administrative, l’article L. 242-5 du CSI restreint l’usage des caméras aéroportées à six finalités :

– la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés, en raison de leurs caractéristiques ou des faits qui s’y sont déjà déroulés, celle des risques d’agression, de vol ou de trafic d’armes, d’êtres humains ou de stupéfiants, ainsi que la protection des bâtiments et installations publics et de leurs abords immédiats, lorsqu’ils sont particulièrement exposés à des risques d’intrusion ou de dégradation ;

(1) À la suite de sa décision rendue le 20 mai 2021 sur la loi dite « Sécurité globale », le Conseil constitutionnel a de nouveau rejeté, dans sa décision rendue le 20 janvier 2022, la possibilité pour les agents de police municipale de recourir aux drones.

(2) Article L. 242-3 du CSI.

(3) Article L. 242-4 du même code.

(4) Idem.

– la sécurité des rassemblements de personnes sur la voie publique ou dans des lieux ouverts au public ainsi que l'appui des personnels au sol, en vue de leur permettre de maintenir ou de rétablir l'ordre public, lorsque ces rassemblements sont susceptibles d'entraîner des troubles graves à l'ordre public ;

– la prévention d'actes de terrorisme ;

– la régulation des flux de transport, aux seules fins du maintien de l'ordre et de la sécurité publics ;

– la surveillance des frontières, en vue de lutter contre leur franchissement irrégulier ;

– le secours aux personnes.

L'autorisation est délivrée par décision écrite et motivée du préfet, qui s'assure du respect des dispositions énoncées dans la présente note, pour une durée maximale de trois mois, renouvelable selon les mêmes modalités. Les caméras aéroportées ne peuvent recueillir les images de l'intérieur des domiciles et de leurs entrées. Si tel est le cas, l'enregistrement est immédiatement interrompu ou supprimé dans un délai de quarante-huit heures à compter de la fin du déploiement du dispositif, sauf dans le cadre d'un signalement à l'autorité judiciaire sur le fondement de l'article 40 du code de procédure pénale.

Conseil constitutionnel, décision n° 2021-834 DC du 20 janvier 2022

Le Conseil constitutionnel a censuré la mise en place d'une procédure d'urgence d'emploi des drones en raison de l'exposition particulière et imprévisible à un risque d'atteinte caractérisé aux personnes et aux biens. Cette procédure avait pour objet d'autoriser les services compétents à déployer des caméras aéroportées pendant une durée de quatre heures maximum sans l'autorisation du préfet, sans la réserver à des cas précis d'une gravité particulière, et sans préciser les informations portées à la connaissance de ce dernier. Le Conseil constitutionnel a jugé que cette disposition n'assurait pas une conciliation équilibrée des objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions, d'une part, et de droit au respect de la vie privée, d'autre part.

Deux réserves d'interprétation ont également été posées : d'une part, l'autorisation du préfet déterminant la finalité et les conditions d'utilisation des drones ne peut être accordée uniquement si le service ne peut employer d'autres moyens moins intrusifs et, d'autre part, le renouvellement d'une telle autorisation ne saurait être décidé par le préfet sans qu'il soit établi que le recours aux drones demeure le seul moyen d'atteindre la finalité poursuivie.

À l'instar de l'usage des caméras aéroportées en matière judiciaire, l'application de ces dispositions reste suspendue à la publication du décret mentionné à l'article L. 242-8 du CSI. Selon les informations recueillies par vos rapporteurs, ce texte règlementaire serait en cours de finalisation et devrait entrer en vigueur d'ici à la fin du premier semestre 2023.

En ce qui concerne la sécurité civile, l'article L. 242-6 du CSI restreint l'usage des caméras aéroportées à deux finalités :

– la prévention des risques naturels ou technologiques ;

– le secours aux personnes et la lutte contre l'incendie.

Contrairement à l'usage des drones dans le cadre des missions de police judiciaire et administrative, le décret d'application de ces dispositions relatives aux seules missions de sécurité civile est entré en vigueur le 27 avril 2022. Les pompiers ont ainsi pu utilement recourir à des caméras aéroportées pour lutter contre les feux qui ont ravagé des dizaines de milliers d'hectares de forêt en bordure du littoral atlantique au cours de l'été 2022.

Dans son discours prononcé le 28 octobre 2022, le président de la République a annoncé l'engagement de moyens supplémentaires dès 2023 afin de renforcer les moyens dont disposent les services d'incendie et de secours, ce qui implique notamment l'acquisition de drones équipés de caméras (1).

c. La nécessité d'une refonte du cadre juridique de la captation d'images de sécurité

Les multiples évolutions législatives et règlementaires précitées témoignent d'une approche parcellaire de l'encadrement des images de sécurité dans notre ordonnancement juridique. Contraintes par la jurisprudence administrative et constitutionnelle, elles donnent l'impression d'une superposition normative manquant de cohérence et de lisibilité. Auditionné le 25 octobre 2022, M. Jérôme Léonnet, directeur général adjoint de la police nationale, a ainsi déploré « *la complexité et l'incomplétude* » du cadre juridique actuel.

Cette complexification s'explique en partie par le besoin d'adapter les règles prévues par le code de la sécurité intérieure aux spécificités propres à chaque vecteur de captation. **Cependant, elle illustre désormais la nécessité d'harmoniser et d'unifier le droit applicable à la captation de l'ensemble des images dans l'espace public aux fins de lutter contre l'insécurité.**

Il convient donc de clarifier et d'uniformiser, dans la mesure du possible, les règles relatives aux finalités pour lesquelles les caméras fixes ou mobiles peuvent être installées, aux modalités opérationnelles de leur utilisation, à l'information et au droit d'accès des personnes concernées par ces enregistrements, à la durée de conservation des images et aux conditions dans lesquelles celles-ci sont stockées et consultées.

Outre l'exigence d'intelligibilité du droit, vos rapporteurs considèrent que le « *grand soir* » des images de sécurité est d'autant plus nécessaire qu'il est

(1) https://www.elysee.fr/emmanuel-macron/2022/10/28/reception-des-acteurs-mobilises-cet-ete-contre-les-feux-de-forets

impératif de garantir la conformité de leur régime juridique aux règles de protection des données personnelles prévues par le RGPD et la loi « Informatique et Libertés ».

Auditionnés par la mission d'information, la CNIL (1) et le Conseil d'État (2) partagent de longue date cette analyse. S'agissant spécifiquement des caméras de vidéoprotection, la Cour des comptes a récemment rappelé le nécessaire respect des nouvelles exigences liées à l'entrée en vigueur du RGPD :

« *La réglementation relative à la vidéoprotection sur l'espace public a été définie dans les années 1990 et n'a pas été modifiée pour tenir compte des évolutions des technologies, des pratiques, ou de l'environnement juridique. Il apparaît désormais urgent de la réformer. Plusieurs dispositions de code de la sécurité intérieure sont obsolètes par rapport à certains outils devenus d'usage courant. Surtout, le code n'a pas encore tiré les conséquences du nouveau cadre juridique relatif à la protection des données à caractère personnel entré en vigueur en mai 2018.* […] *Le cloisonnement entre le régime de la vidéoprotection et celui de la protection des données à caractère personnel doit être remis en cause.*

Par ailleurs, le cadre légal n'identifie pas la gestion du maintien de l'ordre comme finalité de la vidéoprotection, alors que la direction de l'ordre public et de la circulation de la préfecture de police de Paris l'utilise fréquemment à cette fin. De même, le code de la sécurité intérieure n'évoque pas explicitement l'élucidation à des fins judiciaires comme finalité de la vidéoprotection » (3).

Si elle recueille une certaine unanimité, la refonte complète dont il est question représente un travail d'envergure que le Gouvernement a renoncé à mener à court terme. Dans l'étude d'impact annexée au projet de loi relatif aux jeux Olympiques et Paralympiques adopté par l'Assemblée nationale le 11 avril 2023, le ministère de l'Intérieur et des outre-mer en précise les raisons :

« *Une rationalisation de ces règles éparses et disparates a été envisagée afin d'unifier les régimes en vigueur. Néanmoins, dans la mesure où les dispositions applicables aux caméras mobiles* […] *viennent très récemment d'être créées ou modifiées par les lois n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés et n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, et où toutes les mesures d'application de cette dernière ne sont pas encore toutes publiées, il a été estimé préférable de ne pas les faire évoluer de nouveau* » (4).

Néanmoins, vos rapporteurs se félicitent de la mise en conformité, prévue par l'article 6 de ce projet de loi, des articles L. 251-1 à L. 255-1 du code de la

(1) Voir notamment la délibération n° 2022-043 du 14 avril 2022.

(2) Voir notamment l'avis n° 401214 du 20 septembre 2020.

(3) Cour des comptes, référé S2021-2194 du 2 décembre 2021 relatif au plan de vidéoprotection de préfecture de police de Paris, p. 5.

(4) Étude d'impact, pp. 72-73.

sécurité intérieure avec les règles du RGPD et de la loi « Informatique et Libertés ».

L'objectif poursuivi consiste à rendre applicables aux images captées par des caméras de vidéoprotection l'ensemble des garanties protectrices que prévoit la loi « Informatique et Libertés », s'agissant aussi bien du contrôle opéré par la CNIL que des obligations incombant aux responsables des traitements ou du droit d'information et d'accès aux images par les personnes concernées.

Le rapport de notre collègue Guillaume Vuilletet sur l'article 6 de ce projet de loi explicite les enjeux de cette réforme :

Assujettissement de la vidéoprotection aux règles fixées par le RGPD et la loi « Informatique et Libertés », prévu par l'article 6 du projet de loi JOP 2024

L'article L. 251-1 du code de la sécurité intérieure (CSI) établit un régime dual selon l'utilisation des images captées par les caméras de vidéoprotection. En effet, seules les images enregistrées dans des traitements automatisés permettant d'identifier des personnes physiques sont soumises aux règles de protection des données prévues par la loi « Informatique et Libertés » et le RGPD. Les autres images de vidéoprotection ne sont pas assimilées, en l'état du droit, à des données à caractère personnel : elles ne sont donc assujetties ni aux règles de la loi « Informatique et Libertés », ni à celles du RGPD, mais relèvent du régime *ad hoc* fixé par les articles L. 251-2 à L. 251-5 du CSI.

La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des données personnelles avait explicitement exclu de son champ d'application des traitements de données à caractère personnel relevant de la sécurité publique, de la sûreté de l'État et du droit pénal des États-membres.

Pour autant, la Cour de justice de l'Union européenne a considéré, dans un arrêt rendu le 11 décembre 2014 (1), que les systèmes de caméras de vidéoprotection constituent des traitements de données à caractère personnel ayant vocation à être assujettis aux règles encadrant la protection des données personnelles telles qu'elles découlent aujourd'hui du RGPD (2) et de la directive (UE) 2016/680 du 27 avril 2016 dite « police-justice », dont la transposition a été opérée par la loi n° 2018-493 du 20 juin 2018.

Par conséquent, la dualité du régime juridique précité, sur le fondement de l'article L. 251-1 du CSI, s'avère aujourd'hui obsolète. Les systèmes de vidéoprotection mis en œuvre suivant l'ensemble des finalités mentionnées à l'article L. 251-2 du même code, à l'exception des finalités relatives à la sauvegarde des installations utiles à la défense nationale (3) et à la prévention d'actes de terrorisme (4), doivent être appréhendés comme des traitements de données à caractère personnel assujettis au RGPD et à la loi « Informatique et Libertés ».

Source : rapport n° 939 de Guillaume Vuilletet au nom de la commission des Lois de l'Assemblée nationale sur le projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, p. 59.

(1) CJUE, 11 décembre 2014, C-212/13.

(2) Le RGPD a abrogé la directive 95/46/CE.

(3) 2° de l'article L. 251-2.

(4) 6° de l'article L. 251-2.

Auditionnée le 7 février 2023, la direction des libertés publiques et des affaires juridiques (DLPAJ) du ministère de l'Intérieur et des outre-mer admet que les textes relatifs à la captation et aux usages des images collectées dans l'espace public sont « *éparpillés* ». Elle souhaite donc participer à la construction d'un « *cadre cohérent, lisible et harmonisé* » de tous les usages.

Onze ans après l'entrée en vigueur du code de la sécurité intérieure, vos rapporteurs estiment que ce moment est venu.

Recommandation n° 1 : Engager une refonte des règles applicables à l'ensemble des dispositifs de captation d'images dans l'espace public, suivant un double objectif de rationalisation et d'unification du cadre juridique fixé par le code de la sécurité intérieure.

Enfin, vos rapporteurs déplorent les retards accumulés par le ministère de l'Intérieur et des outre-mer comme par le ministère de la Justice quant à la publication des décrets d'application relatifs, d'une part, aux caméras embarquées et, d'autre part, aux caméras aéroportées utilisées à des fins de police judiciaire et de police administrative. Près de quinze mois après la promulgation de la loi qui autorise les forces de sécurité à recourir à ces dispositifs, et alors même que la préparation de ces textes règlementaires aurait pu être anticipée au regard des décisions jurisprudentielles survenues depuis 2020, l'absence de ces décrets interdit encore le déploiement de ces caméras.

S'agissant des drones, **les tergiversations du ministère de la Justice sur la délimitation de leur cadre légal et règlementaire en matière judiciaire pénalisent fortement les services enquêteurs, en les privant d'un outil pourtant utile à leurs missions.** En outre, cette situation révèle une asymétrie de moyens pour le moins paradoxale au détriment des forces de police et gendarmerie, ce qui provoque, à raison, l'incompréhension de leurs dirigeants et représentants syndicaux auditionnés par la mission d'information.

Recommandation n° 2 : Publier de toute urgence les décrets d'application prévus par la loi du 24 janvier 2022 relatifs à l'utilisation des caméras embarquées et des caméras aéroportées en matière de police judiciaire et de police administrative.

2. Le déploiement de moyens techniques modernes confronté à des enjeux opérationnels multiformes

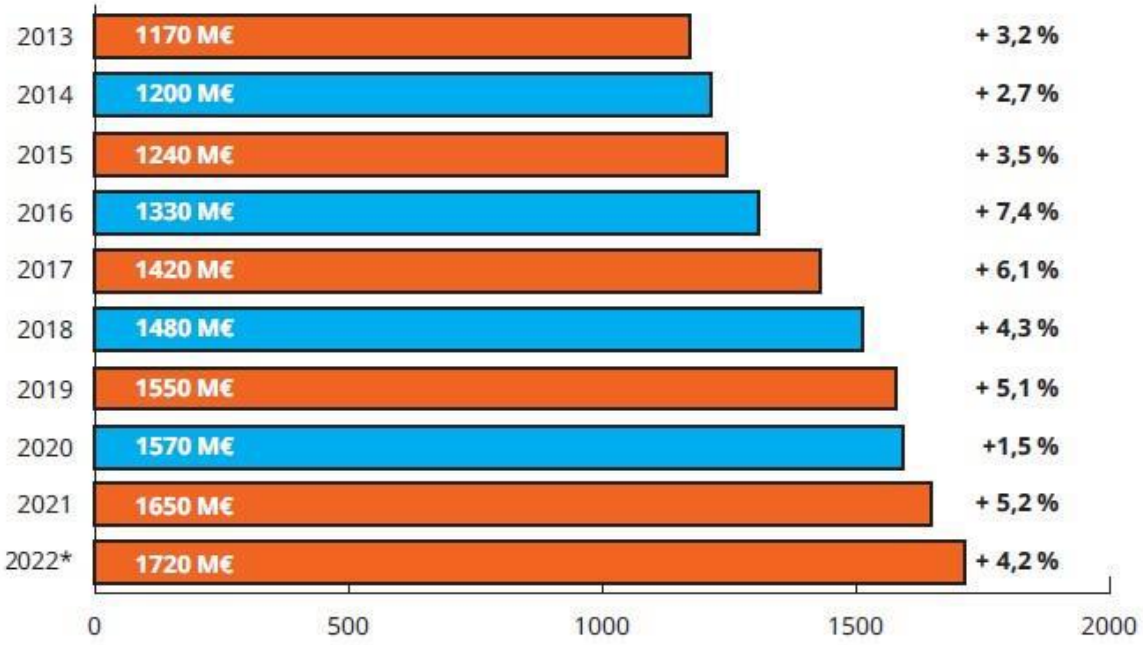
a. Un soutien financier croissant en faveur des dispositifs de captation d'images

Selon les chiffres communiqués par les directions générales de la police et de la gendarmerie nationales à vos rapporteurs, environ 38 000 caméras de

vidéoprotection sont installées sur la voie publique en zone gendarmerie [1] et près de 52 000 en zone police [2]. À la fin de l'année 2022, la police et la gendarmerie disposaient respectivement d'un stock de 31 000 et de 21 000 caméras piétons, ce qui représente, à l'échelle des effectifs des deux forces, une caméra piéton pour cinq agents. Par ailleurs, la gendarmerie détient une flotte d'un peu moins de 500 drones, contre 300 environ pour la police.

Le déploiement de la vidéoprotection dans l'espace public bénéficie d'un fort soutien financier de l'État, agissant à la fois en tant qu'« *acheteur* » au profit des forces de sécurité intérieure que « *co-financeur* » des matériels acquis par les collectivités territoriales.

Le recours croissant à ces outils s'inscrit dans une perspective plus large dépassant les seules finalités sécuritaires. Dans sa contribution écrite remise à l'issue de son audition le 18 octobre 2022, la CNIL fait état d'un marché global de ventes de solutions de vidéosurveillance en constante augmentation depuis dix ans, atteignant désormais plus de 1,7 milliard d'euros :



Évolution des ventes de vidéosurveillance en France en millions d'euros
** Estimation effectuée en juin 2022*
Ventes cumulées des fabricants (matériels et logiciels), distributeurs et installateurs
Source : Etude d'En Toute Sécurité

La CNIL précise également que le « *marché français est détenu essentiellement par des acteurs étrangers. En 2015, plus d'un tiers des équipements de vidéoprotection installés étaient importés de Chine, mais des acteurs étasuniens,*

(1) En juillet 2020.

(2) Au 31 décembre 2022.

allemands et suédois sont également présents. De fait, si la France dispose de leaders mondiaux en matière de sécurité électronique, gestion des identités d'accès et cybersécurité, elle ne dispose pas encore d'acteurs de cette taille pour ce qui est des équipements vidéo ». (1)

Cet engouement pour la vidéoprotection s'appuie sur des sources de financement étatique pérennes. La loi du 5 mars 2007 a créé le Fonds interministériel de prévention de la délinquance et de la radicalisation (FIPDR), destiné à financer la réalisation d'actions dans le cadre des plans de prévention de la délinquance faisant l'objet d'une contractualisation entre l'État et les collectivités territoriales. Selon les documents annexés au projet de loi de finances pour 2023, les actions de sécurisation des sites sensibles au risque terroriste, les projets relatifs à la vidéoprotection de voie publique – caméras et centres de supervision urbains – et aux raccordements aux centres opérationnels de la police ou de la gendarmerie nationales, ainsi que les subventions d'équipements des polices municipales seront financés à hauteur de 30 millions d'euros. Ce montant représente plus du double de celui des crédits annuellement engagés en la matière entre 2007 et 2009 au titre du FIPDR.

Le Laboratoire d'innovation numérique de la CNIL observe que cette stratégie volontariste, inspirée de l'exemple du *Home Office* britannique dans les années 1990, avait grandement facilité l'acquisition des systèmes de vidéoprotection par les communes :

« […] *En février 2014, selon les chiffres du ministère de l'Intérieur, 2 820 communes et 173 établissements publics de coopération intercommunale (EPCI) avaient été accompagnés pour installer 26 614 caméras, pour un montant total de 148,52 millions d'euros de subventions* ». (2)

Les subventions de l'État accordées aux collectivités territoriales désireuses de s'équiper de dispositifs de vidéoprotection peuvent couvrir jusqu'à la moitié de leur coût total, sans préjudice des autres leviers de financement locaux. Lors de son audition, la DPSIS a estimé que le coût moyen d'acquisition et d'installation d'une caméra oscille entre 9 000 euros (3) et 20 000 euros, hors charges d'exploitation. La maintenance avoisine 10 % de l'investissement initial chaque année.

Ces efforts financiers ont vocation à s'amplifier. Le rapport annexé à la loi d'orientation et de programmation du ministère de l'Intérieur et des outre-mer du 24 janvier 2023 indique que « *les crédits du fonds interministériel de prévention de la délinquance et de la radicalisation (FIPDR) consacrés à la vidéoprotection*

(1) Contribution écrite de la CNIL remise à la mission d'information.

(2) Laboratoire d'innovation numérique de la CNIL, « Les caméras au village *», novembre 2021, p. 18.*

(3) S'agissant des zones rurales choisissant pour l'essentiel des vecteurs de transmission autres que la transmission filaire.

seront triplés sur les cinq années à venir et viendront cofinancer les projets portés par les collectivités ». (1)

L'instruction ministérielle du 16 février 2023 relative aux orientations du FIPDR pour l'année en cours précise que le déploiement de la vidéoprotection *« reste la priorité* » au sein du programme intitulé « Sécurisation », qui regroupe l'ensemble des subventions dédiées à l'acquisition de ces dispositifs.

C'est dans cette perspective que la ville de Nantes a annoncé, le 16 mars 2023, le déploiement de 90 caméras de vidéoprotection supplémentaires d'ici à la fin de l'année 2023, dans le but notamment de sécuriser les grands événements sportifs organisés en 2023 et 2024. Confrontée à une augmentation des vols sans violence et des cambriolages au cours de ces dernières années (2), la municipalité bénéficiera d'un co-financement intégral par Nantes Métropole et par l'État, pour un montant total de 2,8 millions d'euros.

Lors du déplacement de la mission d'information à Nantes le 27 octobre 2022, les auditions conduites par vos rapporteurs avec les élus aux conseils municipal et communautaire, les agents des services de police et de gendarmerie et les représentants de la préfecture de Loire-Atlantique ont fait état de la réticence exprimée par certains élus vis-à-vis de la vidéoprotection (3). Cette prudence tient en partie au « reste à charge » supporté par la ville de Nantes s'agissant des coûts liés au fonctionnement de son centre de supervision urbaine (4). Elle peut aussi s'expliquer par une méfiance de principe, plus ou moins assumée, quant à l'efficacité et au caractère intrusif de ces dispositifs.

Si les financements croisés dont bénéficient les communes peuvent contribuer à lever certains obstacles, ils permettent également aux plus petites communes de s'équiper à moindre coût, comme le révèle l'étude menée par le laboratoire d'innovation numérique de la CNIL :

« *Selon une délibération du conseil régional d'Ile-de-France, Nointel (Val d'Oise, 798 habitants) a pour projet d'installer sept caméras sur son territoire en 2020 pour un montant total de 105 156 euros. La municipalité sollicite des financements auprès de la Région Ile-de-France (35 %), du département (6 %) et du fonds de dotation d'équipement des territoires ruraux (25 %). Il ne restera à sa charge qu'environ un tiers du montant total, soit un peu moins de 36 000 euros* ». (5)

---

(1) Rapport annexé à la loi d'orientation et de programmation du ministère de l'Intérieur, p. 27.

(2) Selon le service statistique ministériel de la sécurité intérieure, les vols sans violence constituent l'infraction la plus courante à Nantes en 2022, comme sur le reste du territoire métropolitain. Ces infractions connaissent encore une légère augmentation, passant de 7 610 en 2021 à 7 726 en 2022. L'évolution la plus importante concerne les cambriolages, avec une augmentation de 30 % en un an.

(3) Selon un classement établi en 2019 par « La Gazette des communes *», Nantes, 6e ville la plus peuplée, n'était que la 39e ville la plus « vidéoprotégée ».*

(4) Soit 3 millions d'euros engagés par la municipalité depuis 2018.

(5) Laboratoire d'innovation numérique de la CNIL, « Les caméras au village *», novembre 2021, p. 22.*

Pour autant, ces modes de financement soulèvent d'importantes incertitudes juridiques, au risque de fragiliser le déploiement des systèmes de vidéoprotection sur l'ensemble du territoire. Dans une réponse publiée le 29 décembre 2022 à la question de notre collègue sénateur Jean-Louis Masson, le ministère de l'Intérieur et des outre-mer rappelle que « *le président du conseil régional ne dispose* […] *d'aucune compétence qui justifierait l'octroi de subventions aux communes dans le but de financer le recrutement d'agents de police municipale ou le matériel communal de vidéoprotection sur la voie publique* ». (1)

Au regard des compétences limitativement attribuées au conseil régional par le législateur (2), la jurisprudence administrative a annulé une délibération décidant de la mise en place de subventions pour financer l'équipement communal de vidéoprotection (3). Le Gouvernement estime que cette annulation contentieuse pourrait subséquemment impliquer le remboursement par les communes des sommes que le conseil régional leur aurait déjà versées.

Vos rapporteurs s'inquiètent de l'insécurité juridique qui semble caractériser les aides financières dont les communes sont susceptibles de bénéficier. Une clarification du droit applicable mériterait d'être apportée par le ministère de l'Intérieur et des outre-mer, dans le respect du principe constitutionnel de libre-administration des collectivités territoriales tel qu'encadré par la loi.

Recommandation n° 3 : Clarifier les règles de financement de l'acquisition et de l'installation des systèmes de vidéoprotection par les collectivités territoriales.

Si les moyens financiers investis dans l'équipement de dispositifs de captation d'images s'accroissent, l'emploi sur le terrain des caméras fixes et mobiles par les forces de sécurité demeure confronté à de nombreux enjeux opérationnels.

b. Des enjeux opérationnels multiformes

Que le dispositif soit actuellement déployé – caméras de vidéoprotection et caméras piétons – ou non – caméras embarquées et aéroportées (4) –, plusieurs enjeux d'ordre opérationnel entourent leur utilisation respective.

i. Les caméras de vidéoprotection

Parmi l'ensemble des défis opérationnels que soulève l'utilisation des systèmes de vidéoprotection, trois d'entre eux peuvent plus particulièrement être analysés : la fiabilité des dispositifs techniques mis en place, le déport des images filmées par les caméras et la captation du son.

---

(1) Réponse ministérielle du 29 décembre 2022 à la question écrite n° 01629 du sénateur Jean-Louis Masson.

(2) Articles L. 4211-1 à L. 4221-1 du code général des collectivités territoriales.

(3) Tribunal administratif de Marseille, 17 décembre 2019, n° 1703337.

(4) Depuis l'entrée en vigueur du décret du 27 avril 2022, seules les missions de sécurité civile peuvent permettre l'usage des caméras aéroportées.

Premièrement, l'article L. 254-2 du code de la sécurité intérieure prévoit que les systèmes de vidéoprotection installés doivent être conformes à des normes techniques définies par arrêté du ministre de l'Intérieur. L'arrêté actuellement applicable a été publié le 3 août 2007. Il n'a fait l'objet d'aucune modification depuis son entrée en vigueur, alors même que la technologie de captation vidéo s'est constamment perfectionnée au cours de ces quinze dernières années. Les dispositions prévues par l'arrêté ne sont pas véritablement obsolètes, dans la mesure où elles se contentent de fixer des exigences minimales à respecter, qu'il s'agisse du niveau de résolution (1) et de la fréquence d'images par seconde (2) ou des garanties de traçabilité et d'accès à celles-ci.

Dans sa réponse à la question écrite posée en 2018 par notre collègue Denis Masséglia, le ministère de l'Intérieur s'est lui-même interrogé quant à la nécessité de réviser cet arrêté :

« *Ces exigences techniques ont offert des progrès incontestables en termes d'exploitation d'images issues de ces dispositifs, à la grande satisfaction des services opérationnels. Il est vrai cependant qu'après plus de dix ans de mise en œuvre, ce texte apparaît aujourd'hui perfectible afin d'intégrer les importantes évolutions technologiques et de progresser encore sur l'usage de cette technologie concourant à la sécurité de nos concitoyens* ». (3)

Pour autant, aucune évolution n'a été apportée à ce texte à ce jour. Le besoin de renouveler les spécifications techniques applicables aux systèmes de vidéoprotection est d'autant plus réel que certains dispositifs peuvent faire l'objet de défaillances altérant considérablement leurs fonctions capacitaires. Le laboratoire d'innovation numérique de la CNIL fait état de plusieurs dysfonctionnements ayant affecté certains systèmes installés dans des communes faiblement peuplées :

« *Les problèmes techniques, notamment dus aux conditions météorologiques et à la nuit, ne sont pas rares, et sont loin de se limiter à de simples questions de réglages. En 2014, le maire nouvellement élu de Toufflers (Nord, 3 902 habitants) témoignait des limites de l'installation :* " Depuis que j'ai été élu en mars, j'ai fait quatre demandes de visionnage des bandes à la police intercommunale de Hem. Pour un feu de poubelles, un cambriolage chez le kiné, une voiture cassée et des dégradations sur le stade. Ça n'a jamais servi à rien ! On voit des ombres, mais on ne peut identifier personne... ". […] *Les maires pointent les insuffisances techniques de ces caméras fixes : leur champ de vision est limité et leur résolution ne permet pas d'identifier les plaques d'immatriculation.*

Les pannes peuvent avoir d'autres origines, que ce soient les logiciels, serveurs ou encore les caméras elles-mêmes, quand il ne s'agit pas d'une

(1) Soit au moins 704 x 576 pixels ou 352 x 288 pixels.

(2) Soit au moins six images par seconde.

(3) Réponse ministérielle du 15 janvier 2019 à la question écrite n° 5475 du député Denis Masséglia.

combinaison de ces divers éléments. À deux reprises, en 2009 et en 2016, la ville de Ploërmel (Morbihan, 9 571 habitants) constata à l'occasion d'un audit technique l'obsolescence de son système de vidéo-protection. La première fois, la qualité des images était en cause pour une vingtaine de caméras sur les 42 installées, et la seconde, tout un ensemble de défaillances techniques fut identifié. L'ampleur et la vitesse de dégradations des dispositifs interrogent : à Etaples (Pas de Calais, 10 865 habitants), en 2015, plus de la moitié du parc de 40 caméras installées en 2010, ne fonctionne plus. Toutefois ces limites techniques conduisent généralement les maires à s'équiper de caméras plus performantes et de technologies plus intrusives plutôt que de remettre en cause l'installation des caméras existantes. » (1).

Vos rapporteurs considèrent que la refonte des règles encadrant la captation des images de sécurité pourrait utilement inclure la mise à jour de l'arrêté du 3 août 2007. Dans cette perspective, il conviendrait sans doute de modifier l'alinéa 2 de l'article L. 254-2 du code de la sécurité intérieure, afin de laisser un délai suffisamment long (2) pour garantir la mise en conformité progressive des systèmes de vidéoprotection avec les exigences du futur arrêté.

Recommandation n° 4 : Réviser l'arrêté ministériel du 3 août 2007 afin de mettre à jour les exigences techniques auxquelles doivent satisfaire les systèmes de vidéoprotection.

Deuxièmement, le déport des images filmées par les caméras de vidéoprotection vers les services de police et les unités de gendarmerie constitue l'une des priorités identifiées par l'instruction ministérielle du 16 février 2023 relative aux orientations des politiques soutenues dans le cadre du FIPDR. Conformément à l'objectif de *continuum* de sécurité, il peut aussi être envisagé de favoriser le raccordement des systèmes de vidéoprotection installés par des communes de taille réduite ou moyenne vers des centres de supervision urbaine (CSU) mutualisés avec d'autres communes même taille (3).

Le laboratoire d'innovation numérique de la CNIL mentionne plusieurs projets menés à cette fin :

« *Dans le Loir-et-Cher, dès 2014, 12 communes décident de déporter leurs flux vers le centre d'opérations et de renseignement de la Gendarmerie. Autre exemple, la ville de Carnac (Morbihan, 4 250 habitants, 26 caméras) est la première commune du Morbihan à avoir signé, en 2015, une convention de partage des images de vidéosurveillance avec la gendarmerie du Morbihan. Deux écrans de visualisation ont ainsi été installés : l'un au sein de la police municipale, l'autre au sein de la gendarmerie.* […] *Auparavant réservés aux municipalités dotées de*

(1) Laboratoire d'innovation numérique de la CNIL, « Les caméras au village *», novembre 2021, p. 26.*

(2) Le délai de mise aux normes actuellement prévu s'élève à deux ans.

(3) Dans son rapport sur les polices municipales publié en octobre 2020, la Cour des comptes constate un doublement du nombre de CSU entre 2015 et 2019, passant en quatre ans de 434 à 903.

ressources importantes […] *la mutualisation de ces équipements à l'échelle intercommunale permet aux municipalités plus petites d'en bénéficier* » (1).

Vos rapporteurs estiment que le déport des images présente un intérêt opérationnel majeur, comme l'ont souligné les chefs de la Brigade de recherches et d'intervention (BRI) de la Préfecture de police, du RAID et du GIGN lors de leur audition le 25 octobre 2022. De façon plus large, l'interopérabilité des systèmes de vidéoprotection facilite la coordination des interventions des forces de l'ordre en cas de crise, en leur garantissant l'accès à une même information en temps réel.

Troisièmement, des interrogations émergent quant à la possibilité technique, et surtout à l'opportunité, d'autoriser la captation sonore par le truchement des systèmes de vidéoprotection. Là encore, une telle évolution est matériellement envisageable et n'engendrerait pas de contrainte technique excessive (2). Auditionnée le 11 octobre 2022, Mme Hélène Gaury, directrice technico-commerciale de la société Bouygues ES, a indiqué que la captation sonore peut répondre à des besoins exprimés par certaines personnes publiques ou privées afin, par exemple, de détecter l'usage d'une arme à feu ou des bris de verre (3).

En l'état du droit, la captation sonore est interdite dans le cadre de la mise en œuvre de la vidéoprotection (4). Si les règles applicables aux caméras piétons autorisent un enregistrement « audiovisuel », ce qui inclut par nature la captation sonore, l'expérimentation menée en 2019 par la ville de Saint-Étienne visant à détecter et à capter des sons sur la voie publique a été interrompue par la CNIL. Dans le cadre de son contrôle, la CNIL a en effet estimé qu'un tel dispositif méconnaissait les règles relatives à la protection des données à caractère personnel prévues par le RGPD et la loi « Informatique et Libertés », en l'absence de base légale appropriée.

Vos rapporteurs estiment qu'une captation sonore en continu dans l'espace public ne respecterait pas les garanties de nécessité et de proportionnalité exigées par la jurisprudence constitutionnelle. Cette pratique, dont l'utilité opérationnelle devrait par ailleurs être démontrée, risquerait fort de porter une atteinte excessive au respect du droit à la vie privée.

ii. Les caméras piétons

Pérennisé depuis la loi du 3 juin 2016 et généralisé depuis 2020, l'usage des caméras piétons par les agents de police et les gendarmes s'est rapidement heurté à une contrainte opérationnelle difficile à surmonter. En effet, la batterie des

---

(1) Laboratoire d'innovation numérique de la CNIL, « Les caméras au village *», novembre 2021, pp. 26 et 27.*

(2) L'enregistrement des sons est beaucoup moins « lourd » que celui des images et occuperait donc un espace réduit sur les serveurs stockant ces données.

(3) De tels dispositifs sont par exemple déjà utilisés aux États-Unis.

(4) Les débats lors de l'examen en première lecture de l'article 6 du projet de loi relatif aux jeux Olympiques et Paralympiques à l'Assemblée nationale ont été l'occasion de rappeler ce principe, auquel le Gouvernement n'envisage pas de déroger.

premières caméras piétons utilisées par les forces de l'ordre jusqu'en 2021 présentait un problème majeur d'autonomie. Elle ne permettait pas de procéder à des enregistrements au-delà d'une heure ou deux, alors même que la durée des patrouilles peut dépasser six heures consécutives.

L'ensemble des organisations syndicales de la police nationale auditionnées par la mission d'information ont ainsi relayé la frustration des agents de police quant à l'impossibilité pratique de recourir à cet outil. La résiliation du marché conclu par le ministère de l'Intérieur et le choix, en 2021, d'un nouveau prestataire (1) a permis de résoudre ces difficultés, en dépit de la taille jugée parfois « encombrante » (2) du modèle utilisé.

Le principal enjeu entourant l'usage des caméras piétons concerne les modalités de déclenchement de l'enregistrement. En l'état du droit, seul l'agent équipé de la caméra peut décider de recourir à l'enregistrement. Cette condition restrictive fait l'objet de critiques. D'une part, les contraintes opérationnelles liées au contexte particulier de l'intervention (3) ne permettent pas systématiquement à l'agent de déclencher en temps utile l'enregistrement (4). D'autre part, cet enregistrement « *à la main* » de l'agent suscite des débats quant au caractère discrétionnaire et potentiellement partial du choix d'enregistrer ou non son intervention (5).

Plusieurs solutions ont été évoquées afin d'améliorer l'emploi des caméras piétons, telles qu'un enregistrement continu opéré par la caméra, du début à la fin de la patrouille. Au-delà des éventuelles difficultés techniques, voire juridiques, qu'un tel enregistrement continu et systématique pourrait engendrer, vos rapporteurs rejettent cette idée qui traduit finalement, en creux, une défiance à l'encontre des policiers et des gendarmes justifiant ainsi de filmer chacun de leurs faits et gestes.

En revanche, il pourrait être envisageable d'élargir les conditions de déclenchement de l'enregistrement afin de préserver l'intérêt opérationnel que revêtent les caméras piétons. Ainsi, l'enregistrement pourrait être déclenché à distance par l'autorité hiérarchique en salle de commandement, et automatiquement dès lors que l'agent décide d'utiliser son arme de service. Ces évolutions, auxquelles souscrivent plusieurs syndicats, tels que Alternative Police CFDT et Unité SGP Police FO, auditionnés le 30 novembre 2022, permettraient de pallier

(1) Motorola.

(2) Selon la contribution écrite remise par le syndicat Alliance à la mission d'information en janvier 2023.

(3) L'intervention peut ainsi dégénérer soudainement, ne laissant pas le temps à l'agent de déclencher l'enregistrement.

(4) Quand la caméra est activée, les trente secondes précédant l'activation sont enregistrées. Symétriquement, quand l'agent décide d'arrêter la caméra, trente secondes supplémentaires sont conservées.

(5) L'enregistrement est autorisé seulement lorsque se produit ou est susceptible de se produire un incident lié au contexte de l'intervention ou à la personne filmée.

les difficultés propres à certaines interventions (1) en garantissant de façon effective leur enregistrement audiovisuel.

Recommandation n° 5 : Autoriser le poste de commandement à déclencher à distance les caméras-piétons uniquement à la demande des agents sur le terrain et prévoir un déclenchement automatique de l'enregistrement lorsque l'agent fait usage de son arme.

iii. Les caméras embarquées

Comme précisé précédemment, aucune caméra embarquée n'est utilisée par la police et la gendarmerie à ce jour, en l'absence du décret d'application prévu par l'article L. 243-5 du code de la sécurité intérieure (CSI). Auditionné le 25 octobre 2022, le service des technologies et des systèmes d'information de la sécurité intérieure rattaché à la DGGN et à la DGPN précise que ce type de caméras, dont le coût unitaire oscille entre 2 000 et 10 000 euros, serait destiné à filmer l'extérieur et l'intérieur du véhicule dans le but d'objectiver les éventuelles atteintes à l'intégrité physique des agents et les conditions de leur intervention.

Un *sourcing* (2) a été réalisé par le ministère de l'Intérieur à la fin du premier semestre 2022. Compte tenu du retard règlementaire et des délais d'approvisionnement, la mise en œuvre de ces dispositifs ne devrait pas intervenir avant la fin de l'année 2023. L'une des difficultés pratiques consiste à déterminer la localisation précise de la caméra sur la carrosserie ou dans l'habitacle du véhicule, qu'il s'agisse d'une moto, d'une automobile, ou d'une embarcation fluviale.

L'entreprise Axon (3) et la direction générale de la gendarmerie nationale (4) ont souligné le caractère singulièrement contraignant de la rédaction de la première phrase du second alinéa de l'article L. 243-4 du CSI. Celle-ci prévoit que les caméras embarquées sont employées de telle sorte qu'elles ne visent pas à recueillir les images de l'intérieur des domiciles ni, de façon spécifique, celles de leurs entrées. Dans le cas contraire, l'enregistrement doit être immédiatement interrompu. À défaut, les images enregistrées doivent être supprimées dans un délai maximal de quarante-huit heures.

Concrètement, l'interdiction de filmer les entrées de domiciles met en péril le caractère opérationnel des caméras embarquées. Celles-ci pourront en effet être amenées à filmer, même subrepticement, l'entrée de maisons ou d'immeubles d'habitation selon la physionomie des lieux où se déroule l'intervention.

---

(1) Par exemple en cas de blessure empêchant l'agent de déclencher lui-même sa caméra piéton.

(2) Le sourcing *est défini par l'article R. 2111-1 du code de la commande publique comme la possibilité pour un acheteur «* d'effectuer des consultations ou réaliser des études de marché, de solliciter des avis ou d'informer les opérateurs économiques du projet et de ses exigences *» afin de préparer la passation d'un marché public*

(3) Audition du 10 janvier 2023.

(4) Audition du 29 novembre 2022.

Vos rapporteurs considèrent que l'expression « *de façon spécifique* » n'est pas adaptée aux contraintes pratiques auxquelles seront confrontées les forces de l'ordre sur le terrain. Ils proposent de modifier cette rédaction afin de circonscrire l'interdiction visée par le second alinéa au recueil « *permanent* » de l'image de l'entrée de domiciles, ce qui garantirait la souplesse nécessaire à l'emploi des caméras embarquées conformément aux règles prévues par les articles L. 243-1 et suivants du CSI.

Selon vos rapporteurs, cet ajustement rédactionnel mineur ne déséquilibrerait aucunement le dispositif au regard de la jurisprudence du Conseil constitutionnel à l'occasion des décisions rendues sur la loi du 25 mai 2021, puis sur celle du 24 janvier 2022.

Recommandation n° 6 : Circonscrire l'interdiction de recueil des images de l'entrée d'un domicile par une caméra embarquée à son seul caractère « permanent ».

iv. Les caméras aéroportées

Le recours aux drones par les forces de sécurité présente des contraintes opérationnelles et procédurales très nettement supérieures à celles qui entourent l'utilisation des autres dispositifs de captation d'images de sécurité.

D'une part, du fait de leur position en surplomb, l'interdiction faite aux caméras aéroportées de filmer l'entrée et l'intérieur des domiciles, par analogie avec la règle applicable aux caméras embarquées, s'avère *a priori* difficilement conciliable avec l'utilisation même du drone. Si M. Gil Ancelin, président du Groupe Protec [(1)], estime que les progrès technologiques permettront d'ici deux ans de parvenir à flouter en temps réel ces images « interdites », il convient de constater que cette évolution n'est pas encore d'actualité.

D'autre part, l'article L. 242-2 du CSI impose aux caméras aéroportées d'être équipées de dispositifs techniques permettant de garantir l'intégrité des enregistrements jusqu'à leur effacement, ainsi que la traçabilité des consultations lorsqu'il y est procédé dans le cadre de l'intervention. Cette contrainte ne semble pas poser de difficulté particulière s'agissant des caméras piétons et des caméras embarquées. Néanmoins, elle présente un degré de contrainte plus élevé pour les caméras aéroportées.

Lors de son audition, le service des technologies et des systèmes d'information de la sécurité intérieure a rappelé la nécessité de disposer d'une bande de fréquence adaptée, afin de permettre la transmission des images captées depuis l'air jusqu'au sol, grâce à une connectivité sans fil utilisant des fréquences radio. En l'absence de technique de chiffrement des modèles acquis par la gendarmerie et la police ces dernières années, il est donc indispensable de sécuriser

(1) Audition du 13 décembre 2022.

la fréquence, en prévoyant idéalement à cette fin une bande de fréquence dédiée aux services de police et aux unités de gendarmerie.

Auditionnée le 29 novembre 2022, l'Autorité de régulation des communications électroniques et des postes (ARCEP) précise que les fréquences sont réparties entre les différents affectataires (1), dont font notamment partie le ministère de l'Intérieur et des outre-mer et l'ARCEP. Selon l'ARCEP, et sous réserve du type de drone auquel les forces de sécurité auront recours, les fréquences utilisées pourraient être celles du ministère lui-même ou correspondre à des fréquences libres utilisées, après autorisation, par le ministère de l'Intérieur.

Recommandation n° 7 : Disposer d'une bande de fréquence dédiée à la transmission sécurisée des données captées par des caméras aéroportées.

(1) Selon le tableau national de répartition des bandes de fréquence (TNRBF).

B. SIMPLIFIER LE CADRE JURIDIQUE DE CONSERVATION DES DONNÉES ET ÉVALUER L'EFFICACITÉ DES DISPOSITIFS DE CAPTATION D'IMAGES

1. Des évolutions de nature à faciliter l'utilisation des images de sécurité par les forces de l'ordre et les magistrats

a. Si les conditions d'accès doivent être différenciées selon le dispositif de captation utilisé, les délais de conservation des données doivent être harmonisés

Déterminer la durée de conservation des données et les conditions d'accès aux enregistrements est un équilibre à trouver entre l'objectif de prévention des atteintes à l'ordre public et le droit au respect de la vie privée. La durée doit être limitée et adaptée aux finalités pour lesquelles sont mis en œuvre les systèmes.

● *Les délais de conservation varient de sept à trente jours.*

En matière d'images captées sur la voie publique, les durées de conservation varient selon les dispositifs de captation utilisés.

Pour les images captées sur la voie publique par des caméras fixes, la durée de conservation des images est précisée dans l'autorisation donnée par l'autorité préfectorale et ne peut pas excéder trente jours (article L. 252-3 du CSI). **L'autorisation peut prévoir une durée minimale de conservation** (article L. 252-5 du CSI).

Pour les images captées par des caméras individuelles, les enregistrements sont effacés au bout d'un mois, sauf lorsqu'ils sont utilisés dans le cas d'une procédure judiciaire, administrative ou disciplinaire (article L. 241-1 du CSI). Cette durée a été modifiée par l'article 14 de la loi RPSI [(1)] : elle était auparavant de six mois. L'article 14 a été introduit par amendement lors de l'examen du texte au Sénat par le rapporteur, qui souhaitait aligner le temps de conservation des données sur celui déjà prévu pour les autres dispositifs de captation d'images sur la voie publique.

L'enregistrement n'est pas permanent : il est déclenché lorsqu'un incident se produit ou est susceptible de se produire. **Vos rapporteurs, au cours de leurs travaux, ont écarté l'idée de basculer vers un enregistrement permanent**, qui serait trop intrusif pour les porteurs de caméras et trop coûteux en termes de stockage.

(1) Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure (RPSI).

Une exception existe pour les caméras individuelles portées par les sapeurs-pompiers et les marins-pompiers : l'article L. 241-3 du CSI prévoit que les enregistrements audiovisuels sont effacés au bout de **six mois**.

Pour les images captées par des caméras installées sur des aéronefs, la durée de conservation ne peut pas excéder sept jours, sauf si les enregistrements sont utilisés dans le cadre d'une procédure judiciaire, administrative ou disciplinaire (article L. 242-4 du CSI). La durée de conservation a été modifiée par l'article 15 de la loi RPSI : le passage de trente à sept jours était proposé par le Gouvernement dans le projet de loi initial et tenait compte de l'avis rendu par le Conseil d'État [(1)]. Lorsqu'il n'a pas été possible d'interrompre l'enregistrement et que des images de l'intérieur ou de l'entrée de domiciles ont été filmées, les images doivent être supprimées dans un délai de 48 heures, hors cas de transmission à l'autorité judiciaire sur le fondement de l'article 40 du code de procédure pénale (III de l'article L. 242-5 du CSI).

Pour les images captées par les caméras embarquées, la durée de conservation ne peut également pas excéder sept jours, à l'exception des cas où les enregistrements sont utilisés dans le cadre d'une procédure judiciaire, administrative ou disciplinaire. Ce délai a été modifié par l'article 17 de la loi RPSI : il était auparavant de trente jours. Lorsqu'il n'a pas été possible d'interrompre l'enregistrement et que des images de l'intérieur ou de l'entrée de domiciles ont été filmées, les images doivent être supprimées dans un délai de 48 heures, hors cas de transmission à l'autorité judiciaire sur le fondement de l'article 40 du code de procédure pénale (article L. 243-4 du CSI).

Les données captées par les dispositifs de lecture automatique de plaques d'immatriculation (LAPI) font l'objet d'un cadre particulier : elles peuvent être conservées pendant **quinze jours**. La durée de conservation était auparavant fixée à huit jours : elle a été allongée à quinze jours par l'article 104 de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale. L'arrêté du 18 mai 2009 portant création d'un traitement automatisé de contrôle des données signalétiques des véhicules n'a pas été mis à jour et mentionne toujours huit jours.

Cette période de quinze jours doit permettre de comparer les données issues des lecteurs avec les données relatives aux véhicules volés ou signalés (FOVeS) et avec le système d'information Schengen (SIS). Si cette comparaison a donné lieu à un rapprochement, les données peuvent être conservées un mois. M. Florian Colas, le directeur du renseignement et des enquêtes douanières (DNRED), a indiqué être favorable à ce que cette durée soit étendue à quatre mois. Le projet de loi portant mise en conformité du droit de visite douanière et de modernisation de l'action douanière, présenté par les ministres Bruno Le Maire et Gabriel Attal le 3 avril

(1) Avis sur un projet de loi relatif à la responsabilité pénale et à la sécurité intérieure, Assemblée générale, 8 juillet 2021.

2023, propose justement d'expérimenter pendant trois ans un allongement de la durée de conservation des données des LAPI à quatre mois (1). Vos rapporteurs ne souhaitent pas aller jusque-là et suggèrent d'étendre la durée à trente jours.

Les systèmes de vidéoprotection installés par les opérateurs de transports

Les systèmes de vidéoprotection installés par les opérateurs de transports doivent respecter le cadre instauré par le code de sécurité intérieure aux articles L. 251-1 à L. 255-1.

À titre d'exemple, la SNCF possède un parc de 70 000 caméras, dont 17 000 installées dans les gares et 45 000 embarquées à travers les trains.

L'article 113 de la loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités a autorisé le port de caméras individuelles pour les agents assermentés des exploitants de services de transport. La SNCF a mis en œuvre cette possibilité dès 2020. L'expérimentation doit durer quatre ans.

Le parc de caméras de l'emprise de l'aéroport Roissy-Charles-de-Gaulle comporte environ 10 000 caméras, réparties à la fois sur les parkings, les pistes mais aussi dans les parties ouvertes au public.

Dans les deux cas, la durée de conservation des données maximale s'établit à trente jours pour les dispositifs fixes. L'accès aux images est possible soit dans le cadre de réquisitions judiciaires, soit dans le cadre de l'exercice du droit d'accès par une personne filmée.

Les durées de conservation varient donc de sept à trente jours selon les dispositifs de captation déployés, les caméras individuelles des sapeurs-pompiers mis à part. Vos rapporteurs sont favorables à une harmonisation consistant à fixer à trente jours la durée maximale de conservation quel que soit le dispositif de captation employé.

Recommandation n° 8 : Harmoniser les temps de conservation des images en fixant une durée de 30 jours quel que soit le vecteur de captation utilisé.

Dans tous les cas évoqués ci-dessous, la durée de conservation fixée par la loi constitue **une borne maximale**, et non une obligation. Dans les faits, la durée de conservation dépend largement de la capacité des opérateurs du système à conserver ces données. Les données étant conservées sur des serveurs physiques, le stockage représente un coût très important. Il est donc extrêmement fréquent que les durées de conservation soient bien inférieures à 30 jours, les données étant automatiquement écrasées pour en enregistrer de nouvelles.

Vos rapporteurs ont pu ainsi constater, au cours de leurs travaux, que les images n'étaient pas systématiquement conservées pendant le délai maximal fixé par la loi. À Nice, les données sont conservées pendant 10 jours. S'agissant du parc

(1) Dossier de presse du projet de loi portant mise en conformité du droit de visite douanière et de modernisation de l'action douanière, avril 2023.

de caméras de la SNCF, **les durées de conservation varient même d'une gare à l'autre**. Ainsi, le temps de conservation des données captées par les caméras installées Gare du Nord à Paris est de 4 jours (avec le projet de monter à 14 jours), alors qu'il est de 30 jours en région Auvergne-Rhône-Alpes. Il a cependant été indiqué à vos rapporteurs que si des faits intéressants se produisaient, la SNCF était susceptible de faire une extraction pour conserver les images pendant trente jours (1).

Cette différence d'un système de vidéoprotection à l'autre est source de confusion lors des réquisitions et peut provoquer des pertes de chance pour les victimes d'infractions. Si imposer une durée minimale de conservation immédiatement paraît brutal pour les opérateurs des systèmes, des solutions pour allonger la durée de conservation effective des images captées sur la voie publique devraient être explorées.

Une solution pourrait être de prévoir des durées minimales pour certains évènements, comme les évènements sportifs. C'est l'une des recommandations formulées par les sénateurs MM. François-Noël Buffet et Laurent Lafon dans leur rapport sur les incidents survenus au Stade de France pendant la finale de la Ligue des champions en mai 2022 (2).

Recommandation n° 9 : Tendre à la fixation d'une durée minimale de conservation des données.

● *L'accès aux enregistrements par les professionnels*

Pour les caméras fixes, le régime d'accès diffère sensiblement de celui qui est en vigueur pour les caméras mobiles. Cela s'explique par le fait que peu de caméras appartiennent aux forces de l'ordre, alors que la plupart des caméras ont été installées par les municipalités ou par les opérateurs de transport, par exemple.

L'article L. 251-2 du CSI dresse la liste des finalités pour lesquelles la transmission et l'enregistrement d'images prises sur la voie publique au moyen de la vidéoprotection peuvent être mis en œuvre par les autorités publiques.

Certaines finalités concernent directement les services spécialisés de renseignement, notamment la prévention d'actes de terrorisme. La mission de prévention contre toute forme d'ingérence étrangère, prévue à l'article L. 811-3 du CSI, ne figure pourtant pas dans la liste, alors même que l'exploitation d'images dans le cadre du contre-espionnage pourrait être extrêmement utile aux services. Vos rapporteurs s'interrogent donc sur l'opportunité d'élargir la liste des finalités

(1) La SNCF a ainsi conservé une partie des images enregistrées aux abords du Stade de France le soir de la finale de la Ligue des champions, le 28 mai 2022, en anticipant ainsi les réquisitions judiciaires.

(2) Recommandation n° 12 : « imposer au cas par cas aux opérateurs des systèmes de vidéoprotection, dans les espaces accessibles au public à l'intérieur ou aux abords des équipements, la conservation des images captées le jour des grands évènements sportifs, pendant la durée légale d'un mois », Rapport d'information du Sénat sur les incidents survenus au Stade de France le 28 mai 2022, déposé le 13 juillet 2022.

prévues à l'article L. 251-2 du CSI, afin de garantir aux services de renseignement spécialisés un accès plus large aux images de sécurité.

Recommandation n° 10 : Élargir la liste des finalités d'accès aux images de la vidéoprotection à certaines des missions des services de renseignement spécialisés, notamment le contre-espionnage.

L'accès par les forces de l'ordre aux images issues d'un système de vidéoprotection est prévu par l'autorisation d'installation délivrée par l'autorité préfectorale (article L. 252-3 du CSI) : celle-ci peut ainsi prescrire que certains agents sont destinataires des images et enregistrements. L'autorisation doit préciser les modalités de la transmission ou de l'accès à ces images. La décision peut également être prise à tout moment par arrêté préfectoral, qui doit être signé après avis de la commission départementale de vidéoprotection. Seules l'urgence et l'exposition particulière à un risque d'actes de terrorisme permettent à l'autorité préfectorale de ne pas saisir la commission départementale.

Les personnels qui visionnent les images doivent être individuellement désignés et habilités (article L. 255-1 du CSI). Pour être habilités, les agents doivent suivre une formation en matière de données à caractère personnel, régulièrement mise à jour (article R. 252-12 du CSI).

L'article R. 252-13 du CSI prévoit également que les systèmes de vidéoprotection doivent comporter des dispositifs pour assurer la disponibilité, la confidentialité et l'intégrité des enregistrements, ainsi que la traçabilité des consultations.

Les services de renseignement ont un accès aux images issues des systèmes de vidéoprotection limité par les finalités prévues à l'article L. 251-2 du CSI.

Pour les caméras individuelles, une transmission en temps réel du flux vidéo au poste de commandement du service concerné et aux personnels impliqués dans l'intervention est possible depuis la loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, « *lorsque la sécurité des agents de la police nationale ou des militaires de la gendarmerie nationale ou la sécurité des biens et des personnes est menacée* » (article L. 241-1 du CSI). Auparavant, les images ne pouvaient être consultées qu'à l'issue de l'intervention. Le Conseil constitutionnel a estimé que l'encadrement des conditions de la mise en œuvre de cette transmission et des destinataires possibles était de nature à préserver le droit au respect de la vie privée [(1)].

Le déclenchement de la caméra individuelle ne peut pas être activé à distance à ce jour.

(1) Paragraphe 113 de la décision n° 2021-817 DC du 20 mai 2021.

L'article 241-1 du CSI prévoit également la faculté, pour les personnels auxquels les caméras sont fournies, de **consulter les images enregistrées pendant une intervention lorsque cela est nécessaire** pour « *faciliter la recherche d'auteurs d'infractions, la prévention d'atteintes imminentes à l'ordre public, le secours aux personnes ou l'établissement fidèle des faits lors des comptes rendus d'intervention* ». Cette faculté, ouverte par la loi « Sécurité globale », devait être encadrée au regard des possibilités de visualisation sans motif légitime ou de modification et suppression de l'enregistrement. L'article précise donc que « *les caméras sont équipées de dispositifs techniques permettant de garantir l'intégrité des enregistrements jusqu'à leur effacement et la traçabilité des consultations lorsqu'il y est procédé dans le cadre de l'intervention* ».

Considérant que la nouvelle possibilité de consultation ne concernait qu'un nombre restreint d'hypothèses et était accompagnée de garanties techniques renforcées, le Conseil constitutionnel a validé le dispositif. Il a néanmoins formulé une réserve d'interprétation : l'intégrité des enregistrements et la traçabilité des consultations doivent être garanties jusqu'à leur effacement – à défaut, les droits de la défense et le droit à un procès équitable risqueraient d'être méconnus.

Pour les caméras installées sur les aéronefs, les images peuvent être transmises au poste de commandement du service concerné et aux personnels impliqués dans l'intervention en temps réel ou différé pendant la durée de l'intervention. Comme pour les caméras individuelles, des dispositifs techniques doivent garantir l'intégrité des enregistrements et la traçabilité des consultations (article L. 242-2 du CSI). Dans sa contribution écrite aux travaux de vos rapporteurs [(1)], la direction générale de la police nationale (DGPN) a indiqué que les drones acquis par les services avant l'encadrement juridique ne permettaient pas de répondre aux exigences posées par la loi s'agissant de l'intégrité des enregistrements. Cette inadéquation du matériel déjà acquis aux exigences posées par le législateur est particulièrement regrettable.

La transmission en temps réel n'est pas subordonnée à l'existence de conditions particulières, contrairement à ce qui est prévu pour la transmission en temps réel des images issues des caméras individuelles : la transmission est possible pour les mêmes finalités que la captation.

L'autorité responsable de la mise en œuvre des traitements doit tenir un registre qui précise la finalité poursuivie et la durée des enregistrements réalisés, mais aussi les personnes ayant accès aux images, y compris celles transmises en temps réel (article L. 242-4 du CSI).

L'accès aux enregistrements est interdit, sauf lorsque cela est nécessaire à la suite d'un signalement sur le fondement de l'article 40 du code de procédure pénale (CPP), et à l'exception du cas où elles sont utilisées dans le cadre d'une procédure judiciaire, administrative ou disciplinaire (article L. 242-4 du CSI).

(1) Contribution écrite faisant suite à l'audition du 25 octobre 2022.

Pour les caméras embarquées, la transmission en temps réel des images au poste de commandement et aux personnels impliqués dans l'intervention est possible lorsque la sécurité des agents est concernée (article L. 243-3 du CSI).

L'article L. 243-3 prévoit également la possibilité, pour les personnels participant à l'intervention, de consulter les images dans deux cas : lorsqu'il s'agit d'assurer la sécurité de leurs interventions ou lorsque cette consultation vise à faciliter l'établissement fidèle des faits lors des comptes rendus d'interventions. Cette faculté a été ouverte par l'article 17 de la loi RPSI. Elle s'accompagne des mêmes garanties que celles prévues pour les caméras individuelles : des dispositifs techniques doivent permettre de préserver l'intégrité de l'enregistrement et la traçabilité des consultations. Au-delà de ces consultations, les conditions d'accès aux enregistrements sont similaires à celles détaillées pour les caméras installées sur les aéronefs : l'accès n'est possible que dans le cas d'un signalement à l'autorité judiciaire sur le fondement du même article 40 du code de procédure pénale (article 243-4 du CSI).

Comme pour les caméras installées sur des aéronefs, un registre doit être tenu afin de retracer les enregistrements réalisés et les personnes ayant eu accès aux images (y compris en temps réel).

Pour les caméras mobiles (caméras individuelles, caméras installées sur des aéronefs, caméras embarquées), les mécanismes de traçabilité ont été détaillés à vos rapporteurs par la DGPN :

– mécanismes d'authentification forte des utilisateurs (notamment au moyen d'une carte professionnelle) ;

– historique de la cause d'extraction de la vidéo (cadre judiciaire, administratif, disciplinaire, ou formation) ;

– effacement automatique à l'expiration du délai légal.

S'agissant des LAPI, les données sont comparées avec le fichier des objets et des véhicules trouvés (FOVeS) et le système d'information de Schengen (SIS). Pour permettre cette consultation, les données sont conservées pendant une période quinze jours. Dans le cas où un rapprochement positif avec les fichiers mentionnés précédemment est constaté, les données sont conservées pendant un mois, sans préjudice de leur consultation pour les besoins d'une procédure pénale ou douanière. Dans le cas inverse, les données sont effacées après la période de quinze jours (article L. 233-2 du CSI).

M. Florian Colas, directeur du renseignement et des enquêtes douanières (DNRED) à la direction générale des douanes et des droits indirects du ministère de l'Économie, des finances et de la souveraineté industrielle et numérique, a déploré lors de son audition (1) que la base de données des LAPI ne puisse pas être

(1) Audition du 8 novembre 2022.

interrogée autrement que lorsqu'un rapprochement positif a été constaté. Il a également souligné que la durée de conservation était relativement courte.

Comme indiqué précédemment, vos rapporteurs sont favorables à une extension de la durée de conservation des données LAPI à trente jours quel que soit le cas de figure. Ils souhaitent également que l'accès aux données LAPI soit facilité pour permettre une constatation plus aisée de certaines infractions (terrorisme et criminalité organisée).

Recommandation n° 11 : Modifier l'article L. 233-2 du code de la sécurité intérieure afin de permettre la consultation des données LAPI pour prévenir et caractériser les infractions liées au terrorisme et à la criminalité organisée.

Il convient de souligner que les enregistrements issus des caméras individuelles et des caméras installées sur des aéronefs peuvent être utilisés à des fins de pédagogie et de formation des agents (articles L. 241-1 et L. 242-4 du CSI). Les données sont alors anonymisées.

Comme l'ont souligné plusieurs des interlocuteurs de vos rapporteurs, le cadre juridique en matière de captation d'images, qui privilégie une approche par vecteurs, manque de lisibilité et gagnerait à être simplifié.

Recommandation n° 12 : Réviser le code de la sécurité intérieure pour simplifier le cadre juridique relatif à la captation d'images, en adoptant une approche transversale plutôt qu'une approche par vecteurs.

Les données issues des vidéos sont stockées sur des serveurs physiques, ce qui représente un coût certain pour les forces de l'ordre, mais reste une option plus sécurisée que le stockage dans le *cloud* [nuage numérique] si celui-ci n'est pas souverain. L'accroissement du volume de flux vidéos à sauvegarder doit être anticipé par le ministère de l'Intérieur, pour éviter de devoir recourir à des solutions extra-européennes de stockage dans quelques années.

Recommandation n° 13 : Anticiper la saturation du stockage sur des serveurs physiques et financer la création d'un *cloud* souverain.

b. Les modalités de réquisitions des images gagneraient à être modernisées

En matière de police judiciaire, les images provenant de caméras installées sur la voie publique peuvent être réquisitionnées par un officier de police judiciaire (OPJ) ou par un magistrat. Dans le cadre d'une enquête de flagrance, l'officier de police judiciaire peut, sans l'autorisation du procureur de la République, requérir des informations issues d'un système de données ou d'un traitement de données nominatives (article 60-1 du CPP). Dans le cadre d'une enquête préliminaire, l'OPJ agit sur autorisation du procureur de la République (article 77-1-1 du CPP).

La police municipale peut notamment être sollicitée pour transmettre des images issues des caméras appartenant à la municipalité. Dans les municipalités équipées d'un parc de caméras conséquent, cela peut représenter un volume important. Ainsi, le procureur de Nice, M. Xavier Bonhomme, a indiqué à vos rapporteurs qu'environ 1 500 réquisitions par an étaient délivrées dans le cas d'une enquête judiciaire (flagrance ou préliminaire). Les opérateurs de transports sont aussi régulièrement sollicités par réquisition pour donner aux services d'enquête des images issues de leurs caméras.

Or, les modalités de réquisition sont aujourd'hui contraignantes : après leur extraction, les images doivent être enregistrées sur un support physique (CD-roms, DVD, clé USB), qui doit ensuite être récupéré par un enquêteur. Ce support physique constitue le scellé et permet d'assurer l'intégrité et l'authenticité des preuves.

Au vu du volume et du développement de la vidéoprotection, il apparaît prioritaire à vos rapporteurs de travailler à **créer un scellé numérique**, qui permettrait de transmettre de manière dématérialisée les images issues de caméras. Dans la conception du logiciel permettant la création de ce scellé devront être intégrés des dispositifs techniques permettant de garantir l'intégrité de la vidéo.

Recommandation n° 14 : Créer un scellé numérique pour permettre une transmission dématérialisée des images issues de caméras.

Le service des technologies et des systèmes d'information de la sécurité intérieure (STI(SI)²) recommande lui d'envisager la création d'un *cloud* [nuage numérique] « vidéoprotection », sur lequel les différents opérateurs de système de vidéoprotection pourraient télécharger leurs données. Cette solution permettrait également de dématérialiser les réquisitions judiciaires et administratives.

Recommandation n° 15 : Créer un socle d'hébergement mutualisé et hautement sécurisé, sur lequel les différents détenteurs d'images de vidéo protection (opérateurs de transports, collectivités territoriales) pourraient les télécharger.

La DACG du ministère de la Justice a fait état de travaux en cours pour créer une plateforme numérique permettant un accès à distance aux images de vidéo-surveillance détenues par la SNCF : vos rapporteurs ne peuvent qu'être favorables à la création d'une telle plateforme, de nature à simplifier considérablement le travail des officiers de police judiciaire.

c. Prévoir l'information du public et garantir le droit d'accès par les citoyens est indispensable pour maintenir l'équilibre des dispositifs de captation d'images

● *L'information du public*

Pour les caméras fixes, l'article L. 251-3 du CSI prévoit que l'information du public sur l'existence du système de vidéoprotection et sur l'autorité qui en est responsable doit être claire et permanente.

Pour les caméras individuelles, l'article L. 241-1 du CSI prévoit une information des personnes filmées par le porteur de la caméra lorsqu'il déclenche l'enregistrement, mais aussi une information générale du public faite par le ministre de l'Intérieur.

Pour les caméras installées sur les aéronefs, l'article L. 242-3 du CSI prévoit une information du public par tout moyen approprié de leur utilisation, sauf lorsque les circonstances l'interdisent ou que cette information entre en contradiction avec les objectifs poursuivis. Comme pour les caméras individuelles, une information générale du public doit être faite par le ministre de l'Intérieur.

Pour les caméras embarquées, l'article L. 243-2 du CSI prévoit l'information du public par une signalétique sur le moyen de transport, à l'exception des véhicules utilisés pour des missions où l'absence d'identification est requise.

Pour les dispositifs de lecture automatique de plaques d'immatriculation (LAPI), aucune information du public n'est prévue.

● *Le droit d'accès par les personnes filmées*

Le droit d'opposition n'est pas applicable aux systèmes de vidéoprotection. Pour les caméras individuelles et les caméras installées sur les aéronefs, il est explicitement prévu que le droit d'opposition ne s'applique pas (articles R. 241-6, R. 246-6 et R. 241-15 du CSI). Le droit d'opposition n'est également pas applicable aux LAPI, mais le droit d'accès et de rectification s'exerce de manière indirecte auprès de la CNIL [(1)].

Si le droit d'opposition ne s'applique pas, toute personne intéressée peut demander un accès aux enregistrements d'un système de vidéoprotection qui la concernent. Cet accès peut être refusé « *pour un motif tenant à la sûreté de l'État, à la défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, ou au droit des tiers* » [(2)].

● *Le contrôle des systèmes de vidéoprotection s'exerce à deux niveaux.*

La commission départementale de vidéoprotection, qui donne un avis sur les demandes d'autorisation de systèmes de vidéoprotection (article L. 251-4 du CSI), peut également exercer un contrôle à tout moment sur les conditions de

(1) Article 6 de l'arrêté du 18 mai 2009 portant création d'un traitement automatisé des données signalétiques des véhicules.

(2) Article L. 253-5 du code de la sécurité intérieure.

fonctionnement de ces systèmes (article L. 253-1 du CSI). À l'issue de ces contrôles, elle émet des recommandations, qui peuvent aller jusqu'à la suppression des dispositifs non autorisés.

L'article L. 253-2 du CSI prévoit la possibilité pour la CNIL d'exercer un contrôle sur un système de vidéoprotection afin de vérifier qu'il est utilisé conformément à son autorisation, soit sur demande de la commission départementale de vidéoprotection ou du responsable du système. Elle peut également procéder à ce contrôle de sa propre initiative.

Ce pouvoir de contrôle a été octroyé à la CNIL par l'article 18 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (dite « loi LOPSI II »). Entre 2011 et 2021, la CNIL a procédé à 620 contrôles et a prononcé 6 mises en demeure pour de mauvais usages de dispositifs de vidéoprotection (1).

TABLEAU RÉCAPITULATIF DES DURÉES DE CONSERVATION, DE L'ACCÈS AUX IMAGES ET DE L'INFORMATION DU PUBLIC EN FONCTION DU DISPOSITIF DE CAPTATION D'IMAGES UTILISÉ

	Durée de conservation	**Transmission en temps réel**	**Accès aux images**	**Information du public**	**Interdiction de filmer l'intérieur des domiciles ou leur entrée de manière spécifique**
Caméras fixes	30 jours	Autorisation préfectorale peut prévoir que des agents des FDO soient destinataires des images et, en cas d'urgence, l'avis de la commission départementale de vidéoprotection n'est pas indispensable	Autorisation préfectorale peut prévoir que des agents des FDO soient destinataires des images. Peut également se faire par arrêté préfectoral après avis de la CDV. En cas d'urgence, l'avis de la commission départementale de vidéoprotection n'est pas indispensable	Information du public claire et permanente sur l'existence du système de vidéoprotection et sur l'autorité qui en est responsable	X

(1) Chiffres transmis par la CNIL à la suite de l'audition du 18 octobre 2022.

Caméras individuelles	30 jours	Transmission en temps réel possible lorsque la sécurité des agents ou des biens et des personnes est menacée	Les agents peuvent y accéder en cas de nécessité pour la sécurité des personnes ou des biens, ou pour des besoins opérationnels, à la condition que des dispositifs garantissent l'intégrité des enregistrements et la traçabilité des consultations jusqu'à leur effacement	Information des personnes filmées au moment du déclenchement de la caméra. Information générale faite par le ministre de l'Intérieur	
Caméras installées sur des aéronefs	7 jours	Transmission au centre de commandement possible en temps réel ou différé	Pas d'accès aux images dans le délai de sept jours, sauf signalement sur le fondement de l'article 40 du CPP	Information du public lorsque les dispositifs aéroports sont mis en œuvre par tout moyen approprié, sauf si les circonstances l'interdisent ou que l'information entrerait en contradiction avec les objectifs poursuivis. Information générale du public faite par le ministre de l'Intérieur	X
Caméras embarquées	7 jours	Transmission au poste de commandement concerné et aux personnels possible lorsque la sécurité des agents est menacée	Les agents ayant participé à l'intervention peuvent les consulter pour assurer la sécurité de leurs interventions ou faciliter la rédaction de leurs comptes rendus d'intervention	Information du public par une signalétique sur le moyen de transport, sauf lorsque le véhicule, pour les besoins de la mission, ne doit pas être identifié	X
Dispositifs de lecture automatique de plaques d'immatriculation (LAPI)	15 jours si aucun rapprochement avec le FOVeS et le SIS, un mois si un rapprochement positif a été constaté	*Non pertinent*	Consultation des données interdites, sauf pour tester si rapprochement avec le fichier des véhicules volés et le système d'information Schengen	*Non pertinent*	

Source : commission des Lois.

2. Si le manque de données complique l'évaluation de l'efficacité de la vidéoprotection, il apparaît clairement que son potentiel n'est pas aujourd'hui totalement exploité

La réflexion sur le sujet de l'efficacité de la vidéoprotection n'est pas nouvelle : un rapport des inspections (IGPN, IGGN et IGA) daté de juillet 2009 (1) conclut ainsi, en des termes non équivoques, à l'efficacité de la vidéoprotection à la fois pour prévenir la délinquance et dans le cadre des enquêtes.

« *Les dispositifs de vidéoprotection ont montré leur efficacité en matière de prévention de la délinquance et leur impact en prévention dépasse le périmètre des zones vidéoprotégées. Bien qu'ils apportent une aide indiscutable à de nombreuses enquêtes et interpellations, leur impact sur le taux global d'élucidation reste encore modéré en raison d'une densité de caméras souvent insuffisante, ou de matériels qui ne permettent pas toujours une identification précise des personnes.* »

Ce rapport, qui s'appuie sur l'analyse des statistiques de circonscriptions de police et de brigades de gendarmerie, a fait l'objet de certaines critiques portant notamment sur la méthodologie employée. La Cour des comptes, dans un rapport de juillet 2011, estimait ainsi que « *les résultats contradictoires de cette enquête, ainsi que sa méthode, entièrement basée sur l'analyse des statistiques de l'état 4001, ne permettent pas d'en tirer des enseignements fiables* » (2).

M. Guillaume Gormand, chercheur associé au Centre d'études et de recherche sur la diplomatie, l'administration publique et le politique, exprime également des doutes sur la méthodologie suivie par les inspections.

La date de publication du rapport des inspections, 2009, c'est-à-dire il y a 14 ans, n'en fait pas un outil très pertinent d'analyse aujourd'hui. Il mérite néanmoins d'être mentionné pour contextualiser les réflexions autour de la vidéoprotection.

a. Une efficacité à la fois préventive et pour certaines enquêtes

i. Un effet préventif qui peut être délicat à objectiver

● *La désescalade permise par les caméras individuelles*

Les caméras individuelles portées par les agents ont trois finalités :

– la prévention des incidents au cours d'interventions des agents de la police nationale et des militaires de la gendarmerie nationale ;

– le constat des infractions et la poursuite de leurs auteurs ;

---

(1) Rapport sur l'efficacité de la vidéoprotection, Inspection générale de la police nationale (IGPN), inspection générale de la gendarmerie nationale (IGGN), inspection générale de l'administration (IGA), juillet 2009.

(2) Rapport public thématique de juillet 2011, « L'organisation et la gestion des forces de sécurité publique *», Cour des comptes, p. 147.*

– la formation et la pédagogie des agents.

S’agissant de la première finalité, la DGPN a confirmé que le déclenchement de la caméra individuelle lors d’une intervention était de nature à prévenir une escalade. En effet, comme rappelé *supra*, le déclenchement de la caméra individuelle est visible et fait l’objet d’une information par l’agent qui la porte, ce qui peut suffire parfois à calmer la situation.

Ces éléments rejoignent les conclusions du rapport d’évaluation réalisé par le ministère de l’Intérieur et adressé au Parlement sur l’emploi des caméras mobiles par les agents de police municipale :

« *il ressort de l’analyse des rapports transmis que* ***l’utilité du dispositif de caméras mobiles réside davantage dans le caractère dissuasif du port de l’équipement que par son exploitation****, en termes d’enregistrement, de consultation ultérieure ou d’extraction de données provenant des caméras pour les besoins d’une procédure judiciaire, administrative ou disciplinaire. Un nombre important de communes précisent que leurs agents de police municipale n’ont pas eu l’occasion de procéder à un enregistrement* » (1).

● *L’aspect dissuasif des caméras fixes*

Pour M. David Lisnard, maire de Cannes (2), les caméras fixes ont un réel effet dissuasif et contribuent à générer un sentiment de sécurité parmi les citoyens. Cela se traduit par une demande forte d’installation de caméras supplémentaires par les habitants. M. Bernard Gonzalez, préfet des Alpes-Maritimes a également fait état d’un effet dissuasif.

Les élus locaux entendus par vos rapporteurs à l’occasion d’une table ronde ont également souligné le rôle dissuasif des caméras. M. Romain Colas, représentant de l’Association des petites villes de France, a évoqué au cours de l’audition une utilité « objectivement avérée » : les caméras contribueraient à dissuader la commission de certains types de délits : les atteintes aux véhicules, les trafics et même les rixes.

Si le ressenti des parties prenantes est un élément à prendre en compte, peu d’études ont été menées pour objectiver l’effet dissuasif des caméras sur la délinquance, et leurs résultats peuvent apparaître contradictoires.

Une étude rendue à la ville de Nice en mars 2022 (3) s’est penchée sur l’impact des caméras de vidéoprotection de la ville de Nice sur la délinquance de

---

(1) Rapport d’évaluation sur l’expérimentation de l’emploi des caméras mobiles par les agents de la police municipale, ministère de l’Intérieur, 3 août 2018.

(2) Entretien avec M. David Lisnard, maire de Cannes, au cours du déplacement des rapporteurs le 19 janvier 2023.

(3) « L’impact des caméras de vidéosurveillance de la ville de Nice sur la délinquance de voie publique *», Étude d’une élève de l’École polytechnique en partenariat avec la Direction départementale de la sécurité publique des Alpes maritimes.*

voie publique. L'auteur de l'étude a observé l'évolution de la délinquance de proximité dans un secteur progressivement doté de caméras et constaté une division par deux des faits constatés dans le secteur en question. Il conclut que les caméras jouent effectivement un rôle dissuasif.

Les résultats de cette étude peuvent être nuancés par les différents travaux menés par M. Guillaume Gormand. Dans sa thèse soutenue en novembre 2017, le chercheur s'est penché sur le programme de vidéoprotection de la ville de Montpellier [(1)]. Il constate, à l'issue de son évaluation conduite sur plusieurs secteurs de Montpellier :

« *malgré donc l'intuition communément partagée dans l'imaginaire collectif, il apparaît donc clairement que la mise à l'épreuve rigoureuse de ce bénéfice supposé révèle que* ***l'intérêt dissuasif de la vidéosurveillance demeure parfaitement illusoire lorsqu'elle est installée sur des espaces publics ouverts*** » [(2)].

Ainsi, il paraît difficile d'affirmer avec certitude que les caméras fixes ont réellement un effet dissuasif sur la délinquance.

ii. Une efficacité opérationnelle soulignée par les forces de l'ordre, mais qui mériterait d'être évaluée

Il est nécessaire de s'interroger sur l'efficacité opérationnelle de la vidéoprotection.

Pour des municipalités comme Cannes et Nice, qui accueillent régulièrement de grands évènements, la vidéoprotection est perçue comme très utile au maintien de l'ordre public, ainsi que comme un réel atout pour la gestion de crise. La DGGN souligne, quant à elle, l'apport des caméras aéroportées pour les interventions, notamment pour la gestion de grands évènements.

Les représentants des collectivités locales ont fait valoir que les caméras étaient précieuses pour calibrer le niveau d'intervention, par exemple. Ils l'envisagent comme une aide complémentaire de la présence des policiers municipaux sur le terrain.

Les élus locaux ont également évoqué l'« effet plumeau » des systèmes de vidéoprotection, c'est-à-dire le déplacement de la délinquance vers les quartiers et les communes dépourvus de caméras. Les collectivités seraient ainsi progressivement incitées à s'équiper si elles ne le sont pas.

---

(1) « L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de surveillance de la ville de Montpellier », *thèse présentée par M. Guillaume Gormand, Université Grenoble Alpes, 2017.*

(2) Thèse citée supra, *p 332.*

L'étude conduite à Nice et mentionnée précédemment considère aussi que les caméras de la ville constituent « *une aide à l'enquête précieuse* ». Elle conclut que les secteurs les plus vidéosurveillés sont ceux où la part d'élucidation est la plus grande. Elle souligne également qu'entre janvier et février 2022, 18,82 % des faits ont été élucidés grâce à la vidéo. Enfin, elle observe que l'utilisation des caméras permet de diminuer de près de 17 % le temps d'investigation. M. Bernard Gonzalez, préfet des Alpes-Maritimes, lors de son entretien avec vos rapporteurs (1), avait lui aussi mentionné le gain de temps, pour les enquêteurs, rendu possible par les caméras.

Les forces de l'ordre présentent le recours aux images filmées sur la voie publique comme incontournable.

Selon la DGPN (2), le recours par les forces de l'ordre aux images de sécurité peut avoir plusieurs objectifs :

– établir la matérialité des faits ;

– obtenir une description physique de l'auteur de l'infraction ;

– identifier un mode opératoire ;

– orienter les investigations.

Dans sa contribution écrite, la DGPN souligne notamment l'apport des caméras individuelles pour caractériser une infraction, notamment s'agissant de troubles à l'ordre public.

La DGPN comme la DGGN estiment que les enregistrements issus des caméras individuelles sont des éléments précieux pour confirmer la conformité de l'action des forces de l'ordre en intervention.

S'agissant plus particulièrement des LAPI, le renseignement douanier a confirmé qu'il s'agissait d'une technique particulièrement efficace pour lutter contre le trafic de stupéfiants. L'installation de LAPI aux points stratégiques de franchissement des frontières permet de capter beaucoup de passages, et de détecter des convois.

S'il est compliqué d'obtenir des chiffres à l'échelle nationale, certaines statistiques obtenues par vos rapporteurs au cours de leurs déplacements font état d'une utilité de la vidéoprotection lors des enquêtes.

Ainsi, selon la gendarmerie de Loire-Atlantique, de 2017 à 2021, entre 21 et 26 % des délits d'atteinte aux biens ont été élucidés grâce à la vidéoprotection. Cette gendarmerie a communiqué à vos rapporteurs, à titre

(1) Entretien du 19 janvier 2023.

(2) Contribution écrite aux travaux des rapporteurs, à la suite de l'audition du 25 octobre 2022.

d’exemple, une gazette de la vidéoprotection qui répertorie un certain nombre de dossiers résolus grâce à l’exploitation des systèmes de vidéoprotection.

Édition 3e trimestre 2022 – GGD44 – n°03

La Gazette

« Les belles histoires de la vidéoprotection en Loire-Atlantique »

L’enquête judiciaire relative à un enlèvement suivi d’une séquestration et d’actes de tortures et de barbarie, résolue grâce à la vidéo-protection installée par la commune !

Les auteurs initialement décrits par la victime ont pu être identifiés grâce à la vidéoprotection. Cette exploitation de la vidéoprotection de cette commune du nord du département a permis de mettre en cause des co-auteurs et des complices.

Plusieurs d’entre eux ont déjà été écroués en attendant leur jugement.

Fraudes aux moyens de paiement au préjudice de personnes âgées.

Plusieurs arnaques aux distributeurs de billets au préjudice de personnes âgées, suivies de l’usage de ces moyens de paiement dérobés dans les commerces, ont pu être résolus grâce à la vidéoprotection mise en œuvre dans les banques, dans les commerces concernés et sur la voie publique par les communes où les faits ont été commis.

AGENDA

La dernière commission vidéoprotection de la préfecture s’est déroulée **le 30 septembre 2022.** Félicitations aux communes de **Derval, Aigrefeuille-sur-Maine et Sucé-sur-Erdre** pour leurs dispositifs de vidéoprotection qui a été validés par la commission.

Le prochaine commission vidéoprotection de la préfecture est programmée **le 25 novembre 2022.**

FOCUS

Les caméras dites « intelligentes » d’aide à la prise en compte de décisions peuvent être mise en œuvre dès lors qu’elles ne portent pas atteinte aux libertés individuelles des **individus.**

La captation photographique des immatriculations **sans consultation** du fichier des immatriculations peut donc être mise en œuvre pour faciliter le travail d’investigations.

L’information juridique du trimestre

La vidéoprotection fait ses preuves en terme de dissuasion de passage à l’acte et en matière de résolution des enquêtes judiciaires, notamment sur les atteintes aux biens !

En 2016, 500 caméras étaient mises en œuvre par **61 communes** du département et permettaient de résoudre 332 faits avec une contribution de **11,67 %** dans cette résolution.

Entre 2017 et 2021, le nombre de caméras mis en œuvre est passé de 731 à 1627, le nombre de communes équipées est passé **de 79 à 114**, et la contribution de la vidéoprotection dans la résolution des enquêtes atteint à présent **25,79 %** !

Pensez à...

Lors d’un projet de vidéoprotection par une collectivité, il est possible de financer partiellement cette installation en produisant une demande de subvention.

Le **Fonds Interministériel de la Prévention de la Délinquance et de la Radicalisation (FIPDR)** peut être sollicité auprès des services de la **préfecture** sur production d’un dossier matérialisant la charge financière pour la collectivité.

La **Dotation en Equipement des Territoire Ruraux (DETR)** est déjà un mécanisme de subvention connu par les collectivités locales.

Le **Fonds de Compensation de la TVA (FC-TVA)** permet mécaniquement de récupérer la TVA suite aux dépenses publiques d’investissement. Le taux de cette TVA est dans la plupart des cas de 20 %.

cptm.ggd44@gendarmerie.interieur.gouv.fr – 02.28.24.14.18.

Source : gendarmerie de Loire-Atlantique, à l’occasion du déplacement le 27 octobre 2022.

Si l’efficacité des caméras qui filment sur la voie publique est évidente pour les forces de l’ordre, les travaux menés par le chercheur Guillaume Gormand amènent à nuancer ce constat.

Les limites de la vidéoprotection sont mises en avant à plusieurs reprises dans la thèse de M. Guillaume Gormand. Il explique ainsi que le système de vidéoprotection ne se suffit pas à lui-même :

« *il se trouve alors que la vidéosurveillance permet effectivement de découvrir des évènements préoccupants sur la voie publique. Mais évaluer concrètement cette facette du dispositif révèle qu'elle n'est pas infaillible, que l'extension d'un dispositif de vidéosurveillance ne se traduit pas nécessairement par une évolution quantitative ou qualitative de ses découvertes de faits, ou encore que la découverte d'incidents n'entraîne pas mécaniquement de traitement policier* » (1) .

Sur le volet de l'appui à l'intervention policière, il conclut : « *il ressort de l'évaluation que la vidéoassistance des interventions policières présente* ***un fort potentiel****, mais demeure sous-exploitée* » (2).

Sa conclusion est cependant plutôt positive s'agissant de l'apport de la vidéoprotection à la lutte contre l'insécurité. Il estime ainsi qu'il ne faut pas « *sous-estimer l'importance du rôle joué par la vidéosurveillance dans la lutte contre l'insécurité* » (3). Il souligne ainsi de vrais avantages pour les forces de police, comme la rationalisation des interventions de terrain et l'accompagnement appréciable dans la gestion d'évènements sensibles.

Plus récemment, le chercheur a mené une étude à la demande du Centre de recherche de l'École des officiers de la gendarmerie de Melun sur le rôle des caméras dans la résolution d'enquêtes. Son étude portait sur quatre territoires de la métropole grenobloise, et sur les 1 939 cas étudiés, seules 22 enquêtes élucidées ont bénéficié du concours d'images de caméras (4). L'étude montre également que les résultats varient en fonction des infractions : les affaires d'atteintes aux véhicules et de violences connaissent des taux relativement plus élevés.

L'auteur lui-même appelait, dans un article daté de décembre 2021 (5), à relativiser les résultats obtenus et à multiplier les évaluations. Cette demande d'évaluation a également été formulée par les représentantes de l'association La Quadrature du Net, lors de leur audition par vos rapporteurs.

Or, le constat d'un manque d'évaluation n'est pas nouveau.

---

(1) Thèse citée précédemment, *p. 267.*

(2) Thèse précitée, p. 294.

(3) Thèse précitée, p. 415.

(4) Article du journal Le Monde daté du 22 décembre 2021, « Une étude commandée par les gendarmes montre la relative inefficacité de la vidéosurveillance *».*

(5) Dépêche AEF, « Pour le chercheur Guillaume Gormand, « critiquer la vidéosurveillance, c'est s'attaquer à une religion *», publiée le 10 décembre 2021.*

Dans un rapport publié en 2020 sur les polices municipales [(1)], la Cour des comptes a ainsi souligné le manque d'études consacrées à l'efficacité de la vidéoprotection. Elle relève qu'au cours de son enquête sur les polices municipales, « *aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de délinquance commise sur la voie publique, ou encore les taux d'élucidation* » [(2)] . Elle recommande donc de mener une évaluation de la vidéoprotection centrée sur son apport en matière d'élucidation judiciaire et sur les taux d'élucidation. Cette recommandation rejoint celle déjà formulée en 2011 d'engager une évaluation de la vidéosurveillance de la voie publique dans la prévention de la délinquance et l'élucidation des délits selon une méthode rigoureuse [(3)].

Le laboratoire d'innovation numérique de la CNIL, dans un rapport publié en novembre 2021 [(4)], formulait des réserves quant au déploiement de la vidéoprotection dans les petites communes françaises en l'absence d'études démontrant l'efficacité des caméras sur la baisse des délits.

La CNIL a également déploré, dans son avis sur la proposition de loi relative à la sécurité globale, que « *l'efficacité de ces systèmes au regard des objectifs légitimes d'ordre et de sécurité publics n'ait jamais été rigoureusement évaluée de façon globale* » [(5)].

Le peu d'études sur l'efficacité de la vidéoprotection est en effet regrettable, alors même que les systèmes de vidéoprotection représentent des investissements financiers majeurs, que ce soit en matériel ou en ressources humaines. Vos rapporteurs sont donc très favorables à la conduite d'une évaluation sur l'efficacité de la vidéoprotection, afin d'objectiver les éléments donnés par les forces de l'ordre et les magistrats.

Recommandation n° 16 : Conduire une évaluation de l'efficacité de la vidéoprotection.

b. Une preuve parmi d'autres pendant les débats devant le juge

L'exploitation d'images filmées sur la voie publique est incontournable pour les forces de l'ordre lors de l'enquête, comme l'ont confirmé les procureurs représentants de la CNPR. Cette prégnance des images dans les enquêtes ne se retrouve pas au cours des débats : l'utilisation des images pendant les débats devant le juge apparaît bien moins fréquente.

---

(1) « Les polices municipales », *Cour des comptes, octobre 2020.*

(2) Page 70 du rapport précité.

(3) Rapport public thématique précité de la Cour des comptes, juillet 2011, p. 151.

(4) « Les caméras au village », *publication du Laboratoire d'innovation numérique de la CNIL, rédigée par Antoine Courmont et Jeanne Saliou, 19 novembre 2021.*

(5) Délibération n° 2011-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, CNIL.

Devant le tribunal, aucune preuve n'a *a priori* plus de valeur probante qu'une autre : l'article 427 du code de procédure pénale prévoit qu' « *hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve* ». Les preuves doivent être apportées au cours des débats et être contradictoirement débattues devant le juge, qui décide d'après son intime conviction.

L'autorité judiciaire doit cependant respecter un principe de loyauté dans l'administration de la preuve : la Cour de cassation refuse le recours à une preuve qui aurait été obtenue par un procédé déloyal, c'est-à-dire « *tout comportement consistant à s'exempter des garanties inhérentes au cadre légal d'enquête normalement applicable* » (1). Elle considère que « *porte atteinte au principe de loyauté des preuves le stratagème qui en vicie la recherche par un agent de l'autorité publique* » (2).

La Cour de cassation s'est prononcée récemment (3) sur la possibilité d'utiliser un dispositif mobile de captation d'images en vue de la surveillance d'éventuelles infractions. Le plaignant demandait l'annulation dans la procédure des images prises par drone, arguant du fait que l'article 706-96 du code de procédure pénale n'autorisait cette ingérence d'une autorité publique dans la vie privée que pour les seuls dispositifs fixes de captation d'images. La Cour de cassation a considéré qu'il n'y avait pas lieu de faire une distinction entre dispositif fixe ou dispositif mobile. Sous réserve que le cadre d'enquête autorise le recours à cette technique spéciale d'enquête, les images issues de caméras aéroportées peuvent être présentées en procédure.

Les représentants des magistrats entendus ne considèrent pas la vidéo comme une preuve « reine », qui ferait autorité lorsqu'elle est présentée dans une procédure. Elle est pour eux l'un des éléments de preuve qui sert à construire un faisceau de preuves convergentes, mais qui ne se suffit pas à lui-même et doit faire l'objet d'un débat contradictoire lorsqu'il est présenté devant le juge. Les représentants de l'Union syndicale des magistrats (USM) et de la Conférence nationale des procureurs de la République (CNPR) ont néanmoins souligné, au cours de leurs auditions, que la vidéo représentait un élément probatoire essentiel qui pouvait emporter la conviction d'un juge.

La force probante de la vidéo dépend également de la qualité de l'image projetée, et certaines caméras, anciennes ou endommagées, ne permettent pas d'obtenir une image très claire. Pour autant, les magistrats interrogés par vos rapporteurs n'ont pas fait état de contestations fréquentes des images présentées comme éléments de preuve en procédure.

---

(1) « Loyauté de la preuve et stratagèmes : retour sur la mise au point de l'assemblée plénière », *article publié par M. Hugues Diaz le 16 juin 2020, Dalloz.*

(2) Cour de cassation, assemblée plénière, 9 décembre 2019, n° de pourvoi 18-86.767.

(3) Cour de cassation, chambre criminelle, 15 novembre 2022, n° de pourvoi 22-80.097.

Enfin, même lorsque des images ont été exploitées lors de l'enquête, les vidéos sont loin d'être systématiquement projetées lors des débats : ce sont les procès-verbaux (PV) d'exploitation des vidéos réalisés par les agents des forces de l'ordre qui sont utilisés. La contestation du PV d'exploitation peut néanmoins conduire à un visionnage en direct de la vidéo par le tribunal, sous réserve que celui-ci soit correctement équipé. L'USM s'est cependant fait l'écho de difficultés techniques qui freineraient la projection de vidéos au cours des débats.

La possibilité de croiser les sources d'images sur une même scène ou de procéder à des reconstitutions en 3D pourrait être une piste intéressante pour renforcer la valeur ajoutée de la vidéo à l'audience. Cela nécessiterait auparavant des investissements importants en matériels.

Enfin, les représentants du Syndicat de la magistrature considèrent que les magistrats pourraient être davantage formés, au cours de leur cursus à l'École nationale de la magistrature (ENM), au recueil et au traitement des images numériques dans le procès pénal. Vos rapporteurs partagent ces considérations et souhaitent qu'une évolution de la formation initiale soit envisagée.

Recommandation n° 17 : Prévoir un module pour les magistrats lors de la formation initiale à l'École nationale de la magistrature (ENM) sur le recueil et le traitement des images numériques dans l'enquête.

Si les images issues de vidéos sont plébiscitées par les forces de l'ordre, elles sont plus utiles dans le temps de l'enquête que dans le temps du procès. Au-delà des débats sur l'efficacité et l'utilisation des images filmées sur la voie publique, vos rapporteurs constatent un consensus des personnes interrogées sur le potentiel inexploité des caméras, quelles qu'elles soient.

c. Un constat partagé : le potentiel inexploité des caméras

Le nombre de caméras est trop important pour que les opérateurs du système puissent appréhender l'ensemble des évènements filmés par les caméras ou même que l'ensemble des images puissent être affichées en même temps dans le centre de supervision.

Les différents opérateurs ont développé des techniques pour mieux exploiter leur parc de caméras. La mairie de Cannes, par exemple, sélectionne en fonction des horaires les lieux qui sont observés par les opérateurs. Elle privilégie ainsi les caméras postées aux abords des écoles au moment de l'entrée des enfants le matin, et les caméras situées dans les rues commerçantes au moment de la fermeture des commerces. Pour certains sites sensibles, lorsque l'alarme se déclenche, les caméras se braquent automatiquement sur le bâtiment.

La mairie de Nice a également multiplié les dispositifs pour générer les remontées d'informations. **Des boîtiers d'appels** ont été déployés, dans les commerces, les établissements recevant du public, les hôpitaux : lorsque quelqu'un

appuie sur le bouton, les caméras s'orientent vers le lieu d'origine de l'alerte et les images apparaissent sur le poste du centre de supervision. La police municipale procède ensuite à une levée de doute. **Des bornes d'appel d'urgence** sont également déployées depuis 2019 dans les secteurs à forte affluence et devant les écoles, lieux de culte et stations du tramway. Jouant un rôle à la fois d'émetteur et de récepteur, ces bornes sont utilisées pour signaler à la police municipale un évènement sur la voie publique. Les policiers peuvent alors très rapidement accéder aux images et décider de la marche à suivre en connaissance de cause.

L'usage des caméras par les opérateurs de transports

L'aéroport de Paris-Charles-de-Gaulle mobilise 20 à 30 opérateurs pour surveiller les écrans à chaque instant. Les opérateurs se concentrent, par exemple, sur les caméras positionnées au niveau des déposes-minutes pour repérer les voitures garées de manière abusive et les taxis clandestins. L'analyse des images est également précieuse en cas d'intrusion dans les portes identifiées de sûreté. Des scénarii de parcours sont pré-établis et connus des opérateurs, afin de faciliter leur recherche parmi les nombreux flux vidéos. Enfin, une attention particulière est accordée aux zones sensibles et aux sas anti-retours.

La SNCF utilise ses caméras fixes pour faire de la levée de doute lors du déclenchement d'alarmes, par exemple pour écarter l'hypothèse d'un vol de cuivre en cours.

Une problématique partagée : comment favoriser le repérage des bagages délaissés

Lors du déplacement de vos rapporteurs à l'aéroport de Paris-Charles-de-Gaulle, les représentants du groupe Aéroports de Paris (ADP) ont estimé à 5 le nombre de bagages délaissés par jour. Dès lors qu'un bagage délaissé est repéré, il est procédé systématiquement à une analyse vidéo. Si l'analyse vidéo ne suffit pas à lever le doute, il est fait appel aux démineurs. Dans 99 % des cas, il s'agit d'un oubli.

La SNCF est également très soucieuse de détecter le plus rapidement possible les bagages abandonnés et participe, depuis 2018, à un projet européen visant justement à développer des technologies opérationnelles de détection des bagages abandonnés, sur lequel le présent rapport reviendra (voir partie II A 1 b). ..

Le groupe ADP comme la SNCF ont exprimé leurs souhaits de pouvoir exploiter plus efficacement leur parc de caméras en ayant recours à des logiciels d'intelligence artificielle, notamment pour faire du repérage de bagages abandonnés.

L'objectif est d'anticiper les éventuels évènements, afin que l'opérateur en soit averti le plus rapidement possible et déclenche, si nécessaire, une intervention.

Le chercheur Guillaume Gormand, dans sa thèse, faisait déjà le constat que « *les bénéfices policiers de la vidéosurveillance et de ses enregistrements paraissent constituer des potentiels encore inassouvis* » (1).

L'exploitation du potentiel des dispositifs de captation d'images se heurte aux limites humaines, c'est-à-dire à l'impossibilité pour les opérateurs vidéo de repérer en temps réel l'ensemble des évènements sur un écran, et à la difficulté de

(1) Thèse mentionnée précédemment, p. 304.

rechercher *a posteriori* les évènements dans des heures de flux vidéo. Le recours aux caméras « *augmentées* » doit, dans ce contexte, être débattu.

II. LES IMAGES DE SÉCURITÉ FACE AUX DÉFIS CONTEMPORAINS DE L'INTELLIGENCE ARTIFICIELLE

Le déploiement des caméras dans l'espace public aux fins de lutte contre l'insécurité se conjugue aujourd'hui au développement de systèmes d'intelligence artificielle (SIA) destinés à renforcer l'efficacité des dispositifs de captation d'images. Les progrès technologiques majeurs observés au cours de la dernière décennie font évoluer l'équilibre structurel entre sécurité et libertés. D'une part, ils questionnent l'efficacité des moyens dont les forces de l'ordre doivent disposer afin d'accomplir leurs missions. D'autre part, ils interrogent les bornes éthiques à ne pas dépasser, au risque de dévaler la pente vers une société sous surveillance automatique contre laquelle la littérature (1) et le cinéma (2) nous ont mis en garde.

Parmi ces technologies intéressant la captation d'images de sécurité, deux grandes catégories peuvent être distinguées : d'une part, les caméras dites « augmentées » ou « intelligentes », ayant pour seule finalité de détecter des comportements considérés comme anormaux ou dangereux, et, d'autre part, les techniques de reconnaissance biométrique, dont l'objet est d'identifier ou d'authentifier un individu.

A. LES CAMÉRAS « AUGMENTÉES »

Défini selon des cas d'usage prédéterminés, le recours aux caméras « augmentées » a fait l'objet de plusieurs expériences menées ces dernières années, en l'absence de tout cadre légal ou réglementaire adapté. L'expérimentation prévue par le projet de loi relatif aux jeux Olympiques et Paralympiques examiné à l'Assemblée nationale en mars 2023 représente une première étape, dont l'évaluation permettra éventuellement d'envisager, si ses résultats sont probants, sa pérennisation dans le droit commun.

(1) Dans son essai « La France contre les robots *» publié en 1947, Georges Bernanos évoque les convictions libertaires de la bourgeoisie du début du XX^e^ siècle, contrastant avec l'émergence, quelques décennies plus tard, d'une société désormais obsédée par la question sécuritaire : «* Le petit bourgeois français n'avait certainement pas assez d'imagination pour se représenter un monde comme le nôtre si différent du sien, un monde où à chaque carrefour la Police d'État guetterait les suspects, filtrerait les passants, ferait du moindre portier d'hôtel, responsable de ses fiches, son auxiliaire bénévole et public. Mais tout en se félicitant de voir la Justice tirer parti, contre les récidivistes, de la nouvelle méthode, il pressentait qu'une arme si perfectionnée, aux mains de l'État, ne resterait pas longtemps inoffensive pour les simples citoyens. *»*

(2) Voir notamment le film de Steven Spielberg « Minority Report *», réalisé en 2002, tiré de l'ouvrage éponyme de Philip K. Dick.*

1. Des potentialités réelles confrontées à un vide juridique regrettable

a. Un outil d'aide à la décision impliquant de définir préalablement des cas d'usage

Selon la Commission nationale de l'informatique et des libertés (CNIL) (1), les caméras « augmentées » correspondent à des logiciels de traitements automatisés d'images associés à des caméras fixes ou mobiles visant à extraire diverses informations à partir de flux vidéo qui en sont issus (2). La mise en œuvre de ces traitements algorithmiques peut s'effectuer en temps réel, afin de signaler en direct la réalisation d'un événement que le système a pour mission de détecter, ou *a posteriori*, dans le but de repérer et d'isoler le moment au cours duquel l'événement s'est produit. L'usage de ces dispositifs n'est pas circonscrit aux seuls impératifs de sécurité des personnes et des biens relevant du champ des « *smart cities* » (3). L'analyse de flux de fréquentation d'espaces et de transports ou la caractérisation de comportements à des fins commerciales ou publicitaires (4) présentent également des enjeux économiques susceptibles d'intéresser les acteurs privés. Fortement concurrentiel, le marché mondial des caméras « augmentées » a atteint 11 milliards de dollars en 2020, porté par une croissance annuelle de 7 % (5).

Lors de son audition par la mission d'information le 8 novembre 2022, le préfet Michel Cadot, délégué interministériel aux jeux olympiques et paralympiques (JOP), a énuméré les principaux cas d'usage sécuritaires pour lesquels le recours à des caméras « augmentées » pourrait être autorisé à l'occasion des JOP 2024 :

– comptage de densité de foules dans l'espace public et dans les transports en commun (6) ;

– comptage de flux de circulation de véhicules sur des itinéraires prédéfinis ;

– détection de véhicules arrêtés, de la descente de véhicules d'un individu ou d'un groupe d'individus dans une zone non prévue pour des arrêts de véhicules ;

---

(1) CNIL, position sur les caméras « augmentées » ou « intelligentes » dans les espaces publics, juillet 2022.

(2) Les traitements peuvent être couplés à des caméras préexistantes de vidéoprotection ou spécifiquement déployés par le biais de dispositifs de captation d'images ad hoc.

(3) Soit la capacité d'une ville à utiliser les nouvelles technologies afin d'améliorer la qualité de ses services publics. La ville d'Amsterdam s'est par exemple engagée dans cette voie en expérimentant en 2021 une technologie de gestion des foules dans un lieu de baignade très fréquenté par les habitants et les touristes : https://fr.euronews.com/next/2021/08/27/gestion-des-foules-la-solution-intelligente-d-amsterdam

(4) Dans sa position précitée, la CNIL évoque ainsi « la mesure de l'audience des panneaux publicitaires sur la base d'un comptage des individus passant à proximité ».

(5) Étude de marché sur le « machine vision market *» réalisée en 2021 par le cabinet de consultants Marketsandmarkets.com.*

(6) Ce cas d'usage se serait révélé utile afin de prévenir les troubles survenus lors de la finale de la Ligue des champions de football le 28 mai 2022 grâce à l'évaluation des flux de voyageurs en provenance du RER D.

– détection de changements de rythme ou de direction d'un groupe au sein d'une foule, ou d'un groupe de véhicules dans un flux de circulation ;

– détection de regroupement de personnes ou surdensité ponctuelle d'un espace public ;

– détection de port de dispositifs occultant le visage d'un individu ou d'un groupe d'individus au sein d'une foule ;

– détection d'intrusions ou de tentatives d'intrusion par des accès interdits au public (1) ;

– détection d'objets abandonnés ;

– détection du transport d'objets dangereux ou interdits ou brandis par un ou plusieurs individus au milieu d'une foule.

À ces cas d'usage envisagés dans la perspective des JOP 2024 s'en ajoutent d'autres, tels que la surveillance des frontières afin de lutter contre leur franchissement illégal.

Concrètement, ces caméras « augmentées » sont programmées dans l'optique de détecter la réalisation de l'un de ces cas d'usage. La caractérisation d'un tel événement se traduit, en pratique, par l'émission d'un signal d'attention (2) à destination des opérateurs vidéo qui visualisent les écrans projetant en direct les images filmées par ces caméras. Auditionné par vos rapporteurs (3), le professeur de criminologie Alain Bauer a souligné l'intérêt que peuvent représenter ces traitements algorithmiques pour compenser l'affaiblissement progressif – et inévitable – des capacités de concentration et d'attention des opérateurs qui visualisent des milliers d'images pendant plusieurs heures consécutives au sein d'un CSU. Il s'agit ainsi de conjurer un cercle vicieux dans lequel « *l'accoutumance induit la normalité qui entraîne elle-même l'indifférence, avant d'aboutir à la catastrophe* ».

Auditionnée par la mission d'information le 26 octobre 2022, la Délégation ministérielle aux Partenariats, Stratégies et Innovations de Sécurité (DPSIS) du ministère de l'Intérieur a fait état de recherches scientifiques ayant montré que les opérateurs ne parviennent généralement pas à détecter les incidents dans une scène vidéo après 20 minutes de surveillance. Selon la DPSIS, d'autres recherches ont également révélé qu'après 12 minutes de surveillance vidéo continue, un opérateur

---

(1) Lors du déplacement de la mission d'information à l'aéroport Roissy-Charles de Gaulle le 14 décembre 2022, les représentants du Groupe ADP ont indiqué que le suivi d'une personne ayant pénétré dans une zone interdite d'accès nécessite, en moyenne, 45 minutes d'analyse vidéo aujourd'hui. Le recours à des caméras « augmentées » sur ce cas d'usage contribuerait à réduire significativement la durée d'analyse par les opérateurs vidéos en leur permettant de retracer plus facilement le « parcours » des intrus.

(2) Par exemple via un signal lumineux qui éclaire l'écran sur lequel sont projetées les images révélant un événement qui correspond à l'un des cas d'usage.

(3) Audition du 24 janvier 2023.

est susceptible de manquer jusqu'à 45 % de l'activité à l'écran et qu'après 22 minutes de surveillance, il manque jusqu'à 95 % de l'activité.

Le déplacement effectué par la mission d'information à Nantes lors d'un match de football (1) accueillant plus de 30 000 spectateurs au stade de la Beaujoire a sensibilisé vos rapporteurs à la complexité du contrôle opéré par les policiers et les gendarmes chargés de visionner simultanément une dizaine d'écrans, s'agissant notamment d'images de foules compactes dans des tribunes ou aux abords du stade.

Les caméras « augmentées » permettent donc une multiplication capacitaire, en ce qu'elles sélectionnent et repèrent les événements susceptibles de caractériser un danger. L'œil humain demeure bien sûr requis afin d'expertiser le bien-fondé de l'alerte dont l'opérateur aura pris connaissance, avant que celui-ci, le cas échéant, ne décide de diligenter une levée de doutes par l'envoi de personnels sur site. Cette « *vision par ordinateur* » présente aussi l'avantage de s'appuyer sur un réseau de caméras de vidéoprotection déjà existant, ce qui contribue à valoriser le parc de caméras, tout en facilitant la réaffectation des agents sur le terrain par la réduction du nombre d'opérateurs chargés de visionner les écrans.

(1) Déplacement à Nantes le 27 octobre 2022.

L'utilisation *a posteriori* des caméras « augmentées »

De manière complémentaire à l'usage de la vidéo augmentée en temps réel, les besoins opérationnels des policiers se concentrent également sur l'analyse *a posteriori* des milliers d'heures de vidéos collectées dans le cadre des enquêtes pénales. Notre ancien collègue Cédric Villani a montré l'étendue des bénéfices que comporte le recours en différé aux traitements algorithmiques appliqués à des flux vidéo :

« *L'IA offre ici de nouvelles perspectives, car elle permet non seulement de mieux exploiter les données produites en continu par les systèmes, mais également de mieux exploiter le patrimoine amassé efficacement. À titre d'exemple dans la recherche de contenu dans un ensemble de vidéos, quand il aurait précédemment fallu faire visualiser ces vidéos minute par minute par un ensemble d'opérateurs humains, il est aujourd'hui envisageable d'utiliser des techniques d'IA pour faire ce travail de façon automatique et beaucoup plus rapide.* » (1)

Selon la direction générale de la police nationale (DGPN), auditionnée par la mission d'information le 25 octobre 2022, l'intelligence artificielle pourrait assister l'opérateur afin de procéder à une ré-identification d'objets ou d'individus dans une courte période de temps, là où le traitement des images s'effectue encore de façon manuelle et donc fastidieuse. Dans cette perspective, la DGPN travaille avec la gendarmerie et la préfecture de police au déploiement d'un logiciel d'aide à la détection d'images permettant à un enquêteur d'analyser plus rapidement des flux vidéos issus de sources variées, tels que des extraits de vidéoprotection ou de vidéos saisies dans des supports informatiques.

Lors de son audition le 26 octobre 2022, la *start-up* XXII, l'un des leaders français de l'analyse intelligente de flux vidéos, a présenté à vos rapporteurs les contacts réguliers qu'elle entretient avec les services du ministère de l'Intérieur et du ministère de la Justice afin de mettre en œuvre des solutions d'analyse ciblées d'images issues de caméras de vidéoprotection.

Dans sa position publiée en juillet 2022, la CNIL soulève le risque d'une « *analyse généralisée des personnes* » dont l'ampleur dépend du « *potentiel d'adaptabilité à des cas d'usage potentiellement illimités* ». La détermination des cas d'usage doit être effectuée de la façon la plus neutre possible, en identifiant avec un maximum d'objectivité les situations qui présentent effectivement un risque pour la sécurité des personnes et des biens. Pour autant, ce sont les paramètres pris en compte par l'algorithme, notamment ceux susceptibles de cibler des critères comportementaux (2), qui peuvent exposer les personnes filmées à des risques discriminatoires.

(1) Cédric Villani, « Donner un sens à l'intelligence artificielle *», rapport remis au Premier ministre, mars 2018, pp. 220-221.*

(2) Dans son étude adoptée en assemblée générale plénière le 31 mars 2022 et intitulée « Intelligence artificielle et action publique : construire la confiance, servir la performance *», le Conseil d'État mentionne la conception par une entreprise japonaise d'un outil (AI Guardman) destiné à détecter les vols à l'étalage à partir du langage corporel des auteurs, en comparant les gestes effectués avec des « modèles suspects » prédéfinis, tels que des regards alentour pour s'assurer de l'absence de témoin visuel ou des modalités de prise d'un produit en rayon.*

Comme le rappelle l'Alliance pour la confiance numérique (ACN), entendue par vos rapporteurs le 12 octobre 2022, ces enjeux renvoient à la nécessité de « *détourer des familles d'usage* » de façon suffisamment précise pour constituer une véritable aide à la prise de décision humaine, sur la base des signalements réalisés par les traitements algorithmiques et sans que ces derniers n'entraînent en conséquence une décision systématique ni prédéterminée (1).

Dans son rapport remis au Premier ministre en septembre 2021, notre ancien collègue Jean-Michel Mis tempère, à raison, les risques que l'utilisation de ces caméras « augmentées » est susceptible d'engendrer :

« *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 explicitée 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.* » (2)

Si vos rapporteurs souscrivent à cette analyse, les premiers retours d'expériences portés à leur connaissance soulèvent plusieurs interrogations quant à la fiabilité de certaines de ces technologies.

b. Des expérimentations récentes aux résultats contrastés

Les auditions conduites par la mission d'information ont fait état de plusieurs expériences menées au cours des dernières années à l'initiative de l'État, d'opérateurs de transports, tels que la RATP et la SNCF, et de municipalités. L'ensemble de ces expérimentations s'est déroulé sous le contrôle de la CNIL. Présentés de façon synthétique, les résultats communiqués à vos rapporteurs apparaissent hétérogènes.

S'il est par nature délicat de contre-expertiser les bilans réalisés, il conviendrait de définir en amont de l'expérimentation un cadre d'évaluation à la fois plus précis et standardisé, afin de garantir la pleine objectivité de ces « rétex ». Par ailleurs, certaines expérimentations semblent avoir été effectuées dans des conditions peu satisfaisantes au regard des exigences d'information et de publicité auxquelles elles demeurent soumises (3).

---

(1) Position de l'ACN sur la consultation publique portant sur le projet de position de la CNIL relative aux conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics, 11 mars 2022.

(2) Jean-Michel Mis, « Pour un usage responsable et acceptable par la société des technologies de sécurité »*, rapport remis au Premier ministre, septembre 2021, p. 23.*

(3) Voir ainsi le paragraphe 4.2.4 de la position de la CNIL publiée en juillet 2022.

Auditionnée le 1er février 2023 par la mission d'information, l'entreprise Thales a ainsi présenté un « rétex » de l'expérimentation de caméras « augmentées » installées en 2020-2021 dans la ville de Reims. Cette expérimentation n'a semble-t-il fait l'objet d'aucune information de la part de la municipalité vis-à-vis des citoyens ni même du conseil municipal (1). Vos rapporteurs regrettent l'opacité qui peut entourer la mise en œuvre expérimentale de ces dispositifs : ces zones d'ombre, contraires aux règles prévues par le règlement UE 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 (RGPD) et que rien ne justifie en pratique, nuisent autant au bon déroulement des expérimentations qu'à leur évaluation sereine et objective. **Elles nourrissent ainsi les fantasmes et postures dogmatiques, en jetant le doute quant à leurs finalités réelles, à rebours des objectifs poursuivis par les promoteurs de ces projets.**

Recommandation n° 18 : Déterminer un cadre d'évaluation objectif, précis et standardisé des expérimentations de dispositifs de vidéoprotection « augmentée » et garantir le respect des obligations d'information du public.

Les éléments ci-après ont été transmis par Thales à l'issue de son audition.

(1) « Reims expérimente une intelligence artificielle de Thales pour surveiller ses habitants, et personne n'est au courant », *Street Press, 26 janvier 2023.*

Éléments d'information et de contexte relatifs à l'expérimentation d'analyse de flux vidéo conduite à Reims par Thales.

Dans le cadre de projets de mobilité et de sécurité urbaines avec la ville de Reims, Thales a initié en 2020-2021 une collaboration technologique, en sous-traitance d'un industriel délégataire d'une mission de service public, dans laquelle un logiciel d'analyse de flux dynamique vidéo « Savari » a été testé pour détecter certains comportements et situations à risque, et en faire l'analyse rapide *a posteriori*.

Les cas d'usage retenus pour expérimenter l'intérêt opérationnel ou non du prototype de cette solution se sont concentrés sur la détection des fraudes et incivilités pour les opérateurs de transports, et, en lien avec le Centre de Supervision Urbaine (CSU), sur la détection des dégradations volontaires du réseau de caméras de vidéoprotection, l'analyse d'accident de la circulation ou encore la limitation des regroupements pendant les phases aiguës de pandémie Covid.

En amont et en aval de ce POC (Preuve de concept), Thales est resté vigilant sur l'environnement légal et juridique de cette expérimentation et sur l'absence de dérives possibles : toutes les démarches préalables d'analyse d'impact sur la protection des données (AIPD) ont été conduites sous la responsabilité de l'industriel de premier rang délégataire, en relation régulière avec la préfecture de la Marne. En cas de commission d'une infraction dans le champ d'une caméra, toute lecture et analyse d'images vidéo *a posteriori* et accès aux données étaient systématiquement placés sous la responsabilité d'un officier de police judiciaire ou d'un magistrat. Aucun recours à la reconnaissance faciale ou à l'identification de personne n'a été intégré « nativement » dans la solution. Enfin, le principe d'un échange exhaustif avec la CNIL, à la fin du POC, a été retenu par l'industriel délégataire, les autorités et la CNIL ; avec la contribution souhaitée de Thales.

Le bilan de l'expérimentation est le suivant.

Une pertinence opérationnelle démontrée : avec une très bonne acceptation de cette solution innovante par l'ensemble des acteurs (opérateurs de transport et du CSU, police municipale, industriel délégataire, collectivité et préfecture) et un gain opérationnel perceptible dans le cadre légal existant, sous la supervision du procureur. Des gains de productivité majeurs ont été constatés (en qualité : très peu d'erreurs avant validation humaine, et en temps d'analyse, divisé par 30) dans les phases critiques des enquêtes.

Des difficultés en lien direct avec le contexte COVID ont mis en échec le passage à l'échelle de la solution : en termes de déploiements techniques mais surtout de ressources humaines, ces contraintes sont venues impacter la phase de tests de cette solution prototype et ont conduit au début de l'année 2022 à l'arrêt de l'expérimentation et des développements associés. Le passage à l'échelle industrielle de la solution « Savari » n'a pas été décidé par la branche de Thales en charge de la politique produit et des briques technologiques de solutions globales de type smart cities.

Source : contribution écrite remise par Thales à l'issue de son audition par la mission d'information.

Depuis 2019, le Secrétariat général de la Défense et de la Sécurité nationale (SGDSN) a conduit une analyse du besoin et lancé une opération d'identification des technologies susceptibles de contribuer à la sécurisation de grands évènements internationaux. Plus de 220 solutions technologiques ont été proposées par plus d'une centaine d'entreprises en réponse à ce besoin.

Lors du tournoi de Roland-Garros organisé en septembre-octobre 2020 (1), plusieurs cas d'usage ont été expérimentés s'agissant de la détection des mouvements de foule anormaux et du comptage des flux d'entrée et de sortie. Les « rétex » communiqués à vos rapporteurs présentent des conclusions relativement positives. Sur le plan capacitaire, les évaluations techniques des solutions proposées en matière de densité de spectateurs, ainsi que de flux d'entrée et de sortie, ont conclu à leur bonne adaptation aux cas d'usage, attestant d'un niveau de fiabilité satisfaisant. En revanche, le document précise que « *la détection des comportements suspects n'est pas suffisamment fine pour une intégration opérationnelle* » (2). En outre, les analyses d'impact réalisées par les entreprises ont hélas été transmises trop tardivement à la CNIL pour qu'elle puisse se prononcer en temps utile sur la régularité de l'expérimentation au regard du cadre juridique existant.

En parallèle, le programme d'expérimentations technologiques de sécurité pour la gestion des grands événements conduit par le ministère de l'Intérieur s'opère dans le cadre du contrat stratégique de filière passé entre l'État et les industries de sécurité en 2019. Il vise à évaluer les besoins opérationnels des forces et à y répondre par des outils technologiques innovants. Ce programme doit permettre de proposer une sélection de solutions adaptées à la sécurisation de l'espace public, en étant interopérables et compatibles avec les systèmes existants, dans le but de garantir une meilleure coopération entre les forces de sécurité. Sous l'égide de la DPSIS, près de 170 expérimentations unitaires intégrant, pour certaines d'entre elles, l'usage de caméras « augmentées » ont eu lieu entre avril et décembre 2022. (3)

Sous le contrôle de la CNIL, et en mobilisant à cette fin plusieurs dizaines de volontaires, trois cas d'usage ont par exemple été testés dans la nuit du 20 au 21 octobre 2022 à la Gare du Nord, au moment de sa fermeture au public : la détection de chute d'une personne au sein d'un groupe, le passage de personnes en contre-sens et le port d'une arme. Lors de leur audition par la mission d'information, la SNCF et la DPSIS ont présenté un premier « rétex » de ces expérimentations, dont le bilan complet n'est pas encore disponible. Comme le reconnaît la DPSIS, les résultats obtenus apparaissent contrastés, tant en raison de la faible maturité de certaines technologies que des conditions dans lesquelles plusieurs expérimentations ont été effectuées.

(1) Organisé habituellement en mai-juin, le tournoi 2020 a été décalé en raison de la crise sanitaire.

(2) Document transmis par le SGDSN à la mission d'information à la suite de son audition le 15 novembre 2022.

(3) Pour un montant total d'environ 21 millions d'euros.

« Rétex » transmis par la DPSIS sur les trois expérimentations menées avec la SNCF à la Gare du Nord les 20 et 21 octobre 2022

Plusieurs solutions techniques proposées par des entreprises sélectionnées afin de participer à ces expérimentations ont été mises en œuvre dans la nuit du 20 au 21 octobre 2022 à la Gare du Nord, dans le but de détecter en temps réel des contre-sens et franchissements de zone interdite, des personnes au sol et le port d'urne arme. Les tests ont eu lieu dans un environnement fermé avec trois caméras filmant la scène, dont une caméra d'angle. L'ensemble de ces solutions se sont facilement intégrées au système de vidéoprotection de la Gare du Nord, soulignant ainsi leur interopérabilité. La visualisation des alarmes a été réalisée à travers l'interface graphique de chaque solution. De manière générale, les alarmes peuvent également être visualisées via n'importe quelle interface graphique existante, telle que celle du CSU concerné.

1° Test sur l'entrée à contre-sens d'une personne et le franchissement de zone interdite

Quatre solutions ont été mises en œuvre. Les trois premières solutions proposées atteignent des performances satisfaisantes sur l'ensemble des scénarios de tests, présentant des taux de détection élevés et peu de fausses alarmes. La quatrième solution n'a pas déclenché d'alertes lors de ces expérimentations, après avoir rencontré un problème technique.

2° Test sur la détection d'une personne au sol

Les trois solutions déployées ont présenté des résultats insatisfaisants sur l'ensemble des scénarios de test, avec des taux de détection presque nuls pour les deux premières et des dizaines de fausses alarmes pour la dernière, bien que celle-ci ait réussi à détecter avec succès 64 % des situations sur deux caméras.

3° Test sur le port d'une arme

Les deux solutions mises en œuvre ont présenté des résultats insatisfaisants sur l'ensemble des scénarios de test, avec des taux de détection presque nuls et des dizaines de fausses alarmes. Cependant, la seconde solution a réussi à détecter avec succès 28 % des situations sur deux caméras.

Source : contribution écrite remise par la DPSIS en février 2023.

À l'issue de ces expérimentations, la DPSIS a fourni plusieurs explications et recommandations destinées à améliorer, à terme, l'efficacité de ces dispositifs de vidéoprotection « augmentée ».

Premièrement, la DPSIS considère que les performances décevantes des systèmes mis en place afin de détecter les personnes au sol s'expliquent par la défaillance des réglages préparatoires :

« *Dans la détection de personnes au sol, deux calibrations préliminaires sont essentielles afin de valider la verticalité des personnes en tenant compte des aberrations optiques : personnes debout et personnes allongées. Les experts* […] *expliquent dans leur rapport technique qu'en raison du temps de configuration réduit le soir de l'expérimentation à la Gare du Nord, le double calibrage a été abandonné au profit d'un seul calibrage sur des personnes debout. Des*

ajustements ont été apportés à ce dernier pour maximiser les chances d'obtenir des images pertinentes en un minimum de temps. Malheureusement, ceci a entraîné un dysfonctionnement de l'application. Dans la détection de contresens, une calibration est nécessaire afin de calculer les points de contacts des volontaires au sol et ainsi déterminer leurs positions par rapport à une zone / ligne. En revanche, en raison du temps de configuration réduit, cet algorithme de calibration n'a pas été utilisé, ce qui a conduit à des faux positifs dans certains scénarios. » (1)

Deuxièmement, la DPSIS met en relief un phénomène de « décalage des données » témoignant d'une distorsion entre les données ayant servi à entraîner les algorithmes et celles que ces derniers avaient pour mission de caractériser le jour du test :

« *Les mauvais résultats obtenus lors des expérimentations de détection de personnes au sol et de détection d'armes à feu à la Gare du Nord la nuit du 20 au 21 octobre ne mettent pas en cause la robustesse des modèles IA utilisés mais plutôt les données sur lesquelles les réseaux de neurones ont été entraînés* [...] *Il semble que les mauvais résultats obtenus en Gare du Nord soient dus à un problème appelé "décalage des données". Le décalage des données ("data shifting") est un problème courant dans les modèles de vision par ordinateur, qui se produit lorsque la distribution conjointe des entrées et des sorties diffère entre les étapes d'apprentissage et de test. Le décalage des covariables, un cas particulier de décalage des ensembles de données, se produit lorsque seule la distribution des entrées change. Dans les expérimentations de détection de personnes au sol et de détection d'armes à feu, il semble qu'il y ait un écart important entre les données sur lesquelles les réseaux de neurones ont été entraînés et les données de la Gare du Nord sur lesquelles ces réseaux ont été testés. Ce problème pourra être résolu à l'avenir en entraînant les réseaux de neurones des solutions sur des images de la Gare du Nord.* » (2)

Auditionné par la mission d'information le 12 octobre 2022, le Pr. François Terrier, directeur du programme Intelligence artificielle de l'Institut CEA List, résume cet enjeu de la façon suivante : « *si la réalité dépasse la base de données, l'algorithme sera hors* scope [champ] *de manière systématique* ». La métaphore sportive permet utilement d'appréhender cette contrainte : les performances constatées au cours des entraînements ne préjugent en rien de celles réalisées lors des compétitions.

Troisièmement, s'agissant spécifiquement du cas d'usage de détection de personnes au sol, la DPSIS souligne la difficulté inhérente à « l'estimation de pose », qui consiste à localiser les articulations humaines connues sous le nom de « points clés », tels que les coudes et les poignets :

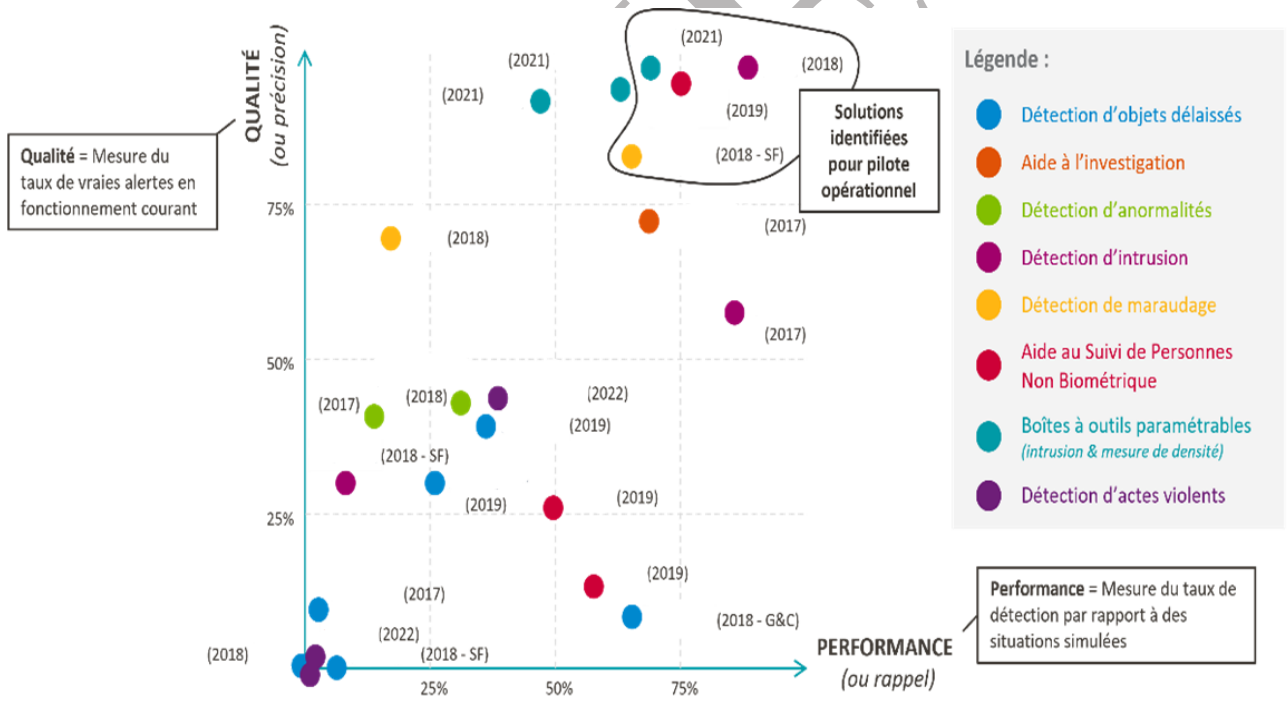
---

(1) Document transmis par la DPSIS à la mission d'information en février 2023.

(2) Idem.

« *Chaque personne est composée d'un certain nombre de points clés. Des lignes sont ensuite tracées entre les paires de points clés pour réussir à dessiner la forme approximative d'une personne. Il y a de nombreuses méthodes d'estimation de pose en fonction de l'entrée et des méthodes de détection. Néanmoins, l'estimation de pose est une tâche difficile dans un environnement réel en raison de la difficulté de détection des articulations (parfois assez petites et peu visibles surtout lorsque les personnes sont loin des caméras), des occlusions, des vêtements et des variations d'éclairage.* » (1)

Particulièrement investie dans le développement des caméras « augmentées » pour des raisons aussi bien commerciales que sécuritaires, la SNCF a également procédé à plusieurs dizaines d'expérimentations depuis 2017. Sous le contrôle de la CNIL, la SNCF a sollicité des grandes entreprises françaises et étrangères ainsi que des *start-up* afin de tester, en conditions réelles, des technologies répondant à des cas d'usage strictement délimités. Là encore, les résultats obtenus varient fortement selon l'objectif assigné à ces caméras « augmentées » :



Source : contribution écrite remise par la SNCF à la suite du déplacement de la mission d'information à la maison de la sûreté de la SNCF à Paris le 30 novembre 2022.

Ces « rétex » illustrent la nécessité de développer avec rigueur, et sur la durée, l'apprentissage des algorithmes. Vos rapporteurs soulignent la sensibilité des processus d'entraînement des systèmes d'intelligence artificielle qui leur ont été présentés lors des déplacements et auditions organisés dans le cadre de la mission d'information : leur cheminement est par essence long, tortueux, itératif. La performance réelle des traitements algorithmiques dépend autant de la représentativité des données d'apprentissage sur lesquels ils ont été bâtis que des

(1) *Idem.*

conditions dans lesquelles ils ont été testés. L'environnement d'un laboratoire n'est pas comparable à celui d'une gare ou d'un aéroport, ce qui peut expliquer des différences majeures de résultats et conduire à s'interroger sur la fiabilité des dispositifs mis en œuvre.

En outre, leur efficacité diffère selon les cas d'usages pour lesquels ils ont été programmés : si le comptage d'un flux de spectateurs ou le repérage d'un individu dans une zone interdite correspondent aujourd'hui à des technologies matures, la détection de personnes au sol, d'objets abandonnés (1), de mouvements de foule ou du port d'une arme présentent une relative complexité, en dépit de l'ampleur des progrès technologiques récemment accomplis.

Par ailleurs, l'usage de caméras « augmentées » suppose également la formation de tous les opérateurs vidéos à l'exploitation de ces outils. La multiplication de signaux d'attention détectant, par erreur, des situations n'ayant en effet pas lieu d'être « suspectes », peut représenter une véritable difficulté pour les agents qui visualisent les écrans. Ils seraient alors confrontés à de potentielles fausses alertes à expertiser le plus rapidement possible. Ces obstacles ne sont pas insurmontables, mais ils ne doivent pas être méconnus ou minimisés – au risque de complexifier la prise de décision et ainsi de perturber l'exercice des missions des forces de sécurité sur le terrain, soit l'exact opposé du but recherché.

c. Le silence du droit : un vide qu'il revient au législateur de combler

Dans le cadre de la stratégie nationale de prévention de la délinquance 2020-2024 élaborée par le Gouvernement en mars 2020 (2), la mesure n° 26 visait l'objectif suivant : « *En matière de vidéoprotection, expérimenter le traitement automatisé de l'image, dans le respect des libertés individuelles* ». L'action correspondant à la mesure était ainsi formulée : « *Tester la connexion avec des logiciels de détection des situations comportant un danger manifeste* (3)*, à l'exclusion de tout traitement permettant l'identification directe ou indirecte des personnes physiques* ».

Ces injonctions des pouvoirs publics à expérimenter l'usage des caméras « augmentées » se heurtent au flou du cadre juridique applicable. Les articles L. 251-1 à L. 255-1 du code de la sécurité intérieure encadrant la vidéoprotection ne prévoient aucune disposition relative à l'utilisation de traitements algorithmiques destinés à détecter en temps réel ou en temps différé des

---

(1) À ce titre, un projet européen intitulé « Prevent PCP *» a été lancé en septembre 2021 dans le but de faire émerger, au sein de l'Union européenne, des solutions de vidéo intelligente répondant à ce besoin. Financé par la Commission européenne à hauteur de 12 millions d'euros et réunissant 24 partenaires, dont la SNCF et la RATP, dans huit pays européens, ces technologies seront testées dans la gare de Paris Nord lors de la Coupe du monde de rugby 2023.*

(2) https://www.cipdr.gouv.fr/wp-content/uploads/2020/03/Tome-1-SNDP-INTERACTIF-1.pdf

(3) Tels qu'un « mouvement de foule inhabituel ou anormal, des cris soudains, une intrusion dans un espace interdit ou le départ d'un incendie ».

événements particuliers. Deux interprétations divergentes peuvent alors être retenues.

La première consiste à considérer que le droit actuel n'interdit pas l'usage pérenne des caméras « augmentées », dès lors que celui-ci se conforme aux obligations découlant des règles prévues par le code de la sécurité intérieure et par la loi « Informatique et Libertés » du 6 janvier 1978.

La seconde appréhende ces nouvelles technologies comme des outils d'une autre nature que celle des dispositifs traditionnels de captation d'images. Lors de son audition le 18 octobre 2022, la CNIL estime qu'il s'agit en effet « *d'un changement d'échelle et de nature dans la surveillance des populations, de leurs attributs et comportements individuels et collectifs* ». L'impact des caméras « augmentées » sur les données à caractère personnel (1), quand bien même elles ne sauraient aboutir à identifier les personnes, s'avère supérieur à celui des caméras de vidéoprotection sans intelligence artificielle, ce qui, selon la CNIL, rend donc indispensable la création d'un cadre juridique spécifique et adapté à ces enjeux :

« *De tels usages de ces dispositifs, même limités dans le temps et l'espace, seraient en effet susceptibles d'affecter les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques et relèveraient donc des domaines réservés à la loi conformément à l'article 34 de la Constitution.* » (2)

Dans une position formulée en juillet 2022 à l'issue d'une consultation publique ouverte six mois plus tôt, la CNIL considère qu'aucune disposition législative en vigueur n'autorise expressément l'utilisation, par la puissance publique, des caméras « augmentées » pour la prévention et la répression d'infractions. Pour autant, la CNIL relève que le recours à ces traitements algorithmiques n'est pas « illicite » par principe. Leur usage requiert un examen au cas par cas des finalités pour lesquels ces dispositifs sont susceptibles d'être mis en œuvre et de leurs modalités de fonctionnement, qui demeurent assujetties au respect des règles prévues par le RGPD et par la loi « Informatique et Libertés ». La légitimité de l'intérêt poursuivi par le responsable du traitement, la nécessité de ce traitement de données (3) et l'absence d'atteinte disproportionnée aux intérêts et droits des personnes concernées constituent les critères habituels à l'aune desquels la CNIL autorise ou non l'expérimentation envisagée.

(1) La CNIL considère que la gradation des risques et de l'impact pour les personnes est fonction de la nature des informations traitées et des décisions prises à l'issue de l'analyse réalisée par l'outil de vidéo « augmentée ». Selon la CNIL, les dispositifs qui auront pour objectif ou pour effet une prise de décision ou des conséquences au niveau individuel engendreront une intrusivité et un risque généralement plus élevés pour la personne que ceux qui ne produisent que des informations agrégées (statistiques) ou des décisions concernant un ensemble de personnes.

(2) Document transmis à la mission d'information par la CNIL, à la suite de son audition le 18 octobre 2022.

(3) L'examen de la nécessité suppose d'évaluer l'existence ou non de moyens moins intrusifs afin d'atteindre la finalité recherchée ainsi que la performance opérationnelle du dispositif au regard de l'objectif poursuivi.

Rejoignant la position exprimée par le Conseil d'État dans un son avis du 12 octobre 2021 [(1)], les observations de la CNIL publiées en juillet 2022 mettent un terme à plusieurs années d'incertitudes et de tâtonnements quant à la légalité de ces technologies déployées dans l'espace public, qu'elles présentent un caractère temporaire ou pérenne.

Vos rapporteurs se félicitent de cette clarification : elle ouvre désormais la voie à la construction d'un cadre expérimental de l'usage des caméras « augmentées » dont il revient au législateur, conformément à l'article 34 de la Constitution, de déterminer le contenu et de fixer les contours [(2)]. Ils observent cependant que les incertitudes juridiques latentes ont provoqué le ralentissement, voire l'abandon d'expérimentations au regard des doutes soulevés quant à leur licéité. Les conséquences furent particulièrement néfastes : incapacité à tester et à évaluer des techniques « grandeur nature », frein à la compétitivité des *start-up* développant ces technologies et dépendance subséquente à des produits commercialisés par des entreprises étrangères.

Auditionné par la mission d'information le 12 octobre 2022, M. Xavier Fischer, président de la *start-up* Datakalab, a souligné à quel point l'indécision des pouvoirs publics en la matière a fragilisé le processus industriel de nombreuses petites et moyennes entreprises ayant investi ce segment de marché. Cette aboulie politico-administrative a également conduit à entraver les moyens d'action dont disposent l'État, les opérateurs de transports et certaines grandes municipalités afin de moderniser leurs outils de vidéoprotection. L'absence de cadre juridique a ainsi pu dissuader les acteurs de l'écosystème de l'intelligence artificielle de recourir, même dans le cadre d'expérimentations très encadrées et sous le contrôle de la CNIL, à ces technologies innovantes.

Ce constat est partagé par la DPSIS. Ses représentants ont rappelé l'étendue des contraintes auxquelles ces expérimentations sont soumises, insistant notamment sur le recours exclusif à des volontaires et sur la rigidité de leur cadre spatio-temporel, en l'absence de fondement légal *ad hoc*. Cette situation a provoqué un ralentissement du rythme des expérimentations et accentué les retards déjà accumulés. Pourtant, comme l'a relevé l'entreprise Bouygues ES lors de son audition le 11 octobre 2022, les besoins exprimés par les forces de sécurité s'amplifient, alors même que les fournisseurs français de solutions innovantes seraient en mesure de répondre à leurs attentes.

Dans cette perspective, l'article 7 du projet de loi relatif aux jeux Olympiques et Paralympiques adopté par l'Assemblée nationale le 11 avril dernier

---

(1) Le rapport d'information n° 627 des sénateurs Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain publié en mai 2022 mentionne un avis du Conseil d'État du 12 octobre 2021, non-publié, qui considère que les traitements des images issues de la vidéoprotection par le biais d'un logiciel d'intelligence artificielle constituent des traitements de données personnelles distincts de ceux des images issus de la vidéoprotection.

(2) Sur le fondement de l'article 23 du RGPD, il apparaît à ce titre nécessaire d'encadrer à l'échelle législative les modalités – sinon l'exclusion – du droit d'opposition.

représente une opportunité afin d'expérimenter les caméras « augmentées », à la seule fin de garantir la sécurité des grandes manifestations sportives, récréatives ou culturelles.

2. La nécessité de définir un cadre conciliant souplesse et stabilité

L'article 7 du projet de loi relatif aux jeux Olympiques et Paralympiques fixe pour la première fois au niveau législatif le cadre expérimental de l'usage des caméras « augmentées ». Il conviendra d'évaluer dès la fin des JOP 2024 la mise en œuvre de ces traitements algorithmiques, qu'il s'agisse de leurs modalités d'autorisation et de fonctionnement, de leur intérêt opérationnel ou des enjeux de souveraineté que leur utilisation soulève.

a. Le cadre expérimental prévu par le projet de loi JOP 2024

L'article 7 du projet de loi autorise l'expérimentation des caméras « augmentées » dans l'espace public jusqu'au 31 mars 2025 [(1)] à la seule fin d'assurer la sécurité des manifestations sportives, récréatives ou culturelles susceptibles d'être exposées, en raison de leur ampleur et de leurs circonstances, à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes.

La délimitation du cadre spatio-temporel de cette expérimentation a suscité de nombreux débats parlementaires. D'une part, il est tout à fait légitime que l'expérimentation à grande échelle, c'est-à-dire au-delà des initiatives locales mobilisant uniquement des personnes volontaires, soit encadrée par des bornes raisonnables, au regard de son caractère dérogatoire au droit commun. D'autre part, il est tout aussi nécessaire de laisser un temps suffisant pour garantir le bon développement de ces technologies, dans le but de tester des produits « matures » dans les meilleures conditions possibles.

Sous réserve de la décision que rendra le Conseil constitutionnel sur la loi JOP 2024, le déploiement de ces caméras « augmentées » n'interviendra pas avant l'automne 2023, eu égard aux contraintes de délais auxquelles seront soumises les phases d'acquisition, de développement et d'autorisation de ces traitements algorithmiques. Si ce calendrier était hélas prévisible, compte tenu des délais de promulgation de la loi puis de *sourcing*, de passation et d'attribution des marchés publics qui permettront à l'État de se doter de ces technologies, vos rapporteurs regrettent que l'expérimentation ne puisse probablement pas débuter à l'occasion des matchs de la Coupe du monde de rugby. Organisé dans neuf villes entre le 8 septembre et le 28 octobre 2023, cet événement planétaire devrait attirer plusieurs millions de spectateurs français et étrangers pendant sept semaines. Il présenterait

(1) Le Gouvernement avait repoussé la fin de l'expérimentation du 31 décembre 2024 au 30 juin 2025, conformément à la préconisation émise par le Conseil d'État dans son avis rendu sur le projet de loi (p. 9). Lors de son examen en première lecture, le Sénat a choisi de maintenir cette date. La commission des Lois de l'Assemblée nationale a rétabli le terme de l'expérimentation au 31 décembre 2024, conformément à la volonté initiale du Gouvernement. Le texte adopté par la commission mixte paritaire réunie le 4 avril 2023 a finalement fixé au 31 mars 2025 le terme de l'expérimentation.

de nombreuses similitudes avec les JOP 2024, tant en termes d'organisation que d'affluence dans les stades et les fan zones. Auditionnée le 7 décembre 2022, la chercheuse au CNRS Myrtille Picaud rappelle ainsi la singularité de ces manifestations sportives :

« *Les grands événements sportifs, comme les JOP, la Coupe du monde de rugby accueillie en France en 2023, sont centraux dans la mise en œuvre de dispositifs de sécurité pour l'espace urbain. Ces grands événements emblématiques sont susceptibles de favoriser un consensus politique sur la nécessité de faire évoluer le cadre règlementaire afin de permettre leur autorisation.* […] *Finalement, ces événements offrent autant d'expérimentations de dispositifs qui nécessitent un calibrage en conditions réelles* ». (1)

Il est dommageable de ne pas avoir mieux anticipé cette échéance en présentant dès l'été 2022 le projet de loi relatif aux JOP 2024, dont l'organisation a été attribuée à la France en septembre 2017. Ce retard législatif, également déploré par la Délégation interministérielle aux jeux olympiques et paralympiques (DIJOP) (2), force aujourd'hui les pouvoirs publics à mener une véritable « course contre la montre », sans doute déjà perdue s'agissant du Triathlon de Paris (3) et de la Coupe du monde de rugby, afin de disposer de technologies suffisamment matures pour être pleinement opérationnelles à l'occasion des JOP 2024.

Le projet de loi prévoit que ces traitements algorithmiques s'appliqueront aux images captées par des systèmes de vidéoprotection et par des caméras aéroportées (4). Son article 7 prévoit qu'ils ont pour unique objet de détecter et de signaler en temps réel des événements prédéterminés susceptibles de présenter des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes. Concrètement, il s'agira, comme expliqué précédemment, d'attirer l'attention d'un gendarme ou d'un agent des services de la police nationale ou municipale, des services d'incendie et de secours et des services internes de sécurité de la SNCF et de la RATP sur une scène dont les images, captées par les caméras situées dans les lieux accueillant ces événements et à leurs abords, font apparaître l'existence des risques précités.

Il est explicitement précisé que ces traitements, soumis aux dispositions du RGPD et de la loi « Informatique et Libertés », ne pourront ni s'appuyer sur des données biométriques, ni procéder à une reconnaissance faciale.

Le projet de loi distingue quatre phases successives de l'expérimentation, au cours desquelles la CNIL exercera un rôle de contrôle et d'accompagnement de

(1) Myrtille Picaud, « Peur sur la ville. La sécurité numérique pour l'espace urbain en France *», Sciences Po, 2021, p. 13.*

(2) Audition du 8 novembre 2022.

(3) 24 et 25 juin 2023.

(4) Sous réserve de l'entrée en vigueur des décrets mentionnés dans la première partie du présent rapport.

l'ensemble des services concernés [1] : le recours à ces traitements, leur développement, leur mise en œuvre et leur évaluation.

Il incombera au pouvoir règlementaire de déterminer les cas d'usage qui constituent les finalités pour lesquelles le traitement algorithmique a vocation à être développé, puis déployé. Un décret, pris après avis de la CNIL, fixera les caractéristiques essentielles de ce traitement, en indiquant notamment les événements prédéterminés qu'il aura pour objet de signaler, les spécificités des situations justifiant son emploi [2], les services susceptibles de le mettre en œuvre, les éventuelles conditions de leur participation financière à son utilisation, et les conditions d'habilitation des agents pouvant accéder à ses résultats.

Le projet de loi précise les conditions dans lesquelles le traitement sera développé, qu'il soit élaboré par les services de l'État ou acheté à un tiers, celui-ci étant tenu de présenter des garanties de compétences et de continuité, de fournir une documentation détaillée, ainsi qu'une déclaration d'intérêts. Plusieurs exigences cumulatives devront être satisfaites :

– s'agissant des traitements nécessitant un apprentissage [3], le choix des données d'apprentissage, de validation et de test doit présenter un caractère pertinent, adéquat, représentatif, loyal, objectif et de nature à identifier et prévenir l'occurrence de biais et d'erreurs [4] ;

– le traitement comporte un enregistrement automatique des évènements, afin de garantir la traçabilité de son fonctionnement ;

– le traitement reste soumis à des mesures de contrôle humain et de gestion des risques permettant de prévenir et de corriger la survenue de biais éventuels ;

– le traitement peut être arrêté à tout moment ;

– le traitement est testé dans des conditions analogues à celles de son emploi et fait l'objet d'un rapport de validation ;

– le traitement validé fait l'objet d'une attestation de conformité établie par l'autorité administrative désignée par décret pris après avis de la CNIL.

Vos rapporteurs approuvent l'ajout opéré dans ce texte par la commission des Lois de l'Assemblée nationale relatif à l'intervention de

---

(1) Dans le plan stratégique 2022-2024 de la CNIL, les caméras « augmentées » correspondent à l'une des thématiques prioritaires de son action.

(2) Une analyse d'impact relative à la protection des données (AIPD) sera simultanément réalisée, afin d'établir le rapport « bénéfices – risques » justifiant le recours à ce traitement.

(3) Selon la CNIL, il s'agit de donner aux machines la capacité d'« apprendre *» à partir de données, via des modèles mathématiques par lesquels les informations pertinentes sont tirées d'un ensemble de données d'entraînement. Le but de cette phase est l'obtention de paramètres d'un modèle qui atteindront les meilleures performances lors de la réalisation de la tâche attribuée au modèle. Une fois l'apprentissage réalisé, le modèle pourra ensuite être déployé.*

(4) Ces données doivent demeurer accessibles et être protégées tout au long du fonctionnement du traitement.

l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Compte tenu des défis liés à la sécurité des systèmes qui hébergeront les traitements algorithmiques et des menaces de cyberattaques susceptibles d'affecter leur fonctionnement, il apparaît tout à fait opportun d'inclure l'ANSSI dans le processus de développement des traitements algorithmiques, afin de vérifier que ces derniers s'intégreront sans dommage ni risque pour l'intégrité des systèmes d'information auxquels sont reliées les caméras de vidéoprotection. Dans un rapport publié le 4 avril 2022, le laboratoire d'innovation numérique de la CNIL explicite la nature de ces risques :

« *Les systèmes d'IA engendrent des risques de sécurité spécifiques en comparaison à des systèmes d'information classiques, tant les nouvelles capacités d'apprentissage automatique (*machine learning*) augmentent la "surface d'attaque" de ces systèmes, en introduisant de nombreuses (et nouvelles !) vulnérabilités* […] *Certaines de ces vulnérabilités peuvent permettre de perturber le fonctionnement du modèle et l'amener à émettre une prédiction incorrecte. D'autres, en revanche, laissent un attaquant libre d'extraire des informations sensibles du modèle, telles que les données sous-jacentes ou le modèle lui-même* ». (1)

Dans la même perspective, un amendement à l'initiative de votre rapporteur Philippe Latombe (2) a été adopté par l'Assemblée nationale lors de l'examen en séance publique de ce projet de loi, afin de privilégier le choix d'entreprises se conformant au respect des règles de cybersécurité définies par l'ANSSI (3)

De façon plus générale, vos rapporteurs considèrent que la sécurité informatique de l'ensemble des dispositifs de captation et de traitement des images dans l'espace public représente une priorité d'autant plus sensible que l'acquisition de produits étrangers, voire extra-européens, nécessite une vigilance particulière.

Recommandation n° 19 : Réaliser, sous l'égide de l'ANSSI, un audit de l'ensemble des systèmes de vidéoprotection susceptibles d'être couplés à des traitements algorithmiques dans le cadre de l'expérimentation autorisée par le projet de loi JOP 2024.

Par ailleurs, le projet de loi prévoit que les images dont la durée de conservation n'est pas expirée pourront être utilisées en tant que données d'apprentissage jusqu'à l'issue de l'expérimentation, pour une durée maximale de

(1) Dossier « Sécurité des systèmes d'IA *», 4 avril 2022.*

(2) Sous-amendé par Éric Bothorel.

(3) Dans sa rédaction adoptée par l'Assemblée nationale le 23 mars 2023, l'amendement précité visait le référentiel dit « SecNumCloud *». Mis en place en 2016, ce référentiel correspond à une certification proposée par l'ANSSI dans le but de garantir un haut de niveau de sécurité des services de* cloud *[nuage numérique].*

douze mois, au-delà de la durée de conservation actuellement prévue par le code de la sécurité intérieure (1).

Cette durée de conservation dérogatoire, limitée à la seule finalité d'entraînement du dispositif, est une condition indispensable à la réussite de l'expérimentation. Ces technologies fonctionnant au moyen d'un système d'apprentissage, **il est essentiel que les traitements algorithmiques puissent s'appuyer sur des données d'entraînement représentatives et pertinentes, sans être contraints de les utiliser dans un laps de temps trop court, ce qui compromettrait leurs performances.** Il convient donc de sécuriser l'utilisation de ces données d'entraînement. La rédaction proposée par l'article 7 du projet de loi JOP satisfait pleinement cet objectif, en prévoyant la sélection d'un échantillon d'images collectées par des caméras de vidéoprotection ou des caméras aéroportées sous la seule responsabilité de l'État, pour une durée maximale de conservation s'élevant à douze mois

Inspirée des dispositions prévues par l'article L. 242-5 du code de la sécurité intérieure régissant l'emploi des caméras aéroportées, l'utilisation du traitement est assujettie à une autorisation préfectorale motivée (2). La décision d'autorisation, qui pourra être suspendue par le préfet à tout moment, devra ainsi comporter des indications concernant :

– le responsable du traitement et les services associés à sa mise en œuvre ;

– la manifestation pour laquelle le traitement a vocation à être utilisé ainsi que son périmètre géographique ;

– les modalités d'information du public et les droits dont il bénéficie ;

– la durée d'autorisation, qui ne peut excéder un mois renouvelable dès lors que les conditions de l'autorisation demeurent réunies ;

Le service responsable du traitement tiendra un registre des suites apportées aux signalements effectués par le traitement. Le préfet et la CNIL seront régulièrement informés des conditions dans lesquelles le traitement sera mis en œuvre.

Vos rapporteurs se félicitent de l'adoption de ces dispositions, qui consacrent de façon inédite à l'échelle législative le recours aux caméras « augmentées » et leurs modalités d'utilisation, afin de lutter contre l'insécurité. Ils estiment qu'un équilibre a été atteint entre, d'une part, les nécessités opérationnelles inhérentes au bon fonctionnement de ces traitements

(1) Soit actuellement 30 jours pour les images captées par des caméras de vidéoprotection en application de l'article L. 252-5 du code de la sécurité intérieure et 7 jours pour les images captées par des caméras aéroportées en application de l'article L. 242-4.

(2) Cette autorisation est donc susceptible de recours devant la juridiction administrative.

algorithmiques et, d'autre part, les indispensables garanties (1) qui doivent encadrer leur mise en œuvre. À son terme prévu le 31 décembre 2024, cette expérimentation devra alors faire l'objet d'une évaluation, préalablement à son éventuelle pérennisation, qui devra, le cas échéant, être expressément décidée par le législateur.

b. Une efficacité à évaluer avant d'envisager l'éventuelle pérennisation de la mesure

Le projet de loi JOP 2024 prévoit la remise par le Gouvernement au Parlement d'un rapport d'évaluation de la mise en œuvre de l'expérimentation au terme de celle-ci, soit le 31 décembre 2024. Le rapport de la commission des Lois de l'Assemblée nationale sur le projet de loi souligne l'intérêt de ce calendrier :

« *Cette concomitance de dates permettra de ne pas anticiper une éventuelle pérennisation des traitements algorithmiques ainsi expérimentés, en créant les conditions d'une réflexion collective approfondie sur l'opportunité de pérenniser ou non ces dispositifs dans le code de la sécurité intérieure.* » (2)

Le contenu de ce rapport d'évaluation sera fixé par un décret en Conseil d'État après avis de la CNIL. Le texte règlementaire déterminera notamment les « *modalités de pilotage et d'évaluation pluridisciplinaire et objective de l'expérimentation* », ainsi que ses « *indicateurs* ». La représentation nationale sera également associée à l'évaluation, deux sénateurs et deux députés ayant vocation à y participer. Le rapport d'évaluation sera rendu public, afin de garantir l'information des citoyens.

À l'issue de son audition par la mission d'information, la CNIL a rappelé le caractère crucial que revêt la phase d'évaluation. Loin d'être une formalité administrative quelconque, l'évaluation de l'expérimentation est l'un des éléments clefs à l'aune desquels le législateur sera amené à décider ou non de la pérennisation de ce dispositif – en ajustant, le cas échéant, ses modalités et son champ d'application au regard des conclusions du « rétex » porté à sa connaissance. C'est à cette condition que le Parlement pourra exprimer un choix libre et éclairé quant aux suites qu'il comptera donner à l'expérimentation.

Dans cette perspective, la CNIL souligne la nécessité de définir un cadre rigoureux pour objectiver la réussite ou l'échec de l'expérimentation. Selon elle, il convient ainsi de :

---

(1) Si elles peuvent parfois prêter le flanc aux critiques portant sur la propension de la loi à « bavarder », les très nombreuses garanties qui entourent la mise en œuvre de l'expérimentation prévue par le projet de loi JOP 2024 peuvent également s'avérer indispensables à la constitutionnalité du dispositif, que le Conseil constitutionnel se chargera très probablement de vérifier, dans le cadre de son contrôle a priori *ou* a posteriori *de la loi adoptée par le Parlement.*

(2) Rapport n° 939 du 9 mars 2023 au nom de la commission des Lois de l'Assemblée nationale sur le projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, p. 69.

– définir scientifiquement la méthodologie, les étapes de l'évaluation, ainsi que son organisation concrète, dans le temps et l'espace ;

– formuler explicitement les hypothèses testées lors de l'expérimentation ;

– détailler les indicateurs et critères de succès et d'échecs de l'expérimentation ;

– préciser les performances techniques attendues : les outils testés fonctionnent-ils aussi bien qu'escompté, par exemple au regard des performances de « laboratoire » ? ;

– expliciter les objectifs opérationnels : les outils testés apportent-ils véritablement une plus-value pour la tâche à réaliser ? ;

– analyser les aspects sociétaux : comment sont perçus par les personnes concernées les outils et technologies testés ? ;

– offrir une analyse contrefactuelle, permettant de comparer les résultats obtenus dans le cadre expérimental avec ceux qui l'auraient été en son absence ou encore dans le cas du déploiement d'une autre solution ;

– présenter de manière transparente le protocole expérimental mis en œuvre afin de permettre un examen contradictoire conforme à la méthodologie scientifique ;

– prévoir des vecteurs de communication à destination des différentes parties prenantes : grand public, média, régulateurs.

Vos rapporteurs approuvent l'ensemble de ces orientations. **La dimension exhaustive et objective de cette évaluation présente ici une importance singulière : en l'absence d'étude française ou internationale menée sur l'usage des caméras « augmentées » [(1)], le bilan qui sera tiré de l'expérimentation sera particulièrement attendu.** Lors de son audition par la mission d'information le 18 octobre 2022, Marie-Laure Denis, présidente de la CNIL, a par exemple suggéré d'associer l'équipe-projet Rainbow [(2)] au sein de l'Institut national de recherches en sciences et technologies du numérique (INRIA). S'ils ne souhaitent pas dresser à ce stade une liste d'évaluateurs chargés de participer au « rétex » qui sera conduit par le Gouvernement, vos rapporteurs considèrent cependant que la sensibilité de l'évaluation requiert la mobilisation d'acteurs scientifiques dont l'expertise ne saurait être discutée.

(1) Qu'il s'agisse de parangonnage ou d'études évaluant l'efficacité des caméras « augmentées » expérimentées en France ou à l'étranger, vos rapporteurs déplorent le manque de documentation quant à l'utilisation passée ou actuelle de ces traitements algorithmiques.

(2) L'équipe-projet Rainbow est notamment chargée de développer la prochaine génération de robots à capteurs capables de naviguer ou d'interagir dans des environnements complexes non structurés avec des utilisateurs humains.

En outre, conformément à la position de la CNIL, il est indispensable d'évaluer ces dispositifs à un niveau plus général que celui correspondant aux quelques collectivités publiques ayant déjà décidé d'y recourir à ce jour, dans un cadre expérimental par nature très contraint. L'éventuel déploiement des caméras « augmentées » ne saurait ainsi « *résulter d'une addition d'initiatives locales, nécessairement sans cohérence* » (1). À la suite de l'ensemble des auditions et des déplacements accomplis par la mission d'information, vos rapporteurs souhaitent insister sur plusieurs points auxquels l'évaluation devra porter une attention particulière.

Premièrement, comme l'a précisé la DIJOP lors de son audition, l'interopérabilité de l'ensemble des systèmes de vidéoprotection constitue l'un des défis techniques majeurs que l'expérimentation devra relever. Qu'il s'agisse des systèmes exploités par les municipalités ou par les opérateurs de transports, la transmission des images filmées par les caméras « augmentées » aux forces de police et de gendarmerie apparaît primordiale afin d'assurer la bonne coordination de l'ensemble des parties prenantes. Le couplage de ces systèmes avec les traitements algorithmiques prochainement expérimentés représente un enjeu de premier plan qui, s'il peut sembler évident, n'en demeure pas moins décisif.

Recommandation n° 20 : Veiller à garantir l'interopérabilité des systèmes de vidéoprotection et d'intelligence artificielle mis en œuvre dans le cadre de l'expérimentation.

Deuxièmement, l'évaluation devra distinguer l'efficacité des traitements algorithmiques utilisés selon le type de caméras auquel ils auront été associés. Lors de leur déplacement en Israël le 15 mars 2023, vos rapporteurs ont été sensibilisés aux possibles contraintes opérationnelles entourant l'usage de caméras aéroportées « augmentées ». En l'état de la technologie, la performance des systèmes d'intelligence artificielle employés via des drones ou dans des véhicules apparaît incertaine : distinguer le mouvement de la caméra de celui des foules, des individus ou des véhicules qu'elle filme peut se révéler complexe. Il s'agira donc de tenir compte des différences existant entre les caméras fixes et mobiles dans l'appréciation des résultats de l'expérimentation.

Recommandation n° 21 : Mesurer l'efficacité des caméras « augmentées » selon le dispositif de captation d'images utilisé.

Troisièmement, si l'ouverture des données et des codes sources s'apparente, selon l'expression pertinente de notre ancien collègue Jean-Michel Mis, à un « *gage de transparence et d'efficacité pour l'action publique* » (2), cette exigence doit être tempérée. D'une part, la complexité des codes utilisés peut

(1) Position de la CNIL sur les caméras « augmentées », juillet 2022, p. 16.

(2) Jean-Michel Mis, « Pour un usage responsable et acceptable par la société des technologies de sécurité *», rapport remis au Premier ministre, septembre 2021, p. 51.*

constituer un obstacle à leur expertise approfondie dans des délais raisonnables – ce qui implique, le cas échéant, de procéder à une évaluation davantage tournée vers l'analyse globale des résultats obtenus par les algorithmes au regard des cas d'usage qu'ils ont pour mission de détecter. D'autre part, la communicabilité des codes demeure assujettie à des impératifs de sécurité publique, dont la méconnaissance pourrait remettre en cause l'intérêt opérationnel que présentent ces technologies pour les forces de sécurité.

Quatrièmement, l'évaluation de l'expérimentation devra intégrer une réflexion quant au cadre juridique du développement et de l'achat de ces technologies par les pouvoirs publics. Au-delà des enjeux économiques *stricto sensu*, **la dimension régalienne de ces sujets doit conduire à s'interroger sur le respect des règles des marchés publics résultant du droit européen de la concurrence.** Il pourrait ainsi être judicieux d'envisager l'exclusion de ces technologies du champ concurrentiel de la fourniture de biens et services, sur le modèle des dispositions de l'article L. 2353-1 du code de la commande publique relatif au principe de préférence européenne applicable aux marchés de défense ou de sécurité.

Recommandation n° 22 : Privilégier l'usage de technologies de vidéoprotection intelligente conçues et développées en France ou sur le territoire d'un État membre de l'Union européenne.

Enfin, sans anticiper les prochaines évolutions du droit européen (1) ni les orientations que choisira d'emprunter le Parlement à l'issue de cette expérimentation, vos rapporteurs considèrent que les pouvoirs publics seront sans doute contraints, dans les années à venir, de répondre à une injonction contradictoire : comment garantir l'existence d'un cadre juridique assez agile pour s'adapter aux évolutions technologiques tout en étant suffisamment stable pour chasser les incertitudes ?

Le caractère « mouvant » de l'intelligence artificielle ne doit pas être une excuse justifiant d'abandonner toute ambition de clarté dans la définition de ce qui est autorisé ou interdit. Comme l'ont rappelé avec justesse les chercheurs Nizar Touleimat et Jamal Atif lors de leur audition le 12 octobre 2022, le droit souple (2) pourrait représenter un instrument pertinent afin d'encadrer l'utilisation des caméras « augmentées », en permettant une évolution à la fois dynamique, précise et normative des principes régissant leur utilisation.

(1) La proposition de règlement sur l'intelligence artificielle publiée par la Commission européenne le 21 avril 2021 pourrait être adoptée d'ici à la fin de l'année 2024.

(2) Selon le Conseil d'État, le droit souple correspond à des normes répondant à trois conditions cumulatives. Premièrement, elles ont pour objet de modifier ou d'orienter les comportements de leurs destinataires en suscitant, dans la mesure du possible, leur adhésion. Deuxièmement, elles ne créent pas par elles-mêmes de droits ou d'obligations pour leurs destinataires. Enfin, elles présentent, par leur contenu et leur mode d'élaboration, un degré de formalisation et de structuration qui les apparente aux règles de droit.

B. LA RECONNAISSANCE FACIALE ET BIOMÉTRIQUE

La CNIL définit la reconnaissance faciale comme une « *technique informatique et probabiliste qui permet de reconnaître automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier* » (1). **L'authentification** consiste à vérifier qu'une personne est bien celle qu'elle prétend être. **L'identification** consiste à identifier un individu au sein d'un groupe.

La reconnaissance faciale fait partie de la catégorie des techniques biométriques, qui permettent d'identifier un individu à partir de ses caractéristiques physiques, biologiques ou comportementales (empreintes digitales, iris…).

1. Une utilisation très limitée de la reconnaissance faciale en France

Le recours à la reconnaissance faciale en France est aujourd'hui marginal. Deux systèmes de reconnaissance faciale sont mis en œuvre pour procéder à l'authentification : le traitement des antécédents judiciaires (TAJ) et le système de passage rapide aux frontières extérieures (Parafe). À cela s'ajoutent plusieurs expérimentations conduites dans des champs très limités.

a. Le fichier de traitement des antécédents judiciaires comprend un outil de reconnaissance faciale utilisé sous le contrôle de l'autorité judiciaire

Le fichier de traitement des antécédents judiciaires a été créé par le décret n° 2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires. C'est un **fichier de traitement automatisé de données à caractère personnel**, commun à la gendarmerie nationale et à la police nationale.

i. Un fichier créé en 2012 qui utilise un logiciel de reconnaissance faciale

Le régime du TAJ est prévu aux articles R. 40-23 à R. 40-34 du code de procédure pénale (CPP).

Les finalités pour lesquelles les forces de l'ordre peuvent mettre en œuvre ce traitement automatisé de données à caractère personnel sont prévues à l'article 230-6 du CPP : « *faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs* ». Les données à caractère personnel utilisées doivent avoir été recueillies au cours d'enquêtes concernant tout crime ou délit, ainsi que les contraventions de cinquième classe, sanctionnant un trouble à l'ordre public ou une atteinte aux biens, personnes, ou à l'autorité de l'État.

Le fichier peut également être utilisé dans le cadre d'enquêtes administratives.

---

(1) Contribution de la CNIL datée du 15 novembre 2019 – « Reconnaissance faciale – Pour un débat à la hauteur des enjeux *».*

L'article 230-10 du CPP prévoit que seuls des personnels spécialement habilités [(1)] peuvent accéder aux informations contenues dans le TAJ pour les besoins des enquêtes judiciaires.

L'article R. 40-26 du CPP prévoit la liste des données qui peuvent être enregistrées dans ce fichier, parmi lesquelles l'identité, la situation familiale, la profession, la nationalité. Ces données sont celles recueillies par les services de la police nationale et les unités de la gendarmerie nationale, ainsi que par les agents des douanes habilités à exercer des missions de police judiciaire.

Parmi ces données, cet article R. 40-26 indique expressément que les photographies comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale **peuvent être enregistrées dans le fichier pour deux catégories de personnes** : celles mises en cause et celles faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou d'une disparition.

Le TAJ comporte donc une fonctionnalité pour opérer des rapprochements entre une photographie obtenue par les forces de l'ordre et les photographies des personnes contenues dans le fichier. Une photographie est entrée dans le logiciel de reconnaissance faciale, qui sélectionne une liste de personnes enregistrées dans le TAJ qui peuvent y correspondre. L'enquêteur procède à l'examen de ces « candidats potentiels » et, si le rapprochement est positif, il le consigne par procès-verbal. Il y a donc une analyse humaine qui confirme l'analyse de l'intelligence artificielle.

Mme Pascale Léglise, directrice des libertés publiques et des affaires juridiques (DLPAJ) du ministère de l'Intérieur et des outre-mer, auditionnée par vos rapporteurs le 7 février 2023, a affirmé qu'il n'était pas possible d'utiliser le fichier pour analyser en temps réel un flux vidéo et identifier quelqu'un.

La durée de conservation des données des personnes majeures mises en causes est de vingt ans. Pour certaines infractions, dont la liste est dressée par l'article R. 40-27 du CPP, les données peuvent être conservées pendant quarante ans. Le droit d'opposition ne s'applique pas pour ce traitement de données (premier alinéa de l'article R. 40-33 du même code).

Le Conseil d'État a validé le recours à l'outil de reconnaissance faciale dans une décision du 26 avril 2022 [(2)]. Le recours avait été porté par l'association La Quadrature du Net, qui demandait l'annulation pour excès de pouvoir de la décision implicite du Premier ministre refusant d'abroger les alinéas 15 et 69 de l'article R. 40-26 du CPP, lesquels prévoient la possibilité de conserver des photographies dans le TAJ.

---

(1) Des personnels spécialement habilités des services de la police et de la gendarmerie nationales, les agents des douanes, les agents des services fiscaux et les inspecteurs de l'environnement. Les magistrats du parquet et les magistrats instructeurs ont également accès au fichier.

(2) Arrêt du Conseil d'État, 10ème chambre, 26 avril 2022, n° 442364, La Quadrature du Net.

Le Conseil d'État rappelle en premier lieu que l'article 88 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après, « loi Informatique et libertés ») prévoit la possibilité de déroger à l'interdiction de traiter des données biométriques aux fins d'identifier une personne physique de manière unique prévue par l'article 6 de la même loi. Cette dérogation n'est admise qu'en cas de « *nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée* ».

Le Conseil d'État considère ainsi qu'« *eu égard au nombre de personnes mises en cause enregistrées dans ce traitement, qui s'élève à plusieurs millions, il est* ***matériellement impossible aux agents compétents de procéder manuellement à une telle comparaison****, de surcroît avec le même degré de fiabilité que celui qu'offre un algorithme de reconnaissance faciale correctement paramétré* ». Il en conclut que l'enregistrement de photographies dans le TAJ répond à la condition de nécessité absolue prévue à l'article 88.

En deuxième lieu, le Conseil d'État s'assure que les garanties juridiques pour les droits et libertés des personnes concernées associées au traitement de données sont suffisantes. Dans ce cadre, il contrôle en particulier quatre éléments :

– les dispositions réglementaires n'autorisent ni la collecte d'images de personnes circulant sur la voie publique ou mises en ligne sur les réseaux sociaux, ni la confrontation de ces images avec les photographies contenues dans le TAJ ;

– seuls les personnels habilités sont autorisés à accéder aux données ;

– toutes les opérations effectuées sur les données du traitement sont retracées dans un journal et conservées pendant six ans (article R. 40-30 du CPP) ;

– la mise en œuvre du traitement est suivie à la fois par un magistrat référent désigné par le ministre de la Justice et par la CNIL.

Malgré cela, des problématiques demeurent sur la mise en œuvre de ce traitement automatisé de données.

ii. Le respect des garanties juridiques est fragilisé par le recours massif au TAJ

La base juridique du fichier TAJ est un décret et non une loi, ce qui, au vu des enjeux attachés à sa mise en œuvre, soulève des interrogations. En outre, le fichier TAJ est utilisé massivement par les forces de l'ordre, ce qui pose la question de la réalité du contrôle réalisé par l'autorité judiciaire.

● ***Une utilisation massive du fichier qui complique son contrôle par l'autorité judiciaire.***

Les différents chiffres illustrent un recours de plus en plus important au fichier TAJ.

Le rapport du magistrat référent établit que le nombre de fiches pour les mis en cause contenues dans le TAJ s'établissait à 16 millions en 2021, contre 14 millions en 2014. Toutes les fiches ne contiennent pas de photographies, mais un rapport parlementaire fait état de 8 millions de fiches contenant des photographies dans le TAJ en 2018 (1).

Selon le rapport du Sénat, l'outil de reconnaissance faciale du TAJ a été utilisé 498 871 fois par la police nationale et 117 000 fois par la gendarmerie nationale en 2021 (2).

Or, l'autorité judiciaire n'opère pas de contrôle a priori et peut intervenir seulement a posteriori pour modifier les données contenues dans la base.

Dans le cadre de certaines enquêtes, dont la liste est dressée par l'article R. 40-29 du CPP, les données peuvent être consultées par les personnels habilités sans autorisation du ministère public. Dans les faits, comme l'a indiqué la direction des affaires criminelles et des grâces, « *le recours à l'outil de reconnaissance faciale du TAJ est laissé à l'initiative des agents de la police et de la gendarmerie nationales et n'est pas soumis à l'accord d'un magistrat* » (3).

Si le ministère public n'est pas consulté, **il n'en demeure pas moins que l'autorité judiciaire contrôle l'utilisation de la base de données**.

L'article 230-8 du CPP prévoit ainsi que le traitement est opéré sous le contrôle du procureur de la République territorialement compétent, qui peut ordonner que les données soient effacées, complétées ou rectifiées, soit d'office, soit à la demande de la personne concernée.

Lorsque les données sont issues de procédures traitées dans plusieurs ressorts judiciaires, **c'est un magistrat référent au niveau national qui est compétent**. Il est désigné par le ministre de la Justice pour « *suivre la mise en œuvre et la mise à jour des traitements automatisés de données à caractère personnel mentionnés à l'article 230-6* » (article 230-9 du CPP).

L'activité du magistrat référent chargé du contrôle des fichiers de police judiciaire et des logiciels de rapprochement judiciaire fait l'objet d'un rapport annuel (article R. 40-32 du CPP). Ce rapport, qui n'est pas rendu public, gagnerait à être diffusé plus largement, au vu des enjeux de protection des données attachés à l'utilisation du TAJ.

---

(1) Rapport d'information déposé par la commission des lois de l'Assemblée nationale sur les fichiers mis à la disposition des forces de sécurité et présenté par MM. Didier Paris et Pierre Morel-À-L'huissier, 17 octobre 2018.

(2) Rapport d'information déposé par la commission des lois du Sénat sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, 10 mai 2022.

(3) Audition du 25 janvier 2023 de la direction des affaires criminelles et des grâces du ministère de la Justice.

Recommandation n° 23 : Prévoir la publication du rapport du magistrat référent chargé de suivre la mise en œuvre et la mise à jour des traitements automatisés de données à caractère personnel.

Vos rapporteurs ont pu constater, au cours de leurs travaux, que l'autorité judiciaire n'a pas les moyens d'effectuer correctement ce contrôle. Ainsi, si le traçage des modifications apportées au TAJ existe, le nombre de consultations par jour rend très théorique la possibilité de contrôler ces modifications.

Ont également été mentionnées par le Syndicat de la magistrature des pratiques hors de tout cadre légal, comme l'injection de photographies issues des réseaux sociaux dans le logiciel ou encore l'utilisation du TAJ au-delà des finalités permises.

Vos rapporteurs considèrent qu'une évolution du fichier pour permettre d'identifier l'origine de la photographie entrée dans le TAJ à des fins de comparaison est indispensable pour écarter tout soupçon de détournement du fichier TAJ à des fins autres que celles prévues par la loi.

Une évolution des infractions pouvant donnant lieu à un enregistrement dans le TAJ pourrait également être envisagée, en supprimant la possibilité d'entrer des données à caractère personnel en cas d'enquête concernant une contravention de cinquième classe.

Recommandation n° 24 : Prévoir l'obligation d'identifier l'origine de la photographie entrée dans le TAJ à des fins de comparaison.

● *Un fichier qui n'est pas régulièrement mis à jour*

La conformité du fichier repose également sur **sa mise à jour régulière**. Si le fichier est bien sous la responsabilité de la direction générale de la gendarmerie nationale (DGGN) et de la direction générale de la police nationale (DGPN), c'est le ministère de la Justice qui est à l'initiative de la mise à jour de la base de données.

Certaines mises à jour sont obligatoires, en fonction de la suite judiciaire donnée. Ainsi, les données à caractère personnel des personnes mises en cause doivent être effacées en cas de décision de relaxe ou d'acquittement devenue définitive, à l'exception des cas où le procureur de la République en prescrit le maintien. À l'inverse, en cas de non-lieu ou de classement sans suite, les données à caractère personnel des personnes mises en cause font l'objet d'une mention, sauf si le procureur de la République en prescrit l'effacement.

D'autres mises à jour peuvent intervenir sur requête des intéressés auprès du procureur de la République territorialement compétent ou du magistrat

référent. Ce magistrat référent du TAJ doit se prononcer sur les demandes d'effacement ou de rectification dans un délai de deux mois. Il peut également agir d'office.

En pratique, **cette mise à jour se fait manuellement**, par la transmission d'une « fiche-navette de mise à jour du TAJ » par l'autorité judiciaire au service de police ou de gendarmerie compétent. Cette transmission, comme l'ont indiqué plusieurs interlocuteurs de vos rapporteurs, demande un temps de travail qui n'est pas réellement comptabilisé et n'apparaît pas comme une priorité dans de nombreuses juridictions.

Ces observations confirment le bilan réalisé en 2020 par le ministère public sur la mise à jour du TAJ (1) :

« *Toutefois, les pratiques demeurent éparses, en fonction de l'activité des parquets, de la désignation ou non en son sein d'un magistrat chargé du contrôle du fichier et des effectifs de greffe dédiés à cette tâche. […] D'une manière générale, les hypothèses de requalification ou de non-lieu qui émanent de juridictions pour mineurs ou du juge d'instruction sont peu prises en cours. […] Le recours à la mention ou à l'effacement des données s'avère variable d'un ressort à l'autre.* ***[…] L'état des effectifs, l'absence de dématérialisation des échanges avec les services gestionnaires, le volume des classements et le temps de traitement sont autant de facteurs relevés comme nuisant à la mise à jour « au fil de l'eau » du fichier.*** »

Dans son rapport d'activité de l'année 2021, transmis à vos rapporteurs, le magistrat référent fait état des difficultés rencontrées par les parquets pour mettre à jour le TAJ. Il estime que l'écart entre les mises à jour réellement effectuées et l'ensemble de celles qui auraient dû l'être s'établissait en 2020 à 974 064. Cela rejoint les calculs effectués par la DACG, **qui évalue à plus d'un million le déficit annuel des mises à jour (2)**.

Vos rapporteurs soulignent la nécessité de procéder dans les meilleurs délais à une mise à jour du TAJ, au risque, à défaut, de fragiliser les procédures judiciaires qui reposeraient sur son utilisation, alors même que c'est un outil essentiel pour les forces de l'ordre.

(1) Rapport annuel du ministère public 2020 – Direction des affaires criminelles et des grâces

(2) Rapport d'activité de l'année 2021 du magistrat référent chargé du contrôle des fichiers de police judiciaire et des logiciels de rapprochement judiciaire, p. 10

Recommandation n° 25 : Procéder à une mise à jour complète du TAJ pour s'assurer que les données à caractère personnel qui ne doivent plus y être n'y sont plus.

Conscient des difficultés, le ministère de la Justice a diffusé une dépêche le 8 décembre 2022 (1) concernant les nouvelles règles relatives à la mise à jour du TAJ et l'impérieuse nécessité d'y procéder. Cette dépêche détaille les nouvelles modalités de mise à jour du TAJ et prévoit la création d'un réseau de référents pour les fichiers de la police judiciaire au sein des parquets généraux et des parquets.

Différents interlocuteurs ont mentionné des travaux en cours pour automatiser cette mise à jour en créant des échanges inter-applicatifs avec Cassiopée, qui permet l'enregistrement d'informations relatives aux plaintes et dénonciations reçues par les magistrats.

Vos rapporteurs appellent de leurs vœux cette interconnexion entre Cassiopée et TAJ. Comme l'indique le magistrat référent dans son rapport, « *il s'agit du seul moyen, eu égard à la masse de données à traiter, d'assurer l'effectivité et la fiabilité du traitement des mises à jour* ».

Recommandation n° 26 : Accélérer l'interconnexion entre TAJ et Cassiopée.

Pour autant, cette interconnexion, **si elle est une étape essentielle pour fiabiliser le fichier, ne représente qu'une partie de la solution**. Le magistrat référent souligne en effet les difficultés rencontrées lorsque la suite judiciaire d'un dossier n'est pas entrée dans Cassiopée, obligeant à solliciter directement les juridictions. **En 2021, les suites judiciaires étaient inconnues (même après sollicitation directe) dans 15,5 % des dossiers examinés par le magistrat.**

Enfin, la gouvernance du TAJ doit être clarifiée : le fait d'avoir deux ministères à la manœuvre, l'Intérieur et la Justice, nuit à la lisibilité du dispositif. Vos rapporteurs souhaitent qu'un seul ministère soit désigné responsable de tous les aspects du TAJ, que ce soit la consultation ou la mise à jour de la base de données.

Recommandation n° 27 : Désigner le ministère, entre la Justice et l'Intérieur, qui soit responsable du TAJ dans tous ses aspects.

Au vu des sérieuses problématiques qui demeurent pour l'utilisation et la mise à jour du TAJ, vos rapporteurs sont **réticents, à ce stade, à proposer d'intégrer un logiciel de reconnaissance faciale dans le fichier des personnes**

(1) DP 2022/0037/H18 – « Évolution des modalités et des outils de mise à jour des fichiers TAJ et FAED, et désignation de magistrats référents pour les fichiers de police judiciaire au sein des parquets et des parquets généraux ».

recherchées, comme l'ont suggéré plusieurs de leurs interlocuteurs au cours de leurs travaux.

b. L'utilisation d'un logiciel de reconnaissance faciale pour faciliter le passage aux frontières

Le système Parafe (passage rapide aux frontières extérieures), installé dans certains aéroports, à la gare du Nord, dans le port de Calais et à l'entrée de l'Eurotunnel, permet un passage automatisé aux frontières. Le passage par un sas Parafe n'est pas obligatoire, le passage par un contrôle manuel étant toujours possible.

Le passage par un sas Parafe est réservé aux ressortissants de l'Union européenne et de certains pays tiers (1) dotés d'un passeport biométrique en cours de validité.

Le logiciel évalue la concordance entre la photographie scannée par le portique et la photographie du passeport, grâce à une technologie biométrique d'authentification fondée sur la reconnaissance faciale. Le fait de porter un masque ou des lunettes peut provoquer des incidents. En cas de doute, l'opérateur peut reprendre la main, soit en communiquant avec le passager, soit en choisissant de procéder à un contrôle manuel. La solution a été fournie par Thales. La mise en œuvre du logiciel est autorisée par l'article R. 232-6 du code de la sécurité intérieure (CSI). Les images prises dans le sas ne sont pas conservées (article R. 232-8 du CSI).

Un opérateur peut suivre le passage des passagers dans cinq sas simultanément. Les représentants de groupe Aéroports de Paris et les représentants de la police aux frontières rencontrés par vos rapporteurs lors de leur déplacement le 14 décembre 2022 ont confirmé que **l'introduction du contrôle automatisé du passeport a considérablement fluidifié le passage des frontières**. C'est devenu un outil indispensable au regard du flux quotidien de passagers. À titre d'exemple, l'aéroport Charles de Gaulle, à Roissy, accueille 130 000 passagers par jour entre les départs et les arrivées.

Dans le sens des départs, le logiciel Parafe est réservé aux personnes majeures. Cette restriction, justifiée par la difficulté à contrôler les interdictions de sortie du territoire (IST) si les mineurs passent par un sas Parafe, apparaît comme une précaution excessive.

Vos rapporteurs sont donc favorables à une évolution pour autoriser à titre expérimental le passage des sas Parafe par les mineurs âgés de plus de 12 ans dans le sens des départs.

---

(1) Andorre, Islande, Liechtenstein, Monaco, Norvège, Saint-Marin, Suisse, Australie, Canada, Corée du Sud, États-Unis, Japon, Nouvelle-Zélande, Royaume-Uni, Singapour.

Recommandation n° 28 : Autoriser à titre expérimental l'utilisation de Parafe pour les enfants au-dessus de 12 ans.

c. Des expérimentations très limitées dont il est difficile de tirer des conclusions définitives

Au-delà des deux usages très précis que sont le TAJ et Parafe, quelques expérimentations de solutions biométriques ont été menées, mais certaines n'ont pas pu aboutir.

● *Le carnaval de Nice en 2019*

Une expérimentation a été menée en février 2019 lors du carnaval de Nice, après plusieurs échanges avec la CNIL et la réalisation d'une analyse d'impact sur la protection des données (AIPD). 5 000 personnes, toutes volontaires, ont participé à l'expérimentation, menée sur quatre sorties du carnaval.

L'expérimentation a été effectuée avec un logiciel de reconnaissance faciale israélien, « *Anyvision* », distribué par une entreprise monégasque. Deux scénarios ont été testés : le contrôle d'accès (comparaison 1 : 1) et la détection d'une personne d'intérêt au milieu d'une foule (comparaison 1 : N).

L'analyse a été réalisée à la fois en temps réel, en relecture et en différé. La ville de Nice, dans sa restitution, fait état d'un taux de fiabilité élevé et souligne que la solution prend en compte le vieillissement d'une personne. Elle souligne également que l'analyse fonctionne avec des photos de très basse résolution. Selon le sondage d'opinion réalisé à l'issue de l'expérimentation, 87 % des personnes interrogées sont favorables à la vidéoprotection (sur un échantillon de 800 personnes).

● *Roland-Garros en 2020*

Parmi les solutions de sécurité expérimentées pendant le tournoi de Roland-Garros en 2020 se trouvait une solution, proposée par Thales, de recours à la reconnaissance faciale pour renforcer la protection des locaux sensibles.

Le test a été réalisé avec les arbitres du tournoi et des salariés volontaires, dont l'accès à des locaux sécurisés se faisait grâce à des badges dématérialisés. Il s'agissait d'authentifier les personnels autorisés en comparant l'image de la personne qui se présentait pour accéder aux locaux à celle existante dans la base de données.

Selon le secrétariat général de la défense et de la sécurité nationale (SGDSN), le retour d'expérience fait état d'une très grande fiabilité de la solution, de nature à élever significativement le niveau de sécurité. L'efficacité de la solution repose cependant sur la qualité des images fournies par les personnes accréditées, ce qui peut compliquer le passage à l'échelle.

● *Les limites posées par la CNIL aux expérimentations*

La CNIL, consultée lors de la mise en œuvre des expérimentations en lien avec des données biométriques, s'assure que les principes de nécessité et de proportionnalité sont bien respectés dans leur mise en œuvre.

En 2019, la CNIL a ainsi été saisie par la région PACA d'une demande de conseil sur la conduite d'une expérimentation de reconnaissance faciale dans deux lycées de la région. La CNIL a considéré que la mise en place de ces dispositifs particulièrement intrusifs, sur des mineurs, n'était « *ni nécessaire, ni proportionnée* » pour atteindre les finalités décrites par la région, à savoir fluidifier et sécuriser les accès. La CNIL conclut en considérant qu' « *un tel dispositif ne saurait donc être légalement mis en œuvre et* [qu'] *il appartient désormais à la région et aux lycées concernés, responsables du dispositif envisagé, d'en tirer les conséquences* » [(1)].

Dans sa contribution écrite [(2)], le préfet Michel Cadot, délégué interministériel aux jeux olympiques et paralympiques (DiJOP), évoque également une expérimentation envisagée à l'Olympique de Marseille en 2021. L'objectif était de tester un dispositif de contrôle d'accès grâce à la reconnaissance faciale de personnels accrédités, pour empêcher tout accès frauduleux et améliorer la fluidité des flux. La CNIL aurait considéré, selon le DiJOP, que « *les objectifs de l'expérimentation ne suffisaient pas à démontrer la nécessité d'un stockage des données dans des serveurs distants (type 3) ou dans le cadre d'une maîtrise partagée (type 2) ni même le recours à la biométrie* ».

Alors que le recours à la reconnaissance faciale est marginal en France, il se développe en Europe et ailleurs. Il devient urgent pour la France de se doter d'un cadre juridique adapté pour la reconnaissance faciale – au risque, à défaut, de devoir légiférer plus tard dans l'urgence, sans le recul nécessaire.

2. Alors que le recours à la reconnaissance faciale se développe en Europe et dans le monde, il est urgent de légiférer en France

Le recours à des logiciels de reconnaissance faciale dans le cadre d'enquêtes judiciaires est déjà une réalité : la France, qui ne dispose pas aujourd'hui d'un cadre juridique approprié pour expérimenter des solutions de reconnaissance biométrique, doit rapidement légiférer pour anticiper les besoins des années à venir.

---

(1) Article publié sur le site de la CNIL le 27 octobre 2019, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position ».

(2) Contribution écrite transmise à la suite de l'audition du 8 novembre 2022.

a. Si l'encadrement juridique de l'utilisation de la reconnaissance faciale n'est pas uniforme, son usage se développe

i. La mise en œuvre de la reconnaissance faciale hors des frontières européennes

Aux États-Unis, la situation varie selon les États. Certaines villes, comme San Francisco, ont interdit tout usage de la reconnaissance faciale. À l'inverse, la police de New-York utilise la technologie de reconnaissance faciale pour comparer les images obtenues dans le cadre judiciaire avec une base de données constituée à partir des photographies de personnes arrêtées et de personnes en liberté conditionnelle. Sur son site, la police de New-York précise qu'une concordance via le logiciel de reconnaissance faciale ne constitue en aucun cas une base juridique pour une arrestation (1). La police de Baltimore aurait également recours à la reconnaissance faciale dans le cadre d'enquêtes policières, mais, selon un rapport du Sénat, la base de données utilisée à des fins de comparaison serait bien plus importante, car elle contiendrait notamment l'intégralité des photos fournies à l'administration pour obtenir un permis de conduire (2).

Dans sa contribution écrite, Mme Pascale Léglise, DLPAJ du ministère de l'Intérieur et des outre-mer évoque également l'utilisation de la reconnaissance faciale en Corée du Sud et à Buenos Aires, à des fins de détection d'actes criminels.

En Israël, il existe un écosystème très développé d'entreprises en pointe sur le développement de solutions d'intelligence artificielle pouvant être couplées à des caméras, incluant des algorithmes de reconnaissance faciale.

La police israélienne utilise déjà des logiciels d'intelligence artificielle pour faciliter l'analyse des images issues des caméras installées par la municipalité ou par la police elle-même. Cette avance technologique s'explique en partie par le contexte sécuritaire très particulier du pays.

---

(1) « NYPD questions and answers – Facial Recognition *», site de la police new-yorkaise.*

(2) Rapport d'information précité, déposé par la commission des lois du Sénat sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, p 35.

Israël : l'usage de la reconnaissance faciale précède l'encadrement juridique

Un projet de loi autorisant l'usage de la reconnaissance faciale par la police a été examiné en première lecture par le parlement israélien (*Knesset*) en février dernier.

Ce texte propose d'autoriser le recours à des solutions de reconnaissance faciale dans les espaces publics pour retrouver des personnes disparues, faciliter les contrôles des accès dans certains lieux publics, mais aussi empêcher la commission de crimes.

Ce texte viendrait légaliser a posteriori l'utilisation faite par les forces de l'ordre israéliennes de logiciels de reconnaissance faciale, dont le programme « *Eagle eye* », utilisé pour traquer les véhicules grâce à la reconnaissance de leurs plaques d'immatriculation (1). Des logiciels de reconnaissance faciale seraient également déployés à certains postes-frontières (2).

Lors des travaux de vos rapporteurs, deux entreprises israéliennes ont été régulièrement évoquées comme proposant des solutions matures de reconnaissance faciale : BriefCam et Oosto. Le logiciel utilisé par la ville de Nice lors de l'expérimentation conduite pendant le carnaval provenait justement de la société Oosto.

(1) « Netanyahu Gov't advancing bill to legalize use of facial recognition cameras », *publié le 19 février 2023 par le journal Haaretz*.

(2) « Israel escalates surveillance of Palestinians with facial recognition program in West Bank », *publié le 8 novembre 2021 par le journal Washington Post.*

La solution de reconnaissance faciale proposée par Oosto, un produit présenté comme mature

Oosto est une entreprise israélienne créée en 2015, spécialisée dans le développement de solution de reconnaissance faciale. Elle présente sa solution de reconnaissance faciale comme étant fiable à 87 %.

Cette solution peut être déployée sur un parc de caméras déjà existant. Elle peut être utilisée en temps réel, par exemple pour suivre un individu et identifier les personnes qu'il rencontre, mais aussi a posteriori, dans le cadre d'une enquête judiciaire par exemple, pour retracer l'ensemble des mouvements d'une personne dans un parc de caméras. Le logiciel serait capable d'identifier un individu même si la photographie utilisée pour faire la comparaison date de trente ou quarante ans.

C'est au client de fixer le seuil de fiabilité à partir duquel se déclenchent les alertes : plus ce seuil est bas, plus le nombre de « faux positifs » sera élevé. L'utilisateur de la solution peut aussi établir différentes listes et différencier les alertes liées à chacune de ces listes.

Il est possible d'activer certains paramètres pour limiter les atteintes à la vie privée des personnes filmées, comme par exemple flouter certains visages, programmer la suppression automatique des visages en l'absence de correspondance, ou encore établir l'impossibilité de revenir en arrière et de trouver un visage.

Le logiciel peut être installé sur un drone ou sur un téléphone portable.

Vos rapporteurs ont pu constater l'étendue des potentiels usages de la solution proposée par Oosto lors d'une présentation par cette société à l'occasion de leur déplacement en Israël le 15 mars 2023.

ii. Alors qu'un règlement européen doit être adopté, des recours ponctuels ont déjà lieu en Europe

● *L'encadrement du traitement des données biométriques sous l'angle de la protection des données personnelles*

L'article 9 du RGPD pose le principe de l'interdiction de tout traitement de données biométriques aux fins d'identifier une personne physique de manière unique. Cette interdiction n'est pas absolue : le paragraphe 2 de l'article dresse la liste des conditions dans lesquelles elle ne s'applique pas. C'est le cas notamment si la personne a donné son consentement explicite au traitement des données (a) ou si la personne concernée a rendu publiques les données en question (e), mais également si le traitement des données est nécessaire pour des motifs d'intérêt public important (g).

La directive (UE) 2016/680 du Parlement européen et du Conseil du 27 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 et abrogeant la décision-cadre 2008/977/JAI du Conseil,

appelée « directive Police-Justice », complète le RGPD, qui n'a pas vocation à s'appliquer aux traitements de données mis en œuvre pour assurer la sûreté de l'État ou aux activités menées par la police.

L'article 10 de la directive « Police-Justice » autorise le traitement de données biométriques aux fins d'identifier une personne physique de manière unique « ***en cas de nécessité absolue****, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée* » et lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre. Pour entrer dans le champ de compétence de cette directive, un traitement de données doit être mis en œuvre 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 par une autorité publique compétente. L'article 27 de la directive prévoit l'obligation de réaliser une analyse d'impact relative à la protection des données lorsque le traitement « *est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques* ».

Le recours à la reconnaissance faciale en Europe

Le recours à la reconnaissance faciale est moindre en Europe mais se développe. Ainsi, la police londonienne utilise une solution de reconnaissance faciale en temps réel pour identifier, au sein des personnes filmées par certaines caméras de vidéosurveillance, celles qui sont sur une *watchlist* précédemment établie.

Vos rapporteurs, à l'occasion d'un déplacement à Monaco le 18 janvier 2023, se sont entretenus avec les responsables monégasques de la sûreté publique. À Monaco, des tests ont été menés avec des logiciels de reconnaissance faciale dans un périmètre délimité et faisant appel à des volontaires de la sûreté publique. Une évolution législative est nécessaire pour aller au-delà, et un projet de loi est en cours de préparation pour autoriser le recours à des techniques de reconnaissance faciale dans l'espace public.

Une expérimentation a également été menée en Allemagne en 2017 dans le métro de Berlin sur des volontaires pour évaluer la capacité des forces de l'ordre à prévenir les risques dans l'espace public grâce à la reconnaissance faciale.

Les informations obtenues par vos rapporteurs dans le cadre de leurs travaux font également état de logiciels de reconnaissance faciale utilisés par la police espagnole ou à l'aéroport de Rome.

La loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles a modifié la loi Informatique et Libertés de 1978 (1) pour la mettre en conformité avec le droit européen. L'article 88 de la loi Informatique et Libertés reprend la formulation de l'article 10 de la directive en autorisant le traitement de données biométriques seulement en cas de nécessité absolue, s'il est autorisé par une disposition législative ou réglementaire. Le II de l'article 31 de la loi de 1978 précise que les traitements de données biométriques doivent être autorisés par décret en Conseil d'État après avis motivé et publié de la CNIL.

(1) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le même raisonnement que pour les caméras augmentées s'applique : en l'absence d'autorisation expresse permise par la loi, le recours à des solutions de reconnaissance faciale n'est pas autorisé, sauf dans les cas très précis prévus par les textes (expérimentation sur des personnes volontaires par exemple).

Comme évoqué plus haut, la CNIL a déjà eu l'occasion de se prononcer sur la légitimité et la proportionnalité de certains usages, puisqu'elle a admis l'expérimentation lancée par la ville de Nice lors du carnaval en 2019 et refusé à la région PACA l'autorisation de mener une expérimentation de contrôle d'accès des établissements scolaires.

Le cadre juridique actuel restreint les possibilités de conduire des expérimentations en conditions réelles, ce qui biaise les résultats obtenus et ne permet pas d'évaluer la fiabilité des algorithmes testés.

● *Un règlement européen sur l'intelligence artificielle en cours de discussion.*

Le cadre européen spécifique à l'intelligence artificielle est en cours d'élaboration. La Commission européenne a présenté, le 21 avril 2021, une proposition de réglementation sur l'intelligence artificielle (1). Elle propose d'adopter une approche fondée sur les risques pour les droits fondamentaux :

– lorsque des systèmes d'intelligence artificielle (SIA) présentent un risque inacceptable, ils seront interdits ;

– lorsque des SIA présentent un risque élevé, comme les technologies utilisées dans le domaine du maintien de l'ordre, des obligations très strictes seront indispensables pour permettre leur mise sur le marché européen ;

– lorsque des SIA présentent un risque limité, les usagers devront être informés de leur interaction avec une machine ;

– enfin, lorsque des SIA ne présentent qu'un risque minime, la Commission européenne considère qu'il n'y a pas lieu de prévoir de règles spécifiques.

Les obligations liées à chaque système sont donc proportionnées aux risques qu'ils présentent pour les droits fondamentaux.

La Commission propose, à l'article 5 du règlement, d'interdire l'utilisation de tout système d'intelligence artificielle permettant l'identification biométrique à distance en temps réel de personnes physiques dans des espaces accessibles au public à des fins répressives, au motif que cette utilisation serait « *particulièrement intrusive pour les droits et les libertés des personnes concernées, dans la mesure où elle peut toucher la vie privée d'une grande partie de la population, susciter un*

(1) *European commission* – « Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial intelligence act) and amending certain union legislative acts ».

sentiment de surveillance constante et dissuader indirectement l'exercice de la liberté de réunion et d'autres droits fondamentaux. » Elle propose néanmoins trois exceptions à cette interdiction :

– la recherche de victimes potentielles d'actes criminels, y compris des enfants disparus ;

– certaines menaces pour la vie ou la sécurité physique des personnes physiques, y compris les attaques terroristes ;

– la détection, la localisation, l'identification ou les poursuites à l'encontre des auteurs ou suspects d'infractions pénales visées dans la décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (1), si ces infractions sont passibles d'une peine ou d'une mesure de sûreté privative de liberté pour une période maximale d'au moins trois ans.

L'utilisation de ces systèmes doit s'accompagner de garanties, en prévoyant notamment des limites appropriées dans le temps et dans l'espace, ainsi que l'autorisation expresse et spécifique d'une autorité judiciaire ou d'une autorité administrative indépendante d'un État membre. Seules les situations d'extrême urgence justifieront l'utilisation de ces systèmes sans autorisation préalable.

Le 6 décembre 2022, le Conseil de l'Union européenne a arrêté un texte de compromis (2). Ce texte complète le paragraphe relatif aux exceptions de déploiement de solutions de reconnaissance biométrique afin d'ajouter la possibilité d'utiliser de telles solutions, sous certaines conditions, pour contrôler les frontières.

Le Parlement européen est également en train d'examiner la proposition de la Commission. En octobre dernier, des propositions de modifications avaient été faites par les co-rapporteurs, allant dans le sens d'une interdiction complète de systèmes d'identification biométrique à distance (3). Le Parlement européen n'avait pas arrêté sa position à la date de remise du rapport.

---

(1) La liste comporte 32 infractions : participation à une organisation criminelle, terrorisme, traite des êtres humains, exploitation sexuelle des enfants et pédopornographie, trafic illicite de stupéfiants et de substances psychotropes, trafic illicite d'armes, de munitions et d'explosifs, corruption, fraude, blanchiment du produit du crime, faux monnayage, cybercriminalité, crimes contre l'environnement, aide à l'entrée et au séjour irréguliers, homicide volontaire, coups et blessures graves, trafic illicite d'organes et de tissus humains, enlèvement, séquestration et prise d'otages, racisme et xénophobie, vols organisés ou avec arme, trafic illicite de biens culturels, escroquerie, racket et extorsion de fonds, contrefaçon et piratage de produits, falsification de documents administratifs et trafic de faux, falsification de moyens de paiement, trafic illicite de substances hormonales et autres facteurs de croissance, trafic illicite de matières nucléaires et radioactives, trafic de véhicules volés, viol, incendie volontaire, crimes relevant de la juridiction de la Cour pénale internationale, détournement d'avion/navire, sabotage.

(2) « Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial intelligence act) and amending certain union legislative acts *», Fourth presidency compromise text.*

(3) Euractiv, 6 octobre 2022, « Loi sur l'IA : la reconnaissance faciale au cœur des discussions au Parlement européen *».*

Une fois celle-ci connue, un trilogue s'engagera entre la Commission européenne, le Conseil de l'Union européenne et le Parlement européen pour arriver à un texte final.

Si vos rapporteurs saluent la volonté des institutions européennes de légiférer sur ce sujet essentiel, il ne leur semble pas souhaitable d'attendre la fin des négociations européennes pour réfléchir et avancer sur un éventuel encadrement juridique français du recours à la reconnaissance faciale, qui pourra au besoin être adapté au futur règlement européen sur l'intelligence artificielle.

b. Autoriser la reconnaissance faciale pour des cas d'usages très limités afin de tenir compte des réticences au sein de la société

i. La société française divisée sur le recours à la reconnaissance faciale

Alors que l'usage à cette technologie se répand dans la sphère privée pour des gestes aussi fréquents que déverrouiller son propre téléphone, le recours à la reconnaissance faciale par la puissance publique est loin de faire l'unanimité au sein de la société française.

● *La volonté des forces de l'ordre et de certaines municipalités de franchir le pas du recours à la reconnaissance faciale*

L'utilisation de logiciels de reconnaissance biométrique présente des avantages comparables à ceux déjà évoqués s'agissant des caméras augmentées, notamment l'optimisation de ressources humaines. Les logiciels de reconnaissance faciale, en ce qu'ils peuvent retrouver une personne à partir d'une photographie vieille de quarante ans, peuvent même aller au-delà de ce qu'un œil humain serait capable de discerner.

Si la position des élus locaux sur l'efficacité de la vidéoprotection n'est pas uniforme, comme ont pu le constater vos rapporteurs au cours de leurs différents déplacements, certaines municipalités disposent aujourd'hui d'un parc important de caméras, fruit de plusieurs années d'investissements.

Comme évoqué dans la première partie de ce rapport, ces municipalités considèrent aujourd'hui ne pas pouvoir exploiter pleinement le potentiel de ces caméras, en l'absence d'intelligence artificielle et notamment de solutions de reconnaissance faciale.

Le maire de Cannes, lors de sa rencontre avec vos rapporteurs au centre de protection urbaine de Cannes [(1)], s'est prononcé en faveur du recours à la reconnaissance faciale, pour donner les meilleurs outils possibles à la police.

Lors de son entretien avec vos rapporteurs au centre de supervision urbain de Nice [(1)], la directrice générale adjointe à la sécurité de la ville de Nice,

(1) Déplacement du 19 janvier 2023.

Mme Véronique Borré, a elle aussi exprimé le souhait de pouvoir expérimenter des logiciels de reconnaissance faciale s'agissant du secours à la personne et de la régulation de l'accès au stade.

Les différents représentants des forces de l'ordre entendus par vos rapporteurs, que ce soient les directions générales ou les syndicats, ont également souligné leur souhait de pouvoir utiliser des solutions de reconnaissance faciale dans certaines de leurs missions, à condition que l'intelligence artificielle demeure une aide à la décision et ne remplace pas l'humain [(2)]. La principale finalité évoquée par les représentants des forces de l'ordre est l'identification d'individus recherchés.

● *L'engagement de certains parlementaires en faveur d'une utilisation encadrée*

Dans une note datée de juillet 2019 [(3)], l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST), organe commun à l'Assemblée nationale et au Sénat, préconisait déjà d'élaborer un cadre législatif d'expérimentation pour tester les solutions en conditions réelles et ne pas dépendre de solutions mises au point par des géants du numérique.

Le rapport rendu en septembre 2021 par notre ancien collègue Jean-Michel Mis [(4)] comporte plusieurs recommandations liées à la reconnaissance biométrique :

– engager un programme d'expérimentations ciblées de la reconnaissance faciale en temps réel dans l'espace public, en visant en priorité les sites les plus pertinents en vue de la coupe du monde de rugby et des jeux Olympiques ;

– prévoir une évolution législative pour expérimenter la reconnaissance faciale en temps réel dans l'espace public à des fins de lutte contre le terrorisme.

Le rapport préconise de confier la supervision et l'évaluation de ces expérimentations à une instance indépendante et collégiale, dont les conclusions seraient rendues publiques.

Dans un rapport publié en mai 2022 [(5)], les sénateurs formulent, quant à eux, plusieurs recommandations liées à l'utilisation de logiciels de

---

(1) À l'occasion du déplacement précité.

(2) Syndicat CFDT, 30 novembre 2022

(3) Office parlementaire d'évaluation des choix scientifiques et technologiques, Note scientifique n° 14 « La reconnaissance faciale *».*

(4) Jean-Michel Mis, « Pour un usage responsable et acceptable par la société des technologies de sécurité *», rapport remis au Premier ministre, septembre 2021.*

(5) Rapport d'information fait au nom de la commission des lois du Sénat par MM. Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, enregistré le 10 mai 2022.

reconnaissance biométrique. Ils distinguent les utilisations en temps réel et a posteriori.

Ils préconisent d'expérimenter la possibilité laissée aux services de sécurité d'exploiter *a posteriori* des images grâce à des logiciels de reconnaissance biométrique pour la recherche d'auteurs ou de victimes des infractions les plus graves. Ils souhaitent également ouvrir la possibilité aux services de renseignement spécialisés d'utiliser a posteriori des logiciels de reconnaissance biométrique dans le cadre de certaines finalités précises, notamment le recueil de renseignements relatifs à la prévention du terrorisme (4° de l'article L. 811-3 du CSI).

Les sénateurs ne ferment pas la porte à une utilisation en temps réel dans l'espace public : ils recommandent de créer un cadre juridique expérimental pour en autoriser le recours ciblé et limité pour diverses finalités, notamment pour faire face à une menace imminente pour la sécurité nationale.

● *Des inquiétudes exprimées par les associations de défense des droits fondamentaux*

L'association La Quadrature du Net, à l'origine du recours contre le fichier TAJ devant le Conseil d'État, est fortement engagée contre l'utilisation de la reconnaissance faciale. Elle dénonce une technologie inefficace et coûteuse. Entendues par vos rapporteurs [(1)], les représentantes de l'association se sont déclarées opposées à un raisonnement par cas d'usage et se prononcent en faveur d'un raisonnement par technologie. Elles ont également partagé leurs craintes que les technologies d'intelligence artificielle favorisent la normalisation des comportements et l'autocensure des personnes lorsqu'elles se déplacent dans l'espace public.

Amnesty International, dans un article posté en ligne le 16 février 2022, expose les problèmes posés selon elle par la reconnaissance faciale. L'association considère que le déploiement de solutions de reconnaissance faciale « *viole le droit à la vie privée* », « *menace le droit de manifester* » et « *porte atteinte au droit à la non-discrimination* » [(2)]. Lors de son audition par vos rapporteurs, ses représentants ont exprimé leur opposition par principe à l'utilisation de solutions utilisant des données biométriques.

● *Des institutions qui se prononcent pour des utilisations limitées, voire pour leur interdiction*

Au niveau européen, le Comité européen de la protection des données (EDPB) et le Contrôleur européen de la protection des données (CEPD) se sont prononcés en faveur d'une interdiction générale de toute utilisation de l'intelligence

(1) Audition du 24 décembre 2022.

(2) « Reconnaissance faciale : quelles menaces pour nos droits ? *», article posté sur le site d'Amnesty International (France) le 16 février 2022.*

artificielle en vue d'une reconnaissance automatisée des caractéristiques humaines dans des espaces accessibles au public [(1)].

En France, la Commission nationale consultative des droits de l'homme a recommandé, dans un avis daté du 7 avril 2022, l'interdiction des usages de l'intelligence artificielle trop attentatoires aux droits fondamentaux, tels que « *l'identification biométrique à distance des personnes dans l'espace public et les lieux accessibles au public* ». Elle admet néanmoins son utilisation « *dès lors que celle-ci est strictement nécessaire, adaptée et proportionnée pour la prévention d'une menace grave et imminente pour la vie ou la sécurité des personnes et celles des ouvrages, installations et établissements d'importance vitale* » [(2)]. Les représentants de la CNCDH ont réitéré cette position pendant l'audition devant vos rapporteurs.

La Défenseure des droits a, quant à elle, alerté à plusieurs reprises sur les risques d'atteintes aux droits fondamentaux que présentent les systèmes biométriques. Dans un rapport publié le 19 juillet 2021 [(3)], la Défenseure rappelle que l'utilisation de systèmes biométriques comporte « *un risque inhérent d'atteinte au droit au respect de la vie privée et à la protection des données* » et présente « *un potentiel inégalé d'amplification et d'automatisation des discriminations* ». Elle met finalement en avant un potentiel effet dissuasif sur l'exercice de certaines libertés qui s'exercent majoritairement dans l'espace public, comme la liberté d'expression, la liberté d'aller et venir ou encore la liberté d'assemblée.

Si ces craintes sont légitimes, vos rapporteurs considèrent qu'il est possible de créer un cadre juridique autorisant l'usage de solutions de reconnaissance faciale comportant des garanties suffisantes pour préserver les libertés fondamentales des citoyens.

ii. Créer un cadre juridique pour expérimenter le recours à la reconnaissance faciale respectueux des libertés fondamentales

La création d'un cadre juridique qui autorise la reconnaissance faciale apparaît indispensable afin de ne pas se priver d'un outil essentiel pour améliorer la sécurité de nos concitoyens.

Ce cadre doit comporter des garanties juridiques solides pour tenir compte des fortes réticences exprimées par une partie de la société.

En matière de technologie biométrique, l'absence prolongée de cadre juridique présente les mêmes risques que ceux précédemment évoqués s'agissant

(1) Avis conjoint 05/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle), 18 juin 2021.

(2) Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux de la CNCDH adopté en assemblée plénière le 7 avril 2022, recommandation n° 6.

(3) « Technologies biométriques : l'impératif respect des droits fondamentaux *», publié le 19 juillet 2021 par le Défenseur des droits.*

des caméras augmentées, soit le désinvestissement par les industriels du marché français et un nombre d'expérimentations insuffisant, forçant plus tard les pouvoirs publics à choisir des solutions développées par des entreprises ne respectant pas les critères européens de protection des données.

La construction de ce cadre juridique peut être nourrie par les réflexions déjà engagées sur le sujet par la CNIL, le Conseil d'État et la Défenseure des droits.

La CNIL a publié en octobre 2019 (1) une contribution sur la reconnaissance faciale, présentant les éléments techniques, juridiques et éthiques à prendre en compte pour légiférer sur la question. Pour elle, l'un des risques majeurs associés à l'utilisation d'une technologie de reconnaissance faciale repose sur la possibilité de traiter des données à distance et à l'insu des personnes, puisqu'elle est une « ***réelle technologie sans contact*** ».

La CNIL alerte également sur le risque de changer de paradigme de la surveillance, en passant « *d'une surveillance ciblée de certains individus à la possibilité d'une surveillance pour tous aux fins d'en identifier certains* ».

Enfin, si elle ne ferme pas la porte au développement de la reconnaissance faciale, la commission met en avant trois exigences essentielles pour l'encadrer :

– la fixation de lignes rouges, avant tout cadre expérimental ;

– le respect des droits des personnes (recueil du consentement lorsque cela est possible, contrôle des données recueillies, transparence, sécurité des données biométriques) ;

– l'adoption d'une véritable démarche expérimentale, sans préjuger de l'issue.

La Défenseure des droits, dans son rapport, se prononce également en faveur d'une autorisation très encadrée : « *si le législateur en venait à autoriser ces technologies, leur utilisation devrait a minima* ***se limiter strictement aux infractions les plus graves et faire l'objet d'autorisations spécifiques****, limitées dans le temps comme dans l'espace, et délivrées au cas par cas par la CNIL ou une autorité de certification compétente* […] *ou par une autorité judiciaire*. » (2)

Enfin, le Conseil d'État, dans une étude sur l'intelligence artificielle publiée en août 2022, appelle à trouver un équilibre dans le déploiement des solutions et à faire œuvre de pédagogie au regard de la perception sociale de certains usages.

« *Dans le champ de la sécurité, il y a lieu de mettre en exergue l'intérêt que présentent les SIA tant pour la détection d'infractions pénales dans certains lieux*

---

(1) Contribution de la CNIL datée du 15 novembre 2019, « Reconnaissance faciale, pour un débat à la hauteur des enjeux *».*

(2) Rapport précité du Défenseur des droits, p 18.

publics particulièrement exposés à un risque de sécurité que pour l'analyse dite « prédictive » et la détection précoce des sinistres […]. *Au sein même des usages policiers, il ne faut pas perdre de vue que les SIA peuvent être utilisés aussi bien pour arrêter les auteurs d'infractions que pour disculper des suspects […] ou retrouver et porter assistance aux victimes* » (1).

Suivant ces principes, vos rapporteurs proposent deux voies pour autoriser l'utilisation de la reconnaissance faciale.

● *Prévoir un cadre expérimental pour utiliser des solutions de reconnaissance faciale* a posteriori *dans un cadre judiciaire*

Le recours à la reconnaissance faciale *a posteriori* doit faire l'objet d'une expérimentation pour en évaluer les avantages et les inconvénients.

En effet, comme le rappelle la CNIL dans sa contribution, la reconnaissance faciale repose sur des estimations statistiques et est donc « *intrinsèquement faillible* » : elle donne une probabilité de correspondance et non un résultat absolu. À cela s'ajoutent les éventuels biais liés au manque de diversité du jeu de données sur lequel a été entraîné l'algorithme.

Les forces de l'ordre pourraient être autorisées à utiliser une solution de reconnaissance faciale sur des images et des vidéos captées sur la voie publique pour retracer le parcours d'un individu suspect *a posteriori*, dans un cadre judiciaire. L'autorisation devrait être délivrée par un magistrat.

L'expérimentation pourrait être conduite dans le ressort de cinq tribunaux judiciaires pour une durée de deux ans, en étant suivie par la CNIL à tous les stades. L'évaluation de l'expérimentation devrait faire état des éventuels biais et des faux positifs générés par l'algorithme.

Cette expérimentation, comme celle proposée par le projet de loi, devrait suivre le cadre présenté par la CNIL. La délégation interministérielle aux partenariats, aux stratégies et aux innovations de sécurité (DPSIS) devrait jouer le rôle de coordonnateur.

L'objectif est également de permettre le développement de solutions françaises et européennes qui soient matures et respectueuses dans leur développement de la protection des données à caractère personnel.

(1) *Étude publiée par le Conseil d'État le 31 août 2022, «* Intelligence artificielle et action publique : construire la confiance, servir la performance *», p 91.*

Recommandation n° 29 : Prévoir un cadre expérimental permettant de tester des solutions de reconnaissance biométrique dans le cadre judiciaire, pour retrouver *a posteriori* un individu.

● *Autoriser, pour certains cas d'extrême urgence ou des recherches sensibles et sous le contrôle de l'autorité judiciaire, un traitement en temps réel dans l'espace public pour les forces d'intervention et le renseignement*

Vos rapporteurs considèrent que le raisonnement par cas d'usages adopté par le règlement européen sur l'intelligence artificielle est le bon, car il permet d'évaluer dans chaque cas si le recours est proportionné et nécessaire. Le recours à un logiciel de reconnaissance faciale en temps réel dans l'espace public pourrait être limité à des cas d'usage très précis.

Le premier cas d'usage serait l'usage de la reconnaissance faciale en cas d'extrême urgence pour retrouver un individu ou un groupe d'individus auteurs ou suspects d'actions qui auraient porté atteinte aux intérêts fondamentaux de la nation au sens de l'article 410-1 du code pénal ou qui auraient commis des actes terroristes. Les forces de sécurité auraient alors la possibilité de recourir à des logiciels de reconnaissance biométrique pour faciliter l'arrestation de l'individu ou du groupe d'individus en question.

L'intervention ayant obligatoirement lieu dans un cadre judiciaire, le recours à la reconnaissance biométrique pourrait être requis par le parquet national antiterroriste et autorisé par un juge des libertés ou par un juge d'instruction antiterroriste.

Le deuxième cas d'usage serait également la recherche d'un individu dangereux dans le cadre de la lutte contre la criminalité organisée. Au vu du caractère très intrusif de la reconnaissance biométrique, l'utilisation de la reconnaissance biométrique pourrait être requise par le parquet de la juridiction interrégionale spécialisée (JIRS) de Paris uniquement sur les dossiers relevant de la compétence de la juridiction nationale chargée de la lutte contre la criminalité organisée (JUNALCO), et devrait être autorisée par un juge d'instruction habilité JUNALCO, sous le contrôle d'un juge des libertés et de la détention.

Le dernier cas d'usage serait la recherche d'un mineur ou de son ravisseur lors du déclenchement du dispositif « alerte-enlèvement » par le procureur de la République, dès lors que ce dernier estime pertinent de recourir à une technologie de reconnaissance biométrique.

Dans les trois cas, les forces de sécurité à l'origine de la demande devraient prouver qu'il n'est pas possible de faire usage d'un moyen d'identification alternatif qui serait moins intrusif pour atteindre les objectifs fixés. Cette limitation vise à s'assurer du caractère subsidiaire du recours à la reconnaissance faciale, une

garantie mise en avant par le Conseil constitutionnel s'agissant du recours aux dispositifs aéroportés (1).

Sous réserve que ces conditions soient respectées, les décisions d'engagement devraient rester à la main des forces de l'ordre. Un déport des images des caméras utilisées devrait être fait vers le centre de commandement des forces de l'ordre.

L'autorisation d'utiliser la photographie ne pourrait pas excéder 144 heures à compter du moment où l'utilisation a été autorisée par l'ordonnance du JLD. Le renouvellement de l'autorisation ne pourrait avoir lieu sans élément nouveau le justifiant. La décision d'autorisation devrait comporter le périmètre géographique dans lequel le traitement a vocation à être utilisé et indiquer le responsable de celui-ci.

Recommandation n° 30 : Autoriser, pour certains cas d'extrême urgence ou des recherches sensibles, le traitement en temps réel de logiciels de reconnaissance faciale pour les forces d'intervention pendant une durée limitée, sous le contrôle de l'autorité judiciaire.

Aucune donnée autre que les alertes et les faux positifs générés par l'algorithme ne pourraient être conservées *a posteriori*.

Le recours à la reconnaissance faciale ne sera opérationnel que dans les lieux équipés de caméras et dont les images sont de bonne qualité. En pratique, ce serait plutôt les caméras des opérateurs de transports et des grandes villes qui pourraient être concernées.

● *Les garanties juridiques indispensables*

Vos rapporteurs ne souhaitent pas autoriser le déploiement de dispositifs d'identification à distance en temps réel dans les lieux publics de manière pérenne et pour d'autres finalités que celles indiquées ci-dessus.

Ils ne sont pas favorables à ce que les collectivités locales soient autorisées à installer des solutions de reconnaissance faciale sur leurs propres caméras. Ils ne souhaitent pas, dans l'immédiat, autoriser les opérateurs de transport à déployer des solutions de reconnaissance faciale sur leurs systèmes de vidéoprotection.

Ils sont enfin opposés à l'utilisation de logiciels de reconnaissance faciale à des fins de maintien de l'ordre public quel que soit le vecteur utilisé (caméras aéroportées, caméras-piétons, caméras embarquées, caméras fixes).

Vos rapporteurs rejoignent en ce sens la Défenseure des droits, qui considère que « *s'agissant des usages les plus intrusifs à l'instar des dispositifs*

(1) *Paragraphe 27 de la décision n° 2021-834 DC du 20 janvier 2022,* Loi relative à la responsabilité pénale et à la sécurité intérieure.

biométriques d'identification à distance en temps réel dans les lieux publics, il apparaît difficile de concevoir comment l'utilisation de ces systèmes pourrait être considérée comme nécessaire et proportionnée à ce jour compte tenu des risques significatifs de détournement d'usage qu'ils représentent ».

S'agissant des logiciels utilisés, **vos rapporteurs considèrent que des règles extrêmement strictes ont vocation à s'appliquer**, que ce soit lors de l'achat de la solution ou lors de sa mise en œuvre.

Deux solutions existent : soit les pouvoirs publics développent leurs propres logiciels, soit ils les acquièrent. Concernant le développement du traitement, les exigences posées dans l'article 7 du projet de loi relatif aux JOP 2024 et rappelées précédemment devront évidemment s'appliquer.

Comme le propose la Défenseure des droits : « *les biais discriminatoires des technologies biométriques doivent être contrôlés à chaque étape de déploiement* » (1). Pour ce faire, chaque solution envisagée devra faire l'objet de plusieurs tests, c'est-à-dire tourner sur des jeux de données mis à disposition par l'État afin de vérifier que les algorithmes ne sont pas sources de biais. L'une des associations entendues par vos rapporteurs s'est dite prête à participer à l'audit des algorithmes. Un comité composé d'universitaires, d'experts, de représentants d'associations, de représentants de la CNIL et d'élus pourrait être désigné pour auditer et suivre l'expérimentation.

À cela pourrait s'ajouter la création d'un dispositif de certification, qui indiquerait aux potentiels utilisateurs que les conditions d'élaboration respectent les normes européennes de protection des données.

La sécurisation des données issues de l'utilisation des logiciels de reconnaissance faciale devrait faire l'objet d'une attention particulière et être contrôlée par la CNIL. La DPSIS insiste sur le fait que **les logiciels devraient être sécurisés *by design***, c'est-à-dire dès la conception, pour anticiper et ainsi minimiser les risques.

Les logiciels utilisés devraient également pouvoir être paramétrés pour que les données biométriques des personnes filmées n'ayant pas fait l'objet d'une alerte ne soient pas conservées.

Recommandation n° 31 : Développer un dispositif de certification des logiciels de reconnaissance faciale qui répondent aux exigences de protection des données à caractère personnel.

S'agissant de la mise en œuvre, tout devrait être encadré par l'autorité judiciaire.

(1) Rapport précité, p 18.

Les personnels chargés de mettre en œuvre les algorithmes devraient impérativement **être habilités** pour le faire et avoir été formés à la prise de décision guidée par algorithme. Ils devraient également avoir signé une charte de déontologie spécifique à l'utilisation de logiciels de données biométriques. L'habilitation serait donnée pour une période limitée et son renouvellement pas garanti.

Vos rapporteurs alertent sur le fait qu'il n'est pas envisageable aujourd'hui de considérer le résultat de traitement de données par des logiciels de reconnaissance biométrique comme des éléments ayant force probante devant les tribunaux, au regard de leur caractère statistique. Une procédure ne pourra donc pas reposer uniquement sur les résultats d'une analyse par un logiciel d'intelligence artificielle.

III. UNE GOUVERNANCE QUI RESTE À DÉFINIR SUIVANT UN TRIPLE OBJECTIF : SÉCURITÉ, LIBERTÉ, SOUVERAINETÉ

Le pilotage de la vidéoprotection et de l'intelligence artificielle dans le domaine de la sécurité apparaît aujourd'hui perfectible. Si certaines structures territoriales doivent être confortées et même revalorisées, d'autres acteurs institutionnels sont appelés à changer de dimension, voire à émerger au cours des prochaines années. **Ces enjeux de gouvernance s'inscrivent dans une perspective plus large** qui correspond aux conséquences qu'entraînent les mutations technologiques contemporaines sur la conciliation des impératifs de sécurité et de protection des libertés.

A. LES STRUCTURES INSTITUTIONNELLES À CONFORTER ET À (RÉ)INVENTER

À l'échelle territoriale, les commissions départementales de vidéoprotection et les comités d'éthique installés dans de nombreuses municipalités exercent une mission de nature administrative et citoyenne qu'il convient de renforcer. À l'échelle nationale, le contrôle public de l'intelligence artificielle requiert désormais des transformations urgentes, conformément à nos standards démocratiques.

1. La nécessaire revalorisation des organes chargés de la vidéoprotection

a. Les commissions départementales de vidéoprotection

Créées par la loi n° 95-73 du 21 janvier 1995 et mises en place par le décret n° 96-926 du 16 octobre 1996, les commissions départementales de vidéoprotection sont chargées, d'une part, d'émettre un avis préalable à l'installation des systèmes de vidéoprotection autorisée par le préfet, et d'autre part, d'exercer un contrôle sur le fonctionnement de ces derniers (1). Régies par les dispositions du titre V du livre II du code de la sécurité intérieure (CSI), ces commissions départementales sont composées des quatre membres suivants (2), désignés pour une durée de trois ans, renouvelable une fois (3) :

– un magistrat honoraire, ou, à défaut, une personnalité qualifiée à raison de sa compétence dans le domaine de la vidéoprotection ou des libertés individuelles, désigné par le premier président de la cour d'appel, président (4) ;

(1) Article L. 251-4 du code de la sécurité intérieure (CSI).

(2) Article R. 251-8 du CSI.

(3) Article R. 251-10 du CSI.

(4) Selon l'article R. 251-11 du CSI, le président dispose d'une voix prépondérante en cas de partage des voix.

– un maire, désigné par la ou les associations départementales des maires, ou, à Paris, un conseiller de Paris ou conseiller d'arrondissement désigné par le Conseil de Paris ;

– un représentant désigné par la ou les chambres de commerce et d'industrie territorialement compétentes ;

– une personnalité qualifiée choisie en raison de sa compétence par l'autorité préfectorale.

Cette composition pluridisciplinaire vise à garantir l'objectivité des avis *ex ante* rendus par les commissions départementales, soit en amont de l'installation des systèmes de vidéoprotection [(1)]. Les articles R. 252-8 et R. 252-9 du CSI déterminent les modalités par lesquelles les commissions départementales prononcent leur avis.

Délivrance des avis rendus par les commissions départementales de vidéoprotection
(extraits du CSI)

Article R. 252-8

Sur chaque demande d'autorisation dont elle est saisie en application de l'article L. 251-4, la commission départementale de vidéoprotection entend un représentant de la police ou de la gendarmerie nationales territorialement compétent ou un agent des douanes ou des services d'incendie et de secours ou un représentant de la police municipale concernée.

La commission départementale de vidéoprotection peut demander à entendre le pétitionnaire ou solliciter tout complément d'information sur les pièces du dossier limitativement énumérées à l'article R. 252-3 et, le cas échéant, solliciter l'avis de toute personne qualifiée qui lui paraîtrait indispensable pour l'examen d'un dossier particulier.

Article R. 252-9

Le délai, dans lequel la commission départementale de vidéoprotection doit émettre son avis, est de trois mois. Il peut être prolongé d'un mois à la demande de la commission.

Le silence gardé par l'autorité préfectorale pendant plus de quatre mois sur une demande d'autorisation vaut décision de rejet.

S'agissant de leur activité *ex post*, l'article L. 253-1 du CSI précise que ces commissions peuvent à tout moment exercer, sauf en matière de défense nationale, un contrôle sur les conditions de fonctionnement des systèmes de vidéoprotection répondant aux conditions fixées aux articles L. 251-2 et L. 251-3 du même code. Dans ce cadre, elles peuvent formuler des recommandations et proposer la suspension ou la suppression des dispositifs non autorisés, non conformes à leur

(1) L'article L. 252-6 du CSI précise que leur avis n'est pas requis lorsque l'autorité préfectorale délivre une autorisation provisoire d'installation d'un système de vidéoprotection, pour une durée maximale de quatre mois, en cas de tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens.

autorisation ou dont il est fait un usage anormal, en informant le maire de la commune concernée de cette proposition.

Contrôle exercé par les commissions départementales de vidéoprotection
(extraits du CSI)

Article R. 253-1

Dans le cadre des contrôles qu'elles exercent de leur propre initiative ou sur saisine, sur le fondement du présent titre, la commission départementale de vidéoprotection ou la Commission nationale de l'informatique et des libertés peuvent déléguer un de leurs membres pour collecter, notamment auprès du responsable du système, les informations utiles relatives aux conditions de fonctionnement d'un système de vidéoprotection et visant à vérifier la destruction des enregistrements, les difficultés tenant au fonctionnement du système ou la conformité du système à son autorisation.

La commission départementale de vidéoprotection peut être réunie à l'initiative de son président pour examiner les résultats des contrôles et émettre, le cas échéant, des recommandations ainsi que pour proposer la suspension ou la suppression d'un système de vidéoprotection lorsqu'elle constate qu'il n'est pas autorisé ou qu'il en est fait un usage anormal ou non conforme à son autorisation.

La Commission nationale de l'informatique et des libertés exerce sa mission de contrôle des systèmes de vidéoprotection dans les conditions fixées par la section 2 du chapitre Ier du titre IV du décret n° 2005-1309 du 20 octobre 2005.

La commission départementale de vidéoprotection exerce sa mission de contrôle dans les mêmes conditions que la Commission nationale de l'informatique et des libertés. Toutefois, pour l'application à la commission départementale de vidéoprotection des dispositions de la section 2 du chapitre Ier du titre IV du décret n° 2005-1309 du 20 octobre 2005, la référence au II de l'article 44 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est remplacée par une référence au présent chapitre.

La commission départementale de vidéoprotection peut demander à entendre le pétitionnaire ou solliciter tout complément d'information sur les pièces du dossier limitativement énumérées à l'article R. 252-3 et, le cas échéant, solliciter l'avis de toute personne qualifiée qui lui paraîtrait indispensable pour l'examen d'un dossier particulier.

Article R. 253-2

À l'issue du contrôle qu'elles peuvent exercer sur les systèmes de vidéoprotection, la commission départementale de vidéoprotection ou la Commission nationale de l'informatique et des libertés peuvent, après en avoir informé le maire, proposer à l'autorité préfectorale la suspension ou le retrait de l'autorisation d'installation. L'autorisation prévue au chapitre II du présent titre peut, après que l'intéressé a été mis à même de présenter ses observations, être retirée en cas de manquement aux dispositions du présent titre et en cas de modification des conditions au vu desquelles elle a été délivrée.

Enfin, l'article L. 253-4 du CSI prévoit que toute personne intéressée peut saisir les commissions départementales ou la CNIL de difficultés tenant au fonctionnement d'un système de vidéoprotection.

Conçues comme des garde-fous destinés à vérifier le respect des exigences légales et règlementaires auxquelles sont assujettis les systèmes de vidéoprotection, les commissions départementales font l'objet de plusieurs critiques. S'il est abusif de les assimiler à des « *coquilles vides* », vos rapporteurs considèrent néanmoins que le potentiel de ces organes de proximité est aujourd'hui insuffisamment exploité, mettant en relief les nécessaires progrès qui restent à accomplir.

Premièrement, **les auditions et déplacements réalisés par la mission d'information ont fait état d'un défaut global de reddition des comptes quant à l'activité réelle des commissions départementales.** En l'absence de publications statistiques consolidées à l'échelle nationale relatives aux avis préalables qu'elles rendent et aux contrôles qu'elles effectuent, il est de prime abord délicat de disposer d'une vue d'ensemble cohérente de leur activité.

Ces zones d'ombre traduisent un défaut de pilotage que le ministère de l'Intérieur et des outre-mer admet lui-même : l'article 6 du projet de loi relatif aux JOP 2024 abroge ainsi l'article L. 251-7 du CSI, qui prévoit la remise à la CNIL d'un rapport annuel portant sur l'activité des commissions départementales. Cette obligation d'information est restée lettre morte depuis 2013, ce qui justifie, selon le Gouvernement, d'en tirer les conséquences dans la loi.

En l'espèce, vos rapporteurs tirent des conclusions opposées à celle du Gouvernement : il convient plutôt de respecter les prescriptions légales applicables, et non de changer celles-ci sous prétexte qu'elles seraient méconnues en pratique. Ce bilan annuel serait d'autant plus utile qu'il permettrait de faire la lumière sur la réalité du fonctionnement de ces commissions départementales, les éventuelles disparités territoriales qui caractérisent leur action, le respect de leurs avis et la portée des contrôles qu'elles réalisent chaque année.

Recommandation n° 32 : Maintenir l'obligation de publication d'un rapport annuel d'activité des commissions départementales de vidéoprotection, faisant notamment état du nombre d'avis rendus en amont de l'installation des systèmes de vidéoprotection et des suites données aux avis, ainsi qu'aux contrôles diligentés sur le fonctionnement de ces systèmes.

Deuxièmement, **le rôle exact qu'exercent les commissions départementales soulève plusieurs interrogations.** Dès 2008, un rapport d'information de la commission des Lois du Sénat soulignait les multiples difficultés affectant leur fonctionnement :

« *La non-permanence de ces commissions, leur petite taille et leur composition en font des organes mal outillés pour développer une expertise technique pointue et pour vérifier la nécessité de chacun des systèmes. Selon la Ligue des droits de l'homme, les membres des commissions départementales se déplaceraient très rarement sur le terrain pour procéder aux vérifications nécessaires. Si dans les départements les plus urbanisés, le volume de travail*

permet aux commissions d'acquérir plus rapidement une expertise, ce n'est pas le cas dans les autres départements. Il en résulte des divergences d'appréciation. » (1)

Ainsi, selon le rapport précité, le bilan de leur activité consultative est « *mitigé* » et celui de leur activité de contrôle est « *assez maigre* » (2). Sur ce point, les derniers chiffres disponibles remontent à 2012 (3) : 589 contrôles ont été opérés cette année-là, contre 584 l'année précédente. Là encore, cette opacité statistique et informationnelle empêche d'établir une analyse claire et précise des divergences susceptibles d'exister entre les commissions départementales, indépendamment de leur volume d'activité. Sollicitée par vos rapporteurs, la DPSIS indique que les contrôles *a posteriori* ne font pas l'objet de recensements spécifiques par les préfectures, rendant presque impossible toute remontée statistique exhaustive.

Cependant, la DPSIS a communiqué, à titre illustratif, les volumes d'activité de certaines commissions départementales. Les résultats font apparaître d'étonnantes disparités : par exemple, si la commission départementale de la Dordogne a diligenté 56 investigations en 2022, les commissions départementales du Val d'Oise et de Seine Saint Denis n'en effectuent qu'une dizaine chaque année.

Auditionnée le 7 février 2023, la DLPAJ du ministère de l'Intérieur et des outre-mer observe que « *la diversité des situations locales* » ne permet pas d'apprécier la régularité des échanges entre l'ensemble des parties prenantes au sein de ces commissions, s'agissant notamment des relations qu'entretiennent les représentants des services préfectoraux et judiciaires.

Lors du déplacement de la mission d'information à Nice le 19 janvier 2023, plusieurs problèmes concrets ont été évoqués avec les membres de la commission départementale de vidéoprotection des Alpes-Maritimes. Outre les cas de régularisation *a posteriori* de l'installation de caméras, l'absence de registre mis à jour énumérant les systèmes de vidéoprotection en cours d'utilisation fragilise l'exercice des prérogatives de contrôle de la commission (4).

En outre, les commissions départementales ne sont pas rendues destinataires de l'autorisation ou du refus d'autorisation délivré par le préfet à la suite de l'avis qu'elles ont rendu. Elles n'ont donc pas les moyens d'évaluer avec acuité le suivi de leurs décisions par les services de l'État. Enfin, les avis préalables prononcés par les commissions départementales ne sont pas publics, ce qui contribue pas à la nécessaire transparence de leur action. L'ensemble de ces obstacles méritent donc d'être levés afin de revaloriser efficacement le rôle des commissions départementales.

---

(1) Rapport d'information n° 131 de Jean-Patrick Courtois et Charles Gautier au nom de la commission des Lois du Sénat, 10 décembre 2008, p. 42.

(2) Le rapport sénatorial précise que 11 % des contrôles opérés en 2007 avaient donné lieu à la constatation d'une infraction, contre 22 % en 2006.

(3) Réponse ministérielle du 11 février 2014 à la question écrite n° 40747 du député Sergio Coronado.

(4) La durée de l'autorisation préfectorale s'élève à cinq ans.

Recommandation n° 33 : Renforcer le rôle des commissions départementales de vidéoprotection en publiant les avis qu'elles prononcent dans le cadre de la procédure d'installation des caméras et en les rendant destinataires de la décision d'autorisation ou de refus prise par le préfet à la suite de leurs avis.

Troisièmement, vos rapporteurs se sont interrogés sur l'opportunité de ressusciter un organe consultatif national chargé de la vidéoprotection. Créée par le décret n° 2007-916 du 15 mai 2007, puis élevée au rang législatif par la loi n° 2011-267 du 14 mars 2011, la Commission nationale de la vidéoprotection a été supprimée par la loi n° 2018-699 du 3 août 2018.

Chargée d'une mission de conseil et d'évaluation relative à la mise en place des systèmes de vidéoprotection, cette structure nationale composée de vingt membres (1) ne s'était plus réunie depuis 2015, témoignant de son inactivité. Tirant les conséquences de cet état de fait, le Gouvernement a justifié sa disparition en arguant de son caractère superfétatoire :

« *Au-delà de l'approche quantitative, le Gouvernement retient une conception qualitative et réexamine périodiquement l'utilité des commissions consultatives en vue de supprimer ou réformer celles qui ajoutent une étape sans intérêt réel pour la qualité des textes ou pour le dialogue avec les partenaires de l'administration. À titre d'illustration, la commission nationale de la vidéoprotection a ainsi été supprimée par l'article 84 de la loi n° 2018-699 du 3 août 2018 visant à garantir la présence des parlementaires dans certains organismes extérieurs au Parlement et à simplifier les modalités de leur nomination. Ce travail de rationalisation et de simplification du paysage administratif mené par le Gouvernement permet ainsi d'améliorer la qualité des textes, de raccourcir les délais, en supprimant des consultations devenues purement formelles, et de développer de nouveaux modes de consultation plus ouverts à la société.* » (2)

Contrairement au maintien, nécessaire, du rapport d'activité des commissions départementales de vidéoprotection, la création d'un nouvel organe consultatif à l'échelle nationale n'apparaît pas indispensable. Le ministère de l'Intérieur peut utilement assurer l'harmonisation des pratiques au sein de chaque

(1) Soit cinq représentants des personnes publiques et privées autorisées à mettre en œuvre un système de vidéoprotection, dont trois sont désignés respectivement par l'Association des maires de France, l'Association des maires des grandes villes de France et le groupement des autorités responsables de transport, six représentants du ministre de l'Intérieur, un membre de la CNIL, deux députés, deux sénateurs et quatre personnalités qualifiées, dont un magistrat du siège et un magistrat du parquet.

(2) Réponse ministérielle du 6 octobre 2022 à la question écrite n° 00520 du sénateur Pierre Charon.

département, en mobilisant les moyens règlementaires dont il dispose [1]. La réintroduction d'une commission nationale, à laquelle la DLPAJ ne serait pas favorable, ne présenterait donc pas de réelle plus-value afin d'améliorer le pilotage global des systèmes de vidéoprotection.

Cependant, l'absence de registres précis et exhaustifs présentant l'emplacement de toutes les caméras de vidéoprotection déployées sur le territoire national demeure problématique. Vos rapporteurs considèrent que le manque d'information quant au nombre et à la localisation des caméras installées dans chaque département pourrait être comblé par la mise en place d'une base de données centralisée. Alimentée par tous les services préfectoraux et supervisée par l'administration centrale du ministère de l'Intérieur et des outre-mer, cette cartographie nationale permettrait de mieux objectiver le déploiement des systèmes de vidéoprotection, ainsi que leur impact sur la lutte contre l'insécurité, au regard des statistiques de délinquance et de criminalité déclinées à l'échelle territoriale.

Recommandation n° 34 : Réaliser, sous l'égide des préfectures et des services centraux du ministère de l'Intérieur et des outre-mer, une cartographie nationale de l'emplacement de toutes les caméras de vidéoprotection installées sur l'ensemble du territoire.

Parallèlement aux commissions départementales de vidéoprotection, de nombreuses villes ont décidé, depuis le début des années 2000, de créer des comités d'éthique chargés de contrôler la mise en place et le fonctionnement des systèmes de vidéoprotection à l'échelle municipale.

b. Les comités d'éthique

Le déploiement progressif des systèmes de vidéoprotection depuis une vingtaine d'années s'est accompagné de réflexions croissantes quant au respect des règles déontologiques qui encadrent la mise en place et l'utilisation de ces outils. Ainsi, de nombreuses municipalités qui recourent à la vidéoprotection ont créé des comités d'éthique, dont l'objet est de veiller à ce que l'usage de ces technologies s'inscrive dans le cadre juridique applicable, en recueillant les doléances des citoyens et en interpellant au besoin les pouvoirs publics [2].

Procédant d'une simple délibération du conseil municipal, ces organismes ne se fondent sur aucune base légale ou règlementaire. Ils représentent donc des espaces d'échanges particulièrement souples, qu'il s'agisse de leurs conditions de création, de leur composition ou de leur fonctionnement. À titre illustratif, les

---

(1) Voir, par exemple, la circulaire du ministre de l'Intérieur du 12 mars 2009 relative aux conditions de déploiement des systèmes de vidéoprotection.

(2) Il convient aussi de noter la création de comités d'éthiques ou déontologiques au sein d'entreprises fabriquant des solutions technologiques dans le domaine de la sécurité publique, à l'image de la société Idemia, auditionnée par la mission d'information le 6 décembre 2022. Le champ d'intervention de son comité est cependant circonscrit à l'accès aux marchés et au contrôle des ventes. Il ne s'étend donc pas aux questions relatives à la conception et à l'utilisation des systèmes d'intelligence artificielle.

métropoles de Lyon en 2003 et de Nantes en 2018 ont créé des comités d'éthique de la vidéoprotection, composés d'élus municipaux de la majorité et de l'opposition, de personnalités qualifiées issues de la société civile (1) voire de responsables des forces de l'ordre, de services préfectoraux et de magistrats judiciaires. Le comité d'éthique de la vidéoprotection à Paris a été mis en place en 2009 par une initiative conjointe du préfet de police et du maire de Paris. Dans son étude publiée en 2021, le laboratoire d'innovation numérique de la CNIL souligne que cette pratique n'est plus réservée aux grandes villes, mais se diffuse aussi dans des communes plus petites :

« *La municipalité de Flers (Orne, 14 779 habitants) expliquait ainsi avoir* "fait le choix, ce qui n'est pas obligatoire, de créer une charte éthique et un comité d'éthique qui sera composé de conseillers (majorité et opposition) et d'un collège de techniciens (des professionnels en lien avec la prévention et la répression de la délinquance)" » (2). À l'inverse, la ville de Nice ne dispose d'aucun comité d'éthique, bien que plus de 4 000 caméras de vidéoprotection soient aujourd'hui utilisées dans l'espace public.

Auditionné par la mission d'information le 24 janvier 2023, Christian Vigouroux, président du comité d'éthique de la Ville de Paris, considère que le comité « *a la force de ne servir à rien* ». Il ne s'agit évidemment pas de démontrer son inutilité, mais au contraire de souligner la place singulière qu'occupe ce comité dans l'écosystème de la vidéoprotection parisienne. Surplombant les autorités compétentes, il jouit d'une forme « d'autorité morale » sur ces questions mêlant sécurité et libertés publiques. Le comité incarne aussi bien une porte d'entrée pour les citoyens qu'un interlocuteur indépendant pouvant être utilement consulté par l'autorité administrative.

À l'instar des commissions départementales de vidéoprotection, les comités d'éthique essuient également des critiques tenant à leur faible influence. Le laboratoire d'innovation de la CNIL observe que « *dans les faits, l'activité de ces comités est limitée : ils se réunissent peu et n'exercent pas de réel contrôle sur l'usage et le développement de la vidéosurveillance* » (3). Un article du journal « *Le Monde* » publié le 27 juillet 2018 (4) souligne ainsi le relatif anonymat de ces comités d'éthique « *plus ou moins fantômes* » dont l'activité réelle serait faible, voire inexistante.

Vos rapporteurs ne partagent pas ce constat injustement sévère. **Les comités d'éthique créés dans ces communes n'ont vocation à se substituer ni aux commissions départementales de vidéoprotection, ni à la CNIL.** Ils n'ont pour objet ni d'exercer des prérogatives de contrôle, ni d'enjoindre aux autorités

---

(1) Universitaires, juristes, membres d'associations de protection des droits de l'homme.

(2) Laboratoire d'innovation numérique de la CNIL, « Les caméras au village *», novembre 2021, pp. 11 et 12.*

(3) Idem.

(4) https://www.lemonde.fr/pixels/article/2018/07/27/videosurveillance-des-comites-d-ethique-sans-pouvoirs-sans-budget-et-parfois-sans-activite_5336791_4408996.html

municipales ou préfectorales de se conformer à leurs préconisations. Ils s'apparentent plutôt à des espaces originaux de dialogue et d'échanges, à des « vigies » rappelant les exigences de protection des libertés individuelles, afin de prévenir les contentieux auxquels les pouvoirs publics sont susceptibles d'être confrontés. Leur force réside aussi dans la souplesse qui caractérise leur organisation, fondée sur une logique de « droit souple », gage de leur adaptabilité et de leur capacité d'influence.

S'il ne semble pas opportun de codifier leur existence au niveau législatif ou règlementaire, **il pourrait être pertinent d'inciter certaines municipalités à développer ce type de structure.** Ainsi, lorsque le nombre de caméras de vidéoprotection installées dépasse un certain seuil par habitant ou que celles-ci sont associées à des technologies d'intelligence artificielle, qu'il s'agisse de vidéoprotection dite intelligente ou de systèmes d'identification biométrique, ces situations pourraient alors justifier la mise en place de garde-fous déontologiques spécifiques, au regard des enjeux démocratiques qu'elles soulèvent.

Recommandation n° 35 : Prévoir la création de comités d'éthiques dans les communes dès lors que le nombre de caméras de vidéoprotection installées excède un certain seuil par habitant, ou qu'un système d'intelligence artificielle est couplé aux dispositifs de captation d'images.

Au-delà des comités d'éthique ou des commissions départementales de vidéoprotection, les enjeux de l'intelligence artificielle dans le domaine de la sécurité appellent la définition d'une nouvelle gouvernance en la matière.

2. Quelle gouvernance de l'intelligence artificielle ?

a. La CNIL : l'autorité administrative indépendante de référence

Forte de son expérience acquise depuis plus de quarante ans dans la protection des données à caractère personnel et des contrôles qu'elle effectue sur les systèmes de vidéoprotection (1), la CNIL apparaît comme l'organisme public idoine afin de relever les défis que posent les progrès de l'intelligence artificielle. L'identification d'une autorité exerçant le rôle de « *chef de file* » en la matière revêt une actualité particulière au regard de la proposition de règlement publiée par la Commission européenne le 21 avril 2021 et dont l'adoption pourrait intervenir au cours de l'année 2024.

La désignation de la CNIL en tant que chef de file national de l'intelligence artificielle fait l'objet d'un relatif consensus. Cependant, elle suscite plusieurs interrogations légitimes.

(1) Selon les informations communiquées à vos rapporteurs, la CNIL reçoit chaque année 7 000 plaintes relatives au fonctionnement des dispositifs de vidéoprotection et mène annuellement près de 600 contrôles sur le terrain.

D’une part, d’autres autorités administratives indépendantes spécialisées dans le domaine du numérique, à l’image de l’Autorité de régulation des communications électroniques et des postes (ARCEP) ou de l’Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) ont été citées pour prendre en charge cette mission lors des auditions menées par la mission d’information. Affichant une certaine forme de prudence voire de réticence à l’idée de confier cette tâche à la CNIL la direction générale des entreprises (DGE) du ministère de l’Économie auditionnée le 9 novembre 2022 a souligné que l’interprétation du RGPD par la CNIL ne semble pas « *particulièrement portée sur le développement de l’innovation* ». En outre, l’intelligence artificielle n’implique pas nécessairement la manipulation de données à caractère personnel, ce qui peut ainsi l’éloigner du cœur d’activité de la CNIL.

D’autre part, la consécration de la CNIL en tant qu’autorité chargée de la gouvernance de l’intelligence artificielle suppose, de sa part, la définition d’une stratégie pluriannuelle lui permettant de s’approprier l’ensemble de ces enjeux. À l’issue de leurs travaux, vos rapporteurs ne doutent pas de la détermination de la CNIL à s’engager pleinement dans cette voie, ce qui implique de renforcer ses moyens techniques et humains afin d’y parvenir dans les meilleurs délais.

L’enjeu capacitaire s’avère ici décisif. Auditionnés le 7 décembre 2022, les chercheurs Jean-Gabriel Ganascia et Erwan Le Pennec ont rappelé la nécessité de « techniciser » le profil d’une partie des agents de la CNIL sur les questions d’intelligence artificielle, au-delà des seules compétences juridiques et informatiques dont dispose son personnel actuel. Les entreprises XXII et Idemia partagent cette analyse et suggèrent que les ressources matérielles et humaines de la CNIL devront s’ajuster à cette nouvelle mission. Dans le cas contraire, son rôle de chef de file ne débouchera que la « *sclérose de son travail de régulation et la neutralisation des capacités d’innovation de la filière industrielle* » [(1)]. Auditionnés le 7 décembre 2022, les sociologues Myrtille Pacaud et Antoine Courmont ont également mis en relief le besoin pour la CNIL de développer des compétences en analyse organisationnelle et sociale, afin de comprendre comment les normes sociales des territoires influent sur les algorithmes que les pouvoirs publics utilisent.

Le renforcement des moyens de la CNIL constitue un préalable communément admis. Dans son rapport remis au Premier ministre en septembre 2021, notre ancien collègue Jean-Michel Mis rappelle que les ressources dont elle bénéficie sont encore insuffisantes à ce jour :

« *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. Le ratio entre le nombre d’agents*

(1) Audition d’Idemia le 6 décembre 2022.

de la CNIL et le nombre d'habitants est le 3eme ratio le plus bas d'Europe. Les besoins en ressources humaines de la CNIL doivent être évalués, afin qu'elle puisse effectuer ses missions, notamment en matière d'accompagnement des entreprises et de compliance [conformité] ». (1)

Cette situation illustre l'ampleur des efforts budgétaires auxquels l'État devra consentir. Il s'agit d'une condition indispensable pour garantir le succès des nouvelles missions qu'il entend confier à la CNIL. En effet, cette exigence est incontournable afin de ne pas entraver l'émergence de technologies développées par des sociétés françaises ou européennes à la demande des collectivités publiques, en permettant leur accompagnement personnalisé, qu'il s'agisse des phases d'identification des besoins sécuritaires, du développement expérimental de ces technologies, ou encore, par la suite, de leur déploiement sur le terrain.

Cette fonction d'accompagnant, déjà prévu par l'article 7 du projet de loi JOP 2024 relatif à l'expérimentation des caméras « augmentées », devra se conjuguer à un rôle plus classique de « *guichet unique* ». L'objectif vise à faciliter les démarches initiées par les acteurs publics et privés qui recourent à des systèmes d'intelligence artificielle. Il reviendra ainsi à la CNIL de délimiter de façon précise et réactive, selon l'expression de Gontran Peubez (2), « *ce qui est rigoureusement interdit de ce qui ne l'est pas* ». Dans une perspective plus opérationnelle, la DLPAJ du ministère de l'Intérieur et des outre-mer se montre ouverte à l'idée d'élargir les prérogatives de la CNIL à la certification des traitements algorithmiques développés.

Dans sa contribution écrite remise à la mission d'information à l'issue de son audition (3), la CNIL précise qu'elle est la seule autorité administrative indépendante à s'être dotée d'une direction dédiée à l'accompagnement (DAC) des acteurs soumis à sa régulation (4). À ce titre, un professionnel ou un collectif peut lui soumettre une « *demande de conseil* » à titre individuel et gratuit, portant sur un point précis, lorsque les outils généraux ou sectoriels ne lui ont pas permis d'y répondre et lorsque son propre délégué à la protection des données (DPO) ou conseil juridique ne s'estime pas en mesure d'y répondre. De même, un fournisseur de solutions peut s'adresser à la CNIL pour recueillir son avis sur le caractère approprié de la solution fournie au regard des règles de protection des données personnelles (5).

---

(1) Jean-Michel Mis, « Pour un usage responsable et acceptable par la société des technologies de sécurité », *rapport remis au Premier ministre, septembre 2021, pp. 58-59.*

(2) Audition du cabinet de conseil OnePoint le 11 octobre 2022.

(3) Contribution écrite remise par la CNIL en novembre 2022.

(4) La CNIL a rendu publique sa charte d'accompagnement des entreprises en février 2021 : https://www.cnil.fr/fr/la-cnil-publie-sa-charte-daccompagnement-des-professionnels

(5) Cependant, compte tenu de ses effectifs limités, la CNIL rappelle qu'elle ne peut pas répondre à toutes les demandes individuelles. Elle peut donc être amenée à privilégier, pour les approfondir, les demandes portées par un collectif sectoriel ou les demandes présentant un intérêt particulier d'un point de vue juridique, sociétal, économique ou technologique.

Sa capacité à produire des normes de « droit souple » [(1)] contribue également à stabiliser et à éclairer le cadre juridique en vigueur, ce qui sécurise les entreprises concernées, au-delà des concertations qu'elle peut mener avec celles-ci.

Vos rapporteurs approuvent l'ensemble de ces orientations visant à identifier la CNIL comme la principale autorité administrative en charge de la gouvernance de l'intelligence artificielle, conformément à la préconisation émise par le Conseil d'État dans son étude intitulée « *Intelligence artificielle et action publique : construire la confiance, servir la performance* », adoptée en assemblée générale le 31 mars 2022. Auditionné le 22 novembre 2022, Thierry Tuot, l'un de ses auteurs, insiste sur l'évolution presque conceptuelle de la raison d'être de la CNIL. Si elle demeure l'organisme protecteur des libertés publiques, elle devient simultanément un régulateur économique chargé de vérifier la conformité des traitements algorithmiques aux exigences légales et règlementaires applicables.

Dans un communiqué publié le 23 janvier 2023, la CNIL a annoncé la création d'un service dédié à l'intelligence artificielle dans le but de renforcer son expertise sur ces systèmes et sa compréhension des risques pour la vie privée.

(1) Recommandations, lignes directrices ou encore référentiels.

Création d'un service de l'intelligence artificielle (SIA) au sein de la CNIL

Le service de l'intelligence artificielle (SIA) créé au sein de la CNIL réunira cinq personnes. Composé de juristes et d'ingénieurs spécialisés, ce service sera rattaché à la direction des technologies et de l'innovation de la CNIL, dont le directeur, Bertrand Pailhès, était précédemment coordonnateur national pour la stratégie d'intelligence artificielle au sein de la direction interministérielle du numérique et du système d'information de l'État (DINSIC). Le service de l'intelligence artificielle aura pour principales missions de :

– faciliter au sein de la CNIL, mais aussi pour les professionnels et les particuliers, la compréhension du fonctionnement des systèmes d'IA ;

– consolider l'expertise de la CNIL dans la connaissance et la prévention des risques pour la vie privée liés à la mise en œuvre de ces systèmes ;

– préparer l'entrée en application du règlement européen sur l'IA (en cours de discussion au sein de l'Union européenne) ;

– développer les relations avec les acteurs de l'écosystème de vidéoprotection, visant à vérifier la destruction des enregistrements, analyser les difficultés tenant au fonctionnement du système ou contrôler la conformité du système à son autorisation.

Plus généralement, en raison de sa composition pluridisciplinaire et de sa nature transversale, ce nouveau service a vocation à travailler avec toutes les directions de la CNIL.

Le SIA apportera également un support dans l'instruction de plaintes et l'adoption de mesures correctrices en cas de manquements liés à l'utilisation d'un système d'IA.

Il sera chargé de l'expertise technique de dossiers relatifs à l'intelligence artificielle comportant des aspects spécifiques à cette technologie. Il contribuera aux travaux du Comité européen de la protection des données (CEPD) et conduira également des projets d'expérimentation en lien avec le laboratoire d'innovation numérique de la CNIL (LINC).

Source : CNIL, janvier 2023.

Vos rapporteurs se félicitent vivement de cette annonce. Plus qu'une simple autorité de contrôle, et dans le sillage de l'article 59 de la proposition de règlement publiée par la Commission européenne le 21 avril 2021, la CNIL doit devenir le véritable « *tiers de confiance* » que solliciteront les pouvoirs publics et les entreprises afin de mener à bien leurs projets dans le domaine de l'intelligence artificielle, s'agissant plus particulièrement des usages sécuritaires, compte tenu de leur impact sur les libertés publiques.

Au regard de la dimension intrinsèquement pluridisciplinaire que revêt l'intelligence artificielle, il serait tout à fait pertinent d'élargir la composition du collège de la CNIL[(1)]. Dans un objectif de transversalité, les présidents de l'ARCOM et de l'ARCEP pourraient utilement intégrer ce collège au sein duquel

(1) La CNIL est composée de 18 membres élus ou désignés par l'Assemblée nationale, le Sénat et le Conseil économique social et environnemental, ainsi que par les juridictions administrative, judiciaire et financière auxquelles ils appartiennent. Le Premier ministre désigne trois personnalités qualifiées. Le président de la Commission d'accès aux documents administratifs (CADA) siège également au sein du collège.

siège déjà le président de la Commission d'accès aux documents administratifs (CADA). Cette extension s'inscrirait pleinement dans l'évolution du rôle de la CNIL en tant que « chef de file » de la régulation des systèmes d'intelligence artificielle, suivant une logique résolument inclusive.

Recommandation n° 36 : Consacrer la CNIL en tant que « chef de file » de la régulation des systèmes d'intelligence artificielle, d'une part en renforçant ses ressources humaines et techniques pour accomplir cette mission et d'autre part, en élargissant la composition de son collège aux présidents de l'ARCEP et de l'ARCOM.

La consécration du rôle-clef de la CNIL doit rapidement s'accompagner d'une réflexion quant à la gestion des bases de données nécessaires à l'apprentissage des traitements algorithmiques.

b. La création d'un « NIST » à l'échelle nationale ou européenne

Le développement des systèmes d'intelligence artificielle repose sur l'utilisation de données d'apprentissage destinées à entraîner les traitements algorithmiques. Ces jeux de données se révèlent particulièrement importants : les données utilisées doivent être nombreuses et diversifiées, afin d'offrir aux traitements le meilleur apprentissage possible. Leur efficacité dépend de leur capacité à appréhender avec justesse les cas d'usage qu'ils sont censés détecter, ce qui suppose au préalable de les « nourrir » avec un volume de données suffisamment représentatives de la réalité des situations qu'ils ont pour objet de caractériser.

Le recours à ces données d'entraînement est indispensable au fonctionnement des algorithmes. Cette contrainte, inhérente par nature à tout système d'apprentissage, soulève cependant plusieurs questions ayant trait à la sélection de ces données, aux modalités de leur usage, à la sécurité et à la durée de leur conservation, ainsi qu'à la protection du droit à la vie privée des individus dont les données personnelles sont utilisées lors de ces phases d'apprentissage. Comme le souligne le rapport de notre collègue Éric Bothorel, remis au Premier ministre en décembre 2020, « *la création d'un dispositif expérimental permettant à titre dérogatoire, la réutilisation de données déjà collectées pour une finalité autre que la constitution de jeux d'apprentissage d'IA, et leur conservation sur une durée plus longue, conditionne largement l'agilité et la capacité d'innovation dans notre pays* ». (1)

Les auditions conduites par vos rapporteurs ont fait état d'une double difficulté entravant aujourd'hui le développement des technologies d'intelligence artificielle en Europe.

---

(1) Éric Bothorel, « Pour une politique publique de la donnée *», rapport remis au Premier ministre, décembre 2020, p. 130.*

D'une part, le cadre juridique actuel régissant l'utilisation de données d'apprentissage est lacunaire et inadapté aux nécessités technologiques précitées. L'article 78 de la loi « Informatique et Libertés » [(1)] précise qu'un décret en Conseil d'État, pris après avis motivé et publié de la CNIL, détermine les conditions dans lesquelles il peut être dérogé en tout ou partie aux principes prévus aux articles 15, 16, 18 et 21 du RGPD [(2)], s'agissant des traitements de données à caractère personnel à des fins de recherche scientifique, historique ou statistique. Si un tel décret a été publié le 14 mai 2020 [(3)], son champ d'application reste en l'espèce circonscrit au domaine de la santé, selon une finalité restrictive. En outre, les expérimentations de systèmes d'intelligence artificielle jusqu'alors acceptées par la CNIL ne se fondent que sur des données à caractère personnel d'individus volontaires pour participer à ces expérimentations, ou sur des données disponibles en source ouverte, dans un cadre par nature étroit. Ces restrictions contraignent très fortement les acteurs publics et privés désireux de tester les traitements algorithmiques, en empêchant toute homothétie entre les données utilisées pour entraîner les algorithmes et l'ensemble des situations susceptibles de survenir dans la réalité.

Inadapté, le cadre juridique actuel fragilise le développement des traitements algorithmiques fondés sur une logique d'apprentissage. Comme analysé précédemment, les expérimentations conduites par les pouvoirs publics et les entreprises présentent des résultats mitigés, principalement en raison du caractère parcellaire des données sur lesquelles les traitements ont été entraînés. Les chercheurs Jean-Gabriel Ganascia et Erwan Le Pennec [(4)] considèrent que l'accès à des bases de données de grande taille améliorera, à terme, les performances des algorithmes. François Terrier, directeur du programme intelligence artificielle du Commissariat à l'énergie atomique (CEA), déplore la pauvreté des bases de données sur lesquelles s'appuient les logiciels de vidéoprotection intelligente, ce qui, selon son expression, « *ne permet pas de traiter le réel* ». [(5)]

Dans l'attente de ces évolutions, les systèmes d'intelligence artificielle se développent en dehors des frontières de l'Union européenne, dans des conditions insatisfaisantes. Le recours à des données peu représentatives des spécificités physiques, comportementales ou culturelles propres à la France ou à l'Europe s'effectue à rebours de nos standards de protection des droits et libertés. Cette situation aboutit aujourd'hui à un triple échec : perte de souveraineté, développement industriel potentiellement biaisé et méconnaissance subséquente

(1) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Règlement (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

(3) Décret n° 2020-567 du 14 mai 2020 relatif aux traitements de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.

(4) Audition du 7 décembre 2022.

(5) Audition du 12 octobre 2022.

des principes européens et nationaux régissant la gestion des données à caractère personnel.

D'autre part, ces freins se conjuguent à l'absence de structure institutionnelle comparable au *National Institute of Standards and Technology* (NIST) américain. Créé en 1901, le NIST est une agence fédérale dépendant du département du commerce des États-Unis. Il représente l'organe de référence chargé d'accompagner les entreprises dans leur processus industriel, en leur fournissant notamment des données aux fins d'apprentissage des traitements algorithmiques.

La fourniture de données d'entraînement par le NIST est sollicitée par des entreprises françaises. Auditionnée le 6 décembre 2022, l'entreprise Idemia a souligné l'étroitesse des marges de manœuvre dont elle dispose afin d'entraîner ses algorithmes. Outre le recueil des données à caractère personnel de ses employés sur la base du volontariat et conformément aux règles rappelées par la CNIL, l'entreprise recourt au NIST pour tester ses traitements, sans être en mesure d'auditer les jeux de données qui lui sont fournis. Cette dépendance à une structure extra-européenne révèle le besoin impérieux d'identifier, en France, ou, à défaut, à l'échelle européenne, une entité susceptible de mettre à disposition des pouvoirs publics et des acteurs privés des échantillons d'images dans le seul but d'entraîner les traitements algorithmiques selon les cas d'usage autorisés, en respectant nos principes démocratiques.

Réclamée par l'ensemble des représentants de la sphère industrielle auditionnés par la mission d'information [(1)], la création de ces « *bacs à sable* » français ou européens requiert un encadrement juridique précis, conformément à l'article 53 de la proposition de règlement publiée par la Commission européenne le 21 avril 2021.

Les cas d'usage pour lesquels ces données à caractère personnel peuvent être utilisées doivent être déterminés de façon limitative. Par ailleurs, comme le précise notre collègue Éric Bothorel, il est nécessaire d'établir « *la démonstration que ces jeux de données d'apprentissage apporteraient une plus-value significative par rapport aux jeux d'apprentissage disponibles en source ouverte ou constitués par simulation d'acteurs volontaires* ». [(2)]

Si la durée de conservation de ces images doit être nécessairement plus longue que celle résultant de l'application du droit commun [(3)], il convient cependant de prévoir une durée maximale afin d'encadrer la phase de développement des traitements. Des exigences particulières de sécurisation, de

(1) Tels que l'Alliance pour la confiance numérique (ACN), auditionnée le 12 octobre 2022.

(2) Éric Bothorel, « Pour une politique publique de la donnée *», rapport remis au Premier ministre, décembre 2020, p. 131.*

(3) Soit, en l'état actuel du droit, sept jours pour les images captées par des caméras aéroportées et trente jours pour les images captées par des caméras de vidéoprotection.

contrôle et d'accès aux images méritent d'être imposées, eu égard aux menaces de cyberattaques et à la sensibilité des données dont il est question.

La constitution d'une base de données représentatives, sous le contrôle d'une autorité nationale ou européenne, est l'un des moyens les plus efficaces afin de lutter contre l'apparition de biais dans le fonctionnement des algorithmes. Cette évolution faciliterait la correction des paramètres utilisés selon chaque cas d'usage, en rendant ainsi effectif le principe de loyauté qui préside à l'emploi de ces systèmes d'intelligence artificielle.

Pour autant, il reste à définir l'organe susceptible d'exercer, en France ou en Europe, les missions dévolues au NIST américain. L'adoption, puis l'entrée en vigueur progressive du règlement européen à compter de 2025 pourraient justifier la mise en place à l'échelle de l'Union européenne d'un organisme, éventuellement adossé au contrôleur européen de la protection des données (CEPD) créé en 2018. Cette solution aurait le mérite d'harmoniser les pratiques au sein des États-membres et d'uniformiser les règles applicables à l'utilisation des données d'apprentissage.

Cependant, la création d'un NIST européen soulève plusieurs difficultés s'agissant des systèmes d'intelligence artificielle déployés en matière de sécurité.

D'une part, les images captées par des caméras aéroportées ou de vidéoprotection sous le contrôle des forces de l'ordre relèvent des enjeux de sécurité publique propres à chaque État-membre. D'autre part, les incertitudes entourant le calendrier de mise en œuvre du règlement européen peuvent entraîner un *statu quo* préjudiciable au développement des traitements algorithmiques, au risque de compromettre leur efficacité dans le cadre de la lutte contre l'insécurité et d'affecter durablement la compétitivité des entreprises françaises du secteur.

Auditionné le 9 novembre 2022, le Pôle d'expertise de la régulation numérique (PEREN), service à compétence nationale du ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, propose de créer une base de données commune, gérée par une entité unique à l'échelle nationale. Sur le modèle du NIST, les entreprises intéressées pourraient y accéder à la seule fin d'entraîner les algorithmes qu'elles développent et de générer des données synthétiques (1), sur la base de jeux de données mis à sa disposition.

L'entité précitée pourrait aussi être chargée de certifier les jeux de données, afin de garantir le respect des exigences de pertinence et de représentativité qui s'attachent à leur utilisation. Au regard de son champ d'intervention et de son expertise technologique, le Laboratoire national de

(1) https://linc.cnil.fr/fr/donnees-synthetiques-dis-papa-comment-fait-les-donnees-12

métrologie et d'essais (LNE) [1] semble présenter les qualités requises afin d'accomplir cette mission.

Dans son communiqué publié le 23 janvier 2023, la CNIL a présenté un programme de travail visant à définir une position officielle sur la constitution de base de données d'entraînement des traitements algorithmiques.

Ce travail [2] donnera lieu à la publication de fiches pratiques au cours de l'année 2023, afin de guider les développeurs dans l'utilisation de ces données.

Dans cette perspective, vos rapporteurs se prononcent résolument en faveur de la gestion d'une base de données centralisée à l'échelle nationale à des fins d'apprentissage des systèmes d'intelligence artificielle, sous la responsabilité d'un organisme *ad hoc* ou du LNE, suivant le modèle du NIST américain.

Recommandation n° 37 : Mettre en place une base de données centralisée à l'échelle nationale à des fins d'apprentissage des systèmes d'intelligence artificielle, sous la responsabilité d'un organisme *ad hoc* ou du Laboratoire national de métrologie et d'essais (LNE), suivant le modèle du NIST américain.

B. LA FRANCE À LA CROISÉE DES CHEMINS : ANTICIPER LES ÉVOLUTIONS DÈS AUJOURD'HUI POUR NE PAS ÊTRE DÉMUNI FACE AUX MENACES DE DEMAIN

Le développement de solutions d'intelligence artificielle pouvant être couplées à des caméras qui sont de plus en plus performantes doit être suivi et anticipé par les pouvoirs publics : elles représentent un défi pour la Justice, mais aussi un enjeu de souveraineté pour les forces de l'ordre.

(1) Établissement public à caractère industriel et commercial, le LNE est placé sous la tutelle du ministère de l'Économie. Il a pour but d'accompagner les industriels dans leur stratégie d'innovation, en exerçant notamment une mission de certification de produits ou de services.

(2) Le périmètre des réflexions initiées par la CNIL couvre les systèmes dont le développement ou l'amélioration nécessite la constitution d'une base de données, la collecte de données auprès de tous types de sources (collecte de données auprès des personnes concernées ou en source ouverte), les phases du développement d'un système nécessaires à sa mise en production ou à son amélioration (conception du système, prétraitement des données, entraînement, entraînement en continu, etc.) et les divers usages relatifs au développement ou à l'amélioration d'un système d'intelligence artificielle (recherche scientifique, recherche et développement, amélioration d'un produit commercial, etc.).

1. La justice doit anticiper les problématiques qui se poseront demain pour les images de sécurité

a. La jurisprudence sur les données de connexion pourrait faire tache d'huile

La jurisprudence de la Cour de justice de l'Union européenne (CJUE) a précisé ce qu'autorise le droit de l'Union s'agissant de la conservation et de l'accès aux données de connexion.

Dans un arrêt d'octobre 2020 (1), la CJUE a conclu que les mesures législatives prévoyant, à titre préventif, **une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation** (2) **étaient contraires au droit de l'Union européenne** (3), sauf dans les cas où l'État fait face à une menace grave, réelle, et actuelle ou prévisible pour la sécurité nationale, et sous réserve que la décision puisse faire l'objet d'un contrôle effectif par une juridiction ou une entité administrative indépendante. Le droit de l'UE opère donc une distinction dans le régime applicable à la conservation des données selon le degré de gravité de l'infraction.

(1) Arrêt de la Cour de justice de l'Union européenne du 6 octobre 2020, affaire La Quadrature du Net contre Premier ministre, *C-511/18.*

(2) Les données de trafic sont les informations techniques générées par l'utilisation des réseaux de communications tels qu'Internet et les données de localisation renseignent sur la position géographique.

(3) Et plus précisément à l'article 15, paragraphe 1 de la directive 2002/58 telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1 de la Charte des droits fondamentaux.

La Cour de cassation schématise ainsi les principes établis par la CJUE dans ses décisions [1] :

	Données relatives à l'identité civile des utilisateurs	**Adresses IP attribuées à la source d'une connexion**	**Données relatives au trafic et à la localisation**
En cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale	Conservation généralisée et indifférenciée	Conservation généralisée et indifférenciée	Conservation généralisée et indifférenciée
Lutte contre la criminalité grave	Conservation généralisée et indifférenciée	Conservation généralisée et indifférenciée pour une période temporellement limitée au strict nécessaire	Pas de conservation généralisée et indifférenciée, mais conservation ciblée pour une période temporellement limitée au strict nécessaire et injonction pour conservation rapide
Infractions ne relevant pas de la criminalité grave	Conservation généralisée et indifférenciée	Pas de conservation	Pas de conservation

Source : Cour de cassation.

La CJUE a également été amenée à se prononcer sur l'accès aux données de connexion.

Dans un arrêt du 2 mars 2021[2], la Cour considère que l'accès aux données de connexion ne peut être autorisé que dans la mesure où il est circonscrit à des procédures visant à **la lutte contre la criminalité grave ou à la prévention des menaces graves contre la sécurité publique**. Elle conclut également que le droit de l'Union « *s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale* ». Le ministère public ne peut donc autoriser l'accès aux données relatives au trafic et aux données de localisation.

(1) Cour de cassation – « Note explicative relative aux arrêts de la chambre criminelle du 12 juillet 2022 », *Conservation des données de connexion et accès.*

(2) Arrêt de la Cour de justice de l'Union européenne du 2 mars 2021, affaire H. K/Prokuratuur, *C-746/18.*

La chambre criminelle de la Cour de cassation a tiré les conséquences des décisions rendues par la CJUE dans quatre arrêts du 12 juillet 2022 (1) .

Dans l'affaire n° 21-83.710, elle a constaté que les articles du code de procédure pénale (CPP) portant sur les réquisitions faites par l'OPJ, que ce soit sur autorisation ou non du procureur de la République(2), sont contraires au droit de l'Union car ils ne prévoient pas un contrôle préalable par une juridiction ou une autorité administrative indépendante. Elle limite néanmoins les conséquences de cette non-conformité en considérant que seules les personnes démontrant l'existence d'une ingérence injustifiée dans leur vie privée suite à l'accès à leurs données personnelles peuvent faire état d'un grief fondé sur l'absence de compétence de l'autorité y ayant eu accès.

Le conseil d'administration de la Conférence nationale des procureurs de la République (CNPR), dans un communiqué publié le 15 juillet 2022, s'inquiète des conséquences de la jurisprudence de la Cour de cassation, faisant le constat de « *l'insécurité juridique majeure à laquelle doit faire face la lutte contre toutes les formes de délinquance* » et soulignant les difficultés pour les services enquêteurs et les magistrats du parquet de recourir à la téléphonie, en l'absence notamment de définition de la notion de « criminalité grave » (3).

Dans un article daté du 5 septembre 2022, Baptiste Nicaud, maître de conférences à l'université de Limoges, estime que « *la limite de l'accès aux données de connexion à ces deux critères que sont la criminalité grave – critère souple et non défini par la CJUE – et la stricte nécessité étaient inévitables eu égard à la jurisprudence de la CJUE* » (4).

La mise en conformité du CPP avait été amorcée avant même les arrêts rendus par la Cour de cassation : l'article 12 de la loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire a ainsi inséré dans le CPP un nouvel article (article 60-1-2) qui limite les réquisitions portant sur les données techniques à certaines infractions (5) .

Néanmoins, la question de l'accès par les magistrats du parquet aux données de connexion demeure. Le ministère de la Justice a ainsi indiqué au sénateur Yves Bouloux, dans une réponse à une question écrite publiée le 9 mars 2023, qu'« *une réflexion approfondie est actuellement menée par les services du ministère afin d'apporter une solution robuste et acceptable en pratique permettant*

(1) Arrêts de la chambre criminelle de la Cour de cassation, pourvois n° 21-83-710, 21-83.820, 21-84.096 et 20-86.652.

(2) Articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale.

(3) Communiqué de presse du conseil d'administration de la Conférence nationale des procureurs de la République, le 15 juillet 2022, « Conséquence des arrêts de la Cour de cassation relatifs aux données de connexion pour la lutte contre la délinquance ».

(4) Article publié sur Dalloz le 5 septembre 2022 par Baptiste Nicaud, maître de conférences à l'université de Limoges et avocat, « Restrictions à la conservation des données de connexion et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE ».

(5) Crime ou délit puni d'au moins trois ans d'emprisonnement.

de garantir l'efficacité de l'action des magistrats et des services enquêteurs en matière de lutte contre la criminalité » [(1)].

Les interlocuteurs de vos rapporteurs étaient partagés sur l'éventualité que cette jurisprudence sur les données de connexion puisse un jour être appliquée aux images filmées sur la voie publique.

M. Jean-Baptiste Parlos, premier président de la Cour d'appel de Rennes et membre de la Conférence nationale des premiers présidents, estime qu'il est possible que l'évolution de la jurisprudence ait pour conséquence que l'autorisation d'accéder aux images captées sur la voie publique ne puisse plus être une prérogative du parquet et doive passer par un juge du siège.

Cette analyse était en partie partagée par les représentants de la Conférence nationale des procureurs de la République. Selon eux, si le rapport à la vie privée n'est pas le même dans le cas de données de connexion et dans celui d'enregistrements vidéo non ciblés sur la voie publique, il ne peut pas être exclu qu'une jurisprudence vienne restreindre la capacité du ministère public à autoriser l'accès aux enregistrements vidéos sur le fondement de l'ingérence dans la vie privée.

Les professeurs de droit entendus en audition [(2)] par vos rapporteurs ont confirmé le risque que la jurisprudence sur les données de connexion soit reproduite s'agissant de l'accès aux images captées sur la voie publique.

Mme Pascale Léglise, DLPAJ du ministère de l'Intérieur et des outre-mer, considère à l'inverse que cette jurisprudence n'aura aucune conséquence sur la conservation et l'accès aux images captées dans l'espace public. La direction des affaires criminelles et des grâces (DACG) du ministère de la Justice, dans sa contribution écrite, souligne que la directive à l'origine de la jurisprudence sur les données de connexion concerne seulement les données à caractère personnel récupérées dans le cadre de services de communications électroniques. Partant de ce constat, elle n'envisage pas, à ce stade, que soient prises les mêmes restrictions pour l'accès aux images captées sur la voie publique.

Vos rapporteurs constatent le mouvement impulsé par le droit européen tendant à restreindre le contrôle des accès aux données à caractère personnel à une juridiction ou à une autorité administrative indépendante et considèrent que cette

---

(1) Réponse écrite du ministère de la Justice, publiée dans le Journal officiel le 9 mars 2023, en réponse à une question écrite n° 03041 de M. Yves Bouloux, sénateur, publiée le 6 octobre 2022, « Accès aux données de connexion dans le cadre des procédures pénales ».

(2) Table ronde du 24 janvier 2023, en présence de Mmes Florence Bellivier et Juliette Tricot, professeures au centre de droit pénal et de criminologie de l'Université Paris-Nanterre, membres du programme « L'appréhension des nouvelles technologies d'investigation et de surveillance par la procédure pénale *», M. Vissarion Giannoulis, post-doctorant, coordonnateur de recherche, M. Antonin Guillard, rédacteur d'une thèse «* Procédure pénale et renseignement : étude de l'hybridation de la répression et de la prévention *», et de M. Thibault Douville, professeur de droit, directeur du master droit du numérique à l'Université de Caen.*

jurisprudence pose, à nouveau, la question du statut du parquet et de son rôle d'autorité de poursuite.

Ils souhaitent ainsi alerter sur le risque que représenterait cette restriction de l'accès aux images, dans un moment où les parties privées ne sont pas soumises à ces exigences et peuvent produire des vidéos, voire de fausses vidéos. Le risque de renforcer l'asymétrie déjà existante entre les forces de l'ordre et les personnes mises en cause est réel.

b. Anticiper la multiplication d'images manipulées produites devant le tribunal

La notion de « *deepfake* » correspond à une fausse vidéo, générée par un outil d'intelligence artificielle. Les progrès réalisés ces dernières années complexifient leur détection, ce qui, transposé dans un procès pénal, constitue un énorme enjeu.

Des experts sont régulièrement sollicités pour travailler sur des images de sécurité. Le département compétent de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) fait ainsi état de 950 saisines annuelles sur le sujet, notamment pour améliorer des images dégradées ou les authentifier.

Le service national de police scientifique (SNPS) a lui été saisi en 2022 de 139 demandes d'expertises vidéo, essentiellement sur des images issues d'enregistrements de systèmes de vidéoprotection. Une dizaine de saisines du SNPS concernait l'authentification de vidéos : il s'agit alors de vérifier le type d'appareil à l'origine de l'enregistrement, de détecter des traces de coupure dans un enregistrement, mais aussi de détecter si l'image a été l'objet de manipulations ou si elle a été générée par l'intelligence artificielle.

Le SNPS a identifié en 2022 deux affaires de *deepfakes*, mais il anticipe une multiplication des saisines en authentification dans les années à venir. Il se prépare à cette augmentation en développant des logiciels de détection et en concentrant les travaux de recherche et développement sur ce sujet.

L'IRCGN comme le SNPS doivent être soutenus dans leurs efforts pour accompagner les évolutions technologiques. Vos rapporteurs estiment qu'il serait pertinent, à cet égard, de leur permettre d'avoir recours à des logiciels de reconnaissance faciale pour confirmer des comparaisons faites manuellement.

Recommandation n° 38 : Autoriser l'IRCGN et le SNPS, dans un cadre strictement judiciaire, à recourir à des logiciels de reconnaissance faciale pour confirmer des comparaisons faites manuellement.

Si ce sont bien les forces de l'ordre qui exploitent les images captées sur la voie publique, les magistrats doivent ensuite en faire l'interprétation.

Depuis le début de leurs travaux, vos rapporteurs ont constaté la multiplication d'images falsifiées (le pape François dans une doudoune blanche par exemple [(1)]), qui illustre l'accessibilité de la technologie. Le logiciel *MidJourney*, qui permet de générer des images artificielles à partir d'une requête textuelle, peut être utilisé en ligne pour la modique somme de 10 dollars par mois. Si les *deepfakes* ne sont pas systématiquement utilisés pour des usages malveillants (la BBC, chaîne britannique, l'a utilisé pour protéger l'identité de personnes interrogées [(2)]), il est probable qu'à l'avenir, que certaines personnes mises en cause y aient recours pour éviter les sanctions.

Vos rapporteurs alertent donc sur la nécessité pour le ministère de la Justice d'anticiper cette évolution, en sensibilisant les magistrats à l'existence de ces *deepfakes* et à l'importance de solliciter des experts au moindre doute. Les représentants de l'USM estiment que les magistrats ne sont pas suffisamment formés sur les images hyper-truquées, alors même que le sujet devrait être soulevé de plus en plus fréquemment s'agissant de vidéos fournies par des personnes privées. Compte tenu du coût des expertises dans ce domaine, une augmentation du budget des frais de justice sur ce poste-là est également à prévoir.

Dans sa contribution écrite aux travaux de vos rapporteurs, la DACG du ministère de la Justice a indiqué que le code pénal permettait déjà de sanctionner l'utilisation malveillante de *deepfakes* : l'article 226-8 du code pénal punit d'une peine d'un an d'emprisonnement le fait de publier le montage réalisé avec l'image ou les paroles d'une personne sans son consentement, sans indiquer explicitement qu'il s'agit d'un montage. L'article 226-4-1 du code pénal sanctionne, lui, le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de nature à l'identifier.

Les rapporteurs s'interrogent néanmoins sur la pertinence de ces deux articles lorsque le *deepfake* est une image complètement artificielle et non pas un montage à partir du visage d'une autre personne.

Recommandation n° 39 : Créer une infraction autonome réprimant le fait de produire une image manipulée devant les tribunaux.

2. Les enjeux de souveraineté liés au développement du marché de la vidéo améliorée

Vos rapporteurs en sont convaincus : **la France a le potentiel d'être pleinement souveraine s'agissant de la production de logiciels d'intelligence artificielle**. Cependant, elle dépend cruellement des importations en ce qui concerne le matériel informatique. En outre, le potentiel de recherche et

(1) « Macron en éboueur, pape en doudoune, Trump en état d'arrestation… Comment repérer les images générées par l'intelligence artificielle », *article de Franceinfo publié le 4 avril 2023*.

(2) « BBC documentary used face-swapping AI to hide protesters' identities », *article paru dans la revue NewScientist le 24 novembre 2022.*

développement est bridé par l'absence d'un cadre juridique clair et prévisible. Il est donc urgent d'encourager le développement par des entreprises françaises de solutions respectueuses des normes européennes.

a. La vidéo augmentée, un marché mondial très important sur lequel la France a des difficultés à se positionner

Selon les données transmises par la CNIL dans sa contribution écrite, le marché de la vidéo augmentée est en croissance rapide – environ 7 % par an – et est estimé à 11 milliards d'euros en 2020. La CNIL observe que le marché se partage entre de grands industriels, plutôt positionnés sur la fabrication de matériels, et des *start-up*, plutôt engagées sur le développement de technologies d'analyse des flux vidéo fondées sur des algorithmes.

Or, vos rapporteurs ont pu constater, au cours de leurs travaux, que la France a des difficultés à se positionner sur le marché de la vidéoprotection et à y prendre toute sa part, que ce soit en matière de matériel ou de logiciels, malgré l'existence d'un réseau académique de qualité et d'entreprises innovantes.

Dans sa contribution écrite, la CNIL explique ainsi :

« *le marché français est détenu essentiellement par des acteurs étrangers.* ***En 2015, plus d'un tiers des équipements de vidéoprotection étaient importés de Chine****, mais des acteurs étatsuniens, allemands et suédois sont également présents. De fait, si la France dispose de leaders mondiaux en matière de sécurité électronique, gestion des identités d'accès et cybersécurité, elle ne dispose pas encore d'acteurs de cette taille pour ce qui est des équipements vidéo* » (1).

Plusieurs des entreprises interrogées ont confirmé cette dépendance de la France aux fournisseurs étrangers, notamment dans le secteur de la vidéo augmentée.

S'agissant du développement de logiciels d'intelligence artificielle pouvant être couplés à des caméras, les chercheurs issus des principaux centres de recherche publics expliquent que les recherches sont freinées à la fois par les difficultés d'accès à la donnée pour entraîner les algorithmes et par la forte dépendance des projets de recherche aux financements européens.

Le cadre normatif, qui restreint fortement les possibilités d'expérimentations, comme indiqué précédemment, dissuade les entreprises d'investir en France. Certaines entreprises françaises ont ainsi fait part des difficultés qu'elles rencontrent en raison de leur mise en concurrence avec des entreprises étrangères qui ne sont pas soumises aux mêmes contraintes. Lors du déplacement de vos rapporteurs à Monaco, la direction de la sûreté publique a indiqué avoir préféré un logiciel développé par une société israélienne à un logiciel développé par une entreprise française en raison du manque de maturité de ce

(1) Contribution écrite de la CNIL aux travaux des rapporteurs.

dernier. À l'inverse, certaines entreprises étrangères interrogées par vos rapporteurs ont indiqué ne pas vouloir s'engager sur le marché français, considéré comme trop incertain.

b. Le développement de solutions européennes et françaises doit être encouragé pour préserver la souveraineté française

L'absence de maîtrise des logiciels développés, alors même que ces logiciels ont vocation à être couplés aux caméras installées sur la voie publique, est un réel facteur de vulnérabilité.

Pascale Léglise, DLPAJ du ministère de l'Intérieur et des outre-mer, a rappelé que les logiciels étrangers utilisés devaient respecter le RGPD (1) et la loi Informatique et Libertés de 1978 (2).

Il n'en reste pas moins que la nécessité d'importer des composants électroniques et des logiciels renforce la dépendance de la France vis-à-vis des entreprises et des pays étrangers. Il faut donc travailler à renforcer les filières françaises et européennes pour proposer des solutions de nature à renforcer la capacité de la France à être souveraine dans le domaine des algorithmes.

Dans son rapport sur la stratégie à adopter concernant l'intelligence artificielle, l'ancien député de l'Essonne Cédric Villani affirme que « *dans les prochaines années, l'utilisation de l'intelligence artificielle sera une nécessité pour assurer les missions de sécurité, conserver l'ascendant face à nos adversaires potentiels, tenir notre rang par rapport aux alliés (aussi bien au sein de coalitions que dans une perspective d'export) et maintenir un niveau de qualité élevé concernant les services dispensés à l'ensemble des personnels des ministères* » (3).

Vos rapporteurs partagent ce point de vue. La question de la capacité de la France à exercer sa **compétence régalienne de sécurité** sur son territoire (*souveraineté interne*) et sur le plan international se pose avec acuité depuis l'émergence de ces nouvelles technologies.

Ils remarquent que l'écosystème français lié à l'intelligence artificielle demeure dynamique, et considèrent que l'objectif de n'avoir recours qu'à des solutions françaises ou européennes n'apparaît pas complètement hors d'atteinte. Ainsi, le délégué interministériel aux Jeux olympiques et paralympiques (JOP), M. Michel Cadot, a indiqué au cours de son audition que 85 % des solutions utilisées dans le cadre des JOP seraient françaises.

---

(1) Règlement (UE) 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, et abrogeant la directive 95/46/CE.

(2) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(3) Rapport de Cédric Villani, parlementaire en mission, publié le 28 mars 2018, « Donner un sens à l'intelligence artificielle – Pour une stratégie nationale et européenne », p 219.

Les universitaires entendus par vos rapporteurs ont également souligné l'existence, au niveau européen, d'un mouvement visant à développer des outils européens pour maintenir une forme d'autonomie pour les États membres de l'Union sur l'usage de l'intelligence artificielle.

La CNIL suggère que c'est la partie logicielle de la chaîne qui devrait être soutenue par les pouvoirs publics, car il s'agit d'un domaine dans lequel la France peut encore être compétitive, contrairement à la production de matériel.

Vos rapporteurs rejoignent la CNIL sur ce point, et considèrent que la création d'une base de données centralisée, évoquée précédemment, est justement de nature à encourager l'innovation et le développement de solutions d'intelligence artificielle par les entreprises françaises.

Au-delà d'un accès à des jeux de données, vos rapporteurs plaident pour un investissement public renforcé dans le développement de solutions françaises et européennes d'intelligence artificielle, afin de soutenir activement le développement d'une filière française.

Recommandation n° 40 : Soutenir, par le biais d'appels à projets, les entreprises françaises qui développent des solutions d'intelligence artificielle pouvant être couplées avec des images.

La sécurisation des données est également un vrai enjeu.

Le risque cyber a ainsi été souligné à plusieurs reprises pendant les auditions. La représentante de Bouygues, lors de son audition, a indiqué que quatre caméras sur dix installées dans le monde présentent un risque cyber. L'entreprise Atos juge que le déploiement de la 5G va encore accroître le risque de captation des images et des données.

Les problématiques de stockage des données, déjà évoquées précédemment, ne concernent pas que les forces de l'ordre. Les entreprises ont elles-mêmes des inquiétudes concernant la saturation de l'hébergement de leurs données sur des serveurs physiques. Certaines entreprises ont indiqué avoir recours à des solutions de stockage américaines, en l'absence de *cloud* [nuage numérique] européen ou français. Or, les travaux européens ne semblent malheureusement pas encore, à ce stade, aboutis [(1)]. Vos rapporteurs déplorent ce retard et espèrent qu'une solution européenne sera rapidement accessible aux entreprises et aux forces de l'ordre.

Recommandation n° 41 : Créer un *cloud* souverain et non soumis à des règles d'extra-territorialité.

(1) Article publié le 30 mai 2022 sur Contexte, « Gaia-X, ou les illusions perdues d'un cloud européen ».

CONCLUSION

À l'issue de six mois de travaux, les 41 recommandations formulées par la mission d'information s'inscrivent dans des horizons temporels différents et dessinent des perspectives dans des domaines multiples. Les urgences de court terme, qu'elles concernent l'entrée en vigueur de dispositions règlementaires très attendues ou l'expérimentation prochaine des caméras « augmentées », ne doivent pas occulter des enjeux de moyen et long terme. Ainsi, l'immixtion, progressive mais inéluctable, de l'intelligence artificielle dans les technologies de sécurité pose des défis considérables, qui doivent conduire à s'interroger sur l'équilibre habituel entre l'impératif de sécurité et la nécessaire protection des libertés.

La définition d'un cadre juridique clair et précis, sans être rigide ni lacunaire, représente un objectif ambitieux. C'est au Parlement qu'il revient de se saisir régulièrement de l'ensemble de ces questions, à l'épreuve des évolutions techniques et sociétales auxquelles nous sommes collectivement confrontés. C'est aussi à cette condition que la France consolidera sa souveraineté, en permettant à ses représentants de choisir librement, et de façon éclairée, les règles permettant de concilier, aujourd'hui et demain, la préservation de l'ordre public et le respect des droits fondamentaux.

Dans « L'art poétique », Nicolas Boileau écrivait : « *Hâtez-vous lentement, et sans perdre courage, vingt fois sur le métier remettez votre ouvrage* ». Gageons que ce rapport d'information puisse utilement nourrir les nombreux débats qui entourent légitimement les questions de sécurité, au cœur de notre vie démocratique.

TRAVAUX DE LA COMMISSION

LISTE DES RECOMMANDATIONS

Recommandation n° 1 : Engager une refonte des règles applicables à l'ensemble des dispositifs de captation d'images dans l'espace public, suivant un double objectif de rationalisation et d'unification du cadre juridique fixé par le code de la sécurité intérieure.

Recommandation n° 2 : Publier de toute urgence les décrets d'application prévus par la loi du 24 janvier 2022 relatifs à l'utilisation des caméras embarquées et des caméras aéroportées en matière de police judiciaire et de police administrative.

Recommandation n° 3 : Clarifier les règles de financement de l'acquisition et de l'installation des systèmes de vidéoprotection par les collectivités territoriales.

Recommandation n° 4 : Réviser l'arrêté ministériel du 3 août 2007 afin de mettre à jour les exigences techniques auxquelles doivent satisfaire les systèmes de vidéoprotection.

Recommandation n° 5 : Autoriser le poste de commandement à déclencher à distance les caméras-piétons uniquement à la demande des agents sur le terrain et prévoir un déclenchement automatique de l'enregistrement lorsque l'agent fait usage de son arme.

Recommandation n° 6 : Circonscrire l'interdiction de recueil des images de l'entrée d'un domicile par une caméra embarquée à son seul caractère « permanent ».

Recommandation n° 7 : Disposer d'une bande de fréquence dédiée à la transmission sécurisée des données captées par des caméras aéroportées.

Recommandation n° 8 : Harmoniser les temps de conservation des images en fixant une durée de 30 jours quel que soit le vecteur de captation utilisé.

Recommandation n° 9 : Tendre à la fixation d'une durée minimale de conservation des données.

Recommandation n° 10 : Élargir la liste des finalités d'accès aux images de la vidéoprotection à certaines des missions des services de renseignement spécialisés, notamment le contre-espionnage.

Recommandation n° 11 : Modifier l'article L. 233-2 du code de la sécurité intérieure afin de permettre la consultation des données LAPI pour prévenir et caractériser les infractions liées au terrorisme et à la criminalité organisée.

Recommandation n° 12 : Réviser le code de la sécurité intérieure pour simplifier le cadre juridique relatif à la captation d'images, en adoptant une approche transversale plutôt qu'une approche par vecteurs.

Recommandation n° 13 : Anticiper la saturation du stockage sur des serveurs physiques et financer la création d'un cloud souverain.

Recommandation n° 14 : Créer un scellé numérique pour permettre une transmission dématérialisée des images issues de caméras.

Recommandation n° 15 : Créer un socle d'hébergement mutualisé et hautement sécurité, sur lequel les différents détenteurs d'images de vidéo protection (opérateurs de transports, collectivités territoriales) pourraient les télécharger.

Recommandation n° 16 : Conduire une évaluation de l'efficacité de la vidéoprotection.

Recommandation n° 17 : Prévoir un module pour les magistrats lors de la formation initiale à l'École nationale de la magistrature (ENM) sur le recueil et le traitement des images numériques dans l'enquête.

Recommandation n° 18 : Déterminer un cadre d'évaluation objectif, précis et standardisé des expérimentations de dispositifs de vidéoprotection « augmentée » et garantir le respect des obligations d'information du public.

Recommandation n° 19 : Réaliser, sous l'égide de l'ANSSI, un audit de l'ensemble des systèmes de vidéoprotection susceptibles d'être couplés à des traitements algorithmiques dans le cadre de l'expérimentation autorisée par le projet de loi JOP 2024.

Recommandation n° 20 : Veiller à garantir l'interopérabilité des systèmes de vidéoprotection et d'intelligence artificielle mis en œuvre dans le cadre de l'expérimentation.

Recommandation n° 21 : Mesurer l'efficacité des caméras « augmentées » selon le dispositif de captation d'images utilisé.

Recommandation n° 22 : Privilégier l'usage de technologies de vidéoprotection intelligente conçues et développées en France ou sur le territoire d'un État membre de l'Union européenne.

Recommandation n° 23 : Prévoir la publication du rapport du magistrat référent chargé de suivre la mise en œuvre et la mise à jour des traitements automatisés de données à caractère personnel.

Recommandation n° 24 : Prévoir l'obligation d'identifier l'origine de la photographie entrée dans le TAJ à des fins de comparaison.

Recommandation n° 25 : Procéder à une mise à jour complète du TAJ pour s'assurer que les données à caractère personnel qui ne doivent plus y être n'y sont plus.

Recommandation n° 26 : Accélérer l'interconnexion entre TAJ et Cassiopée.

Recommandation n° 27 : Désigner le ministère, entre la Justice et l'Intérieur, qui soit responsable du TAJ dans tous ses aspects.

Recommandation n° 28 : Autoriser à titre expérimental l'utilisation de Parafe pour les enfants au-dessus de 12 ans.

Recommandation n° 29 : Prévoir un cadre expérimental permettant de tester des solutions de reconnaissance biométrique dans le cadre judiciaire, pour retrouver a posteriori un individu.

Recommandation n° 30 : Autoriser, pour certains cas d'extrême urgence ou des recherches sensibles, le traitement en temps réel de logiciels de reconnaissance faciale pour les forces d'intervention pendant une durée limitée, sous le contrôle de l'autorité judiciaire.

Recommandation n° 31 : Développer un dispositif de certification des logiciels de reconnaissance faciale qui répondent aux exigences de protection des données à caractère personnel.

Recommandation n° 32 : Maintenir l'obligation de publication d'un rapport annuel d'activité des commissions départementales de vidéoprotection, faisant notamment état du nombre d'avis rendus en amont de l'installation des systèmes de vidéoprotection et des suites données aux avis, ainsi qu'aux contrôles diligentés sur le fonctionnement de ces systèmes.

Recommandation n° 33 : Renforcer le rôle des commissions départementales de vidéoprotection en publiant les avis qu'elles prononcent dans le cadre de la procédure d'installation des caméras et en les rendant destinataires de la décision d'autorisation ou de refus prise par le préfet à la suite de leurs avis.

Recommandation n° 34 : Réaliser, sous l'égide des préfectures et des services centraux du ministère de l'Intérieur et des outre-mer, une cartographie nationale de l'emplacement de toutes les caméras de vidéoprotection installées sur l'ensemble du territoire.

Recommandation n° 35 : Prévoir la création de comités d'éthiques dans les communes dès lors que le nombre de caméras de vidéoprotection installées excède un certain seuil par habitant, ou qu'un système d'intelligence artificielle est couplé aux dispositifs de captation d'images.

Recommandation n° 36 : Consacrer la CNIL en tant que « chef de file » de la régulation des systèmes d'intelligence artificielle, d'une part en renforçant ses ressources humaines et techniques pour accomplir cette mission et d'autre part, en élargissant la composition de son collège aux présidents de l'ARCEP et de l'ARCOM.

Recommandation n° 37 : Mettre en place une base de données centralisée à l'échelle nationale à des fins d'apprentissage des systèmes d'intelligence artificielle, sous la responsabilité d'un organisme ad hoc ou du Laboratoire national de métrologie et d'essais (LNE), suivant le modèle du NIST américain.

Recommandation n° 38 : Autoriser l'IRCGN et le SNPS, dans un cadre strictement judiciaire, à recourir à des logiciels de reconnaissance faciale pour confirmer des comparaisons faites manuellement.

Recommandation n° 39 : Créer une infraction autonome réprimant le fait de produire une image manipulée devant les tribunaux.

Recommandation n° 40 : Soutenir, par le biais d'appels à projets, les entreprises françaises qui développent des solutions d'intelligence artificielle pouvant être couplées avec des images.

Recommandation n° 41 : Créer un cloud souverain et non soumis à des règles d'extra-territorialité.

PERSONNES ENTENDUES

Mardi 11 octobre 2022

- **Bouygues énergies et services**
  - — Mme Hélène Gaury, directrice technico-commerciale
- **Datakalab**
  - — M. Xavier Fischer, président
- **One Point**
  - — M. Gontran Peubez, associé en charge des activités data et intelligence artificielle

Mercredi 12 octobre 2022

- **Centre national de la recherche scientifique (CNRS)**
  - — M. Jamal Atif, coordinateur du défi Intelligence artificielle, chargé de mission à l'INS2I
- **Commissariat à l'énergie atomique et aux énergies alternatives** (**CEA**)
  - — M. François Terrier, chercheur expert en intelligence artificielle (IA) et directeur du programme IA de CEA Tech
  - — M. Patrick Sayd, chercheur expert en IA et directeur du Service d'IA pour le langage et la vision de l'institut List du CEA
  - — M. Nizar Touleimat, responsable affaires européennes, sécurité et défense et coordinateur du projet européen Starlight
- **INRIA**
  - — Mme Sandrine Mazetier, directrice générale déléguée à l'appui aux politiques publiques
- **Alliance pour la Confiance Numérique (ACN)**
  - — M. Daniel Le Coguic, président
  - — M. Yoann Kassianides, délégué général

Mardi 18 octobre 2022

- **Commission nationale de l'informatique et des libertés (CNIL)**
  - — Mme Marie-Laure Denis, présidente
  - — M. Thomas Dautieu, directeur de l'accompagnement juridique
  - — M. Bertrand Pailhès, directeur des technologies et de l'innovation
  - — Mme Chirine Berrichi, conseillère pour les questions parlementaires et institutionnelles

Mardi 25 octobre 2022

- **Direction Générale de la Police Nationale (DGPN)**
  - — M. Jérôme Léonnet, directeur général adjoint
  - — M. Alex Gadré, conseiller juridique
  - — Mme Marie-Laure Arnaud-Guidoux, conseillère doctrine défense planification renseignement
- **Table ronde d'interventions spécialisées**

  Brigade de Recherche et d'Intervention (BRI) de la Préfecture de police de Paris
  - — M. Simon Riondet, commissaire divisionnaire

  Groupement d'Intervention de la Gendarmerie Nationale (GIGN)
  - — M. David Cazimajou, colonel, commandant en second

  Recherche Assistance Intervention Dissuasion (RAID)
  - — M. Jean-Baptiste Dulion, chef du service
- **Ministère de l'Intérieur - Service des technologies et des systèmes d'information de la sécurité intérieure — ST(SI)2**
  - — M. Frédéric Aubanel, chef du service

Mercredi 26 octobre 2022

- **Société XXII**
  - — M. William Eldin, président
  - — M. François Mattens, directeur des affaires publiques
  - — Mme Clara Legros, responsable juridique

- **Délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité**
  - — M. Olivier-Pierre de Mazières, préfet, délégué ministériel
  - — Mme Élisabeth Sellos-Cartel, chargée des sujets de vidéoprotection

Mardi 8 novembre 2022

- **Direction générale des douanes et droits indirects (DGDDI)**
  - — Mme Élisabeth Melscoët, adjointe au chef du bureau, directrice des services douaniers
- **Direction nationale du renseignement et des enquêtes douanières (DNRED)**
  - — M. Florian Colas, directeur
  - — Mme Marie Friocourt, secrétaire générale
  - — Mme Alice Cherif, conseillère juridique
  - — Mme Florence Lalanne, conseillère juridique adjointe
- **Délégation interministérielle aux jeux olympiques et paralympiques Paris 2024 (DIJOP)**
  - — M. Michel Cadot, délégué interministériel
  - — M. Christophe Delaye, commissaire divisionnaire de police, conseiller en charge de la sécurité

Mercredi 9 novembre 2022

- **Direction générale des entreprises**
  - — M. Aurélien Palix, sous-directeur des réseaux et des usages numériques
  - — M. Julien Vignon, directeur de projet intelligence artificielle
  - — Mme Emmanuelle Legrand, chargée de mission intelligence artificielle
- **Pôle d’expertise et de régulation numérique (PeREN)**
  - — M. Nicolas Deffieux, directeur
  - — M. Victor Amblard, analyste des données
- **Préfecture de police**
  - — M. Charles Moreau, préfet, secrétaire général pour l’administration
  - — M. Arnaud Mazier, directeur de l’innovation, de la logistique et des technologies
  - — M. Philippe Dalbavie, conseiller juridique

Mardi 15 novembre 2022

- **Secrétariat général de la défense et de la sécurité nationale (SGDSN)**
  - — M. Nicolas de Maistre, directeur de la protection et de la sécurité de l'État
  - — Mme Catherine Munsch, conseillère juridique
  - — M. François Murgadella, conseiller technologie de sécurité
- **Direction générale de la Sécurité intérieure (DGSI)**
  - — M. Nicolas Lerner, directeur
  - — Mme Caroline Boussion, conseillère juridique

Mercredi 16 novembre 2022

- **Table ronde des syndicats de commissaires de police**

  Syndicat des commissaires de la police nationale (SCPN)
  - — M. Christophe Gradel, secrétaire général adjoint

  Syndicat indépendant des commissaires de police (SICP)
  - — M. Matthieu Valet, porte-parole
- **Syndicat des cadres de la sécurité intérieure (SCSI)**
  - — M. Christophe Miette, secrétaire national
  - — M. Léo Moreau, chargé de mission

Mardi 22 novembre 2022

- **Commission nationale consultative des droits de l'homme (CNCDH)**
  - — M. Jean-Marie Burguburu, président
  - — M. Thomas Dumortier, conseiller juridique
- **Conseil d'État**
  - — M. Thierry Tuot, conseiller d'État

Mardi 29 novembre 2022

- **Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP)**
  - — M. Franck Tarrier, directeur mobile et innovation
  - — M. Patrick Lagrange, chef de l'unité fréquences et technologies

- **Direction générale de la gendarmerie nationale (DGGN)**
  - — M. Bruno Jockers, major général
  - — M. Antoine Lagoutte, lieutenant-colonel
  - — M. Christophe Meneau, chef d'escadron

- **Table ronde élus locaux**

Association des maires de France (AMF)

- — M. Denis Mottier, chargé de mission sécurité
- — M. Lionel Ledemay, chargé de mission sécurité
- — Mme Charlotte de Fontaines, chargée des relations avec le Parlement

Association des Petites Villes de France (APVF)

- — M. Romain Colas, maire de Boussy-Saint-Antoine
- — M. Elias Maaouia, conseiller

Assemblée des départements de France (ADF)

- — M. Alexandre Touzet, président du groupe de travail sur la prévention de la délinquance et de la radicalisation, vice-président du département de l'Essonne
- — M. Jean-Baptiste Estachy, conseiller sécurité
- — M. Brice Lacourieux, conseiller relations avec le Parlement

Régions de France

- — M. Frédéric Péchenard, vice-président du conseil régional d'Île-de-France, chargé de la sécurité et de l'aide aux victimes
- — M. Enguerrand Delannoy, conseiller parlementaire de la présidente de la Région Île-de-France
- — M. Salem Belgourch, directeur du service sécurité et aide aux victimes
- — M. Alexandre Gaye, chargé de mission coordination transversale des politiques de sécurité

Intercommunalités de France (ex AdCF)

- — M. Luc Strehaiano, président de la communauté d'agglomération de Plaine Vallée
- — M. Dominique Guilloux, directeur sécurité publique et prévention
- — Mme Montaine Blonsard, responsable des relations avec le Parlement

Mercredi 30 novembre 2022

- **Table ronde des syndicats représentatifs de la police nationale**

  Unité SGP Police FO

  — M. Jérôme Moisant, secrétaire général adjoint

  — M. Dominique Le Dourner, secrétaire national aux conditions de travail

  Alternative Police CFDT

  — M. Pascal Jakowlew, secrétaire national

  — M. Guillaume Ruet, secrétaire national

- **Table ronde des représentants des avocats**

  Conseil national des barreaux

  — M. Boris Kessel, membre de la commission libertés et droits de l'homme

  — M. Gérard Tcholakian, membre de la commission libertés et droits de l'homme

  — M. Philippe Baron, président de la commission numérique

  — Mme Émilie Guillet, chargée d'affaires publiques

  Conférence des bâtonniers

  — M. Jérôme Dirou, membre du bureau, président de la commission pénale

  Barreau de Paris

  — M. Vincent Nioré, vice-bâtonnier

  — M. Julien Brochot, membre du conseil de l'ordre des avocats

Mardi 6 décembre 2022

- **Coordination nationale du renseignement et de la lutte contre le terrorisme**

  — M. Hugues Bricq, coordonnateur adjoint

  — M. Basile Jomier, conseiller

- **Société IDEMIA**

  — M. Yves Portalier, senior vice-président pour la France

  — Mme Sandra Valerii, vice-présidente affaires publiques et relations presse groupe

  — M. Vincent Bouatou, directeur général adjoint

Mercredi 7 décembre 2022

- **Conférence des premiers présidents des cours d'appel**
  - — M. Jean-Baptiste Parlos, premier président de la cour d'appel de Reims
- **Table ronde de chercheurs en sciences sociales**
  - — M. Antoine Courmont, directeur scientifique de la chaire Villes et numérique de Sciences Po
  - — M. Myrtille Picaud, chargée de recherche en sociologie au CNRS
- **Table ronde de mathématiciens**
  - — M. Yann Gousseau, mathématicien, professeur à Télécom Paris et responsable de l'équipe images
  - — M. Jean-Michel Morel, mathématicien à l'École normale supérieure Paris-Saclay
  - — M. Erwan Le Pennec, professeur en mathématiques appliquées à l'École Polytechnique
  - — M. Jean-Gabriel Ganascia, président du comité d'éthique du CNRS, spécialiste en intelligence artificielle, apprentissage machine et fouilles de données

Mardi 13 décembre 2022

- **Unité Magistrats**
  - — M. Marc Lifchitz, secrétaire général adjoint
  - — Mme Valérie Dervieux, déléguée régionale sur le ressort de la Cour d'appel de Paris
- **Security Systems (Groupe PROTEC)**
  - — M. Gil Ancelin, président

Mercredi 14 décembre 2022

- **La quadrature du net**
  - — Mme Marne Strazielle, directrice de la communication
  - — Mme Noémie Levain, juriste

- **Table ronde**

  Amnesty International France

  — Mme Katia Roux, chargée de plaidoyer libertés

  La Ligue des droits de l'homme

  — Mme Nathalie Tehio, membre du Bureau national

Mardi 10 janvier 2023

- **Groupe Axon**
  — Mme Cathy Robin, directrice générale France, Belgique, Afrique, Europe centrale et orientale
  — M. Christophe Thibault, directeur France

Mercredi 11 janvier 2023

- **Union syndicale des magistrats**
  — M. Aurélien Martini, secrétaire général adjoint
  — M. Thierry Griffet, trésorier national
- **Syndicat de la magistrature**
  — M. Laurent Desgouis, secrétaire national
  — M. Thibaut Spriet, secrétaire national
- **Société Atos**
  — M. Philippe Oliva, directeur général délégué, co-CEO en charge des activités BDS & Digital (« Evidian »)
  — M. Jean-Philippe Poirault, directeur big data et cybersécurité (BDS)

Mardi 24 janvier 2023

- **M. Alain Bauer,** professeur de criminologie au Conservatoire national des arts et métiers (CNAM)
- **Table ronde de professeurs de droit**
  — Mmes Florence Bellivier et Juliette Tricot, professeures au centre de droit pénal et de criminologie de l'université Paris-Nanterre, membres du programme « L'appréhension des nouvelles technologies d'investigation et de surveillance par la procédure pénale »
  — M. Vissarion Giannoulis, post-doctorant, coordonnateur de recherche

— M. Antonin Guillard, rédacteur d'une thèse « Procédure pénale et renseignement : étude de l'hybridation de la répression et de la prévention »

— M. Thibault Douville, directeur du master Droit du numérique à l'université de Caen

- **Comité d'éthique de vidéosurveillance de la ville de Paris**

— M. Christian Vigouroux, président

Mercredi 25 janvier 2023

- **Ministère de la Justice - Direction des affaires criminelles et des grâces (DACG)**

— Mme Sophie Macquart-Moulin, adjointe du directeur

— Mme Pauline Lemercier, magistrate

Mercredi 1er février 2023

- **Groupe Thales**

— M. Lionel Le Clei, vice-président, conseiller opérationnel sécurité globale du président-directeur général

Mardi 7 février 2023

- **Ministère de l'Intérieur - Direction des libertés publiques et des affaires juridiques**

— Mme Pascale Léglise, directrice

— Mme Léa Quiau, cheffe du bureau du droit des données et des nouvelles technologies

DÉPLACEMENTS

Jeudi 27 octobre 2022 : Nantes

- **Préfecture de Loire-Atlantique**
  — M. Didier Martin, préfet
- **Football club de Nantes**
  — M. Waldemar Kita, président
  — M. Loïc Morin, secrétaire général
  — M. Olivier Feneteau, directeur de la sécurité
- **Table ronde**
  — Représentants de la mairie de Nantes
  — Représentants de l'intercommunalité Nantes Métropole
  — Représentants de la police nationale
  — Représentants de la gendarmerie nationale
  — Représentants du Handball club de Nantes
  — Représentants des organisateurs du festival de musique *Hell Fest*

Mercredi 30 novembre 2022 : maison de la Sûreté de la SNCF, Paris

- **SNCF**
  — M. Xavier Roche, directeur de la sûreté
  — M. Christophe Bouteille, directeur adjoint de la sûreté, directeur des opérations SUGE
  — M. Jérôme Cipriani, secrétaire général de la direction de la sûreté
  — M. Jérôme Bertin, directeur de la prospective
  — M. Rémi Legrand, directeur du département programmes, performances et innovations
  — M. Nicolas Despalles, responsable du laboratoire innovation et programme vidéo intelligent GPU
  — M. Armand Raudin, responsable du programme vidéo et innovation
  — Mme Laurence Nion, conseillère parlementaire

Mercredi 14 décembre 2022 : Aéroport Charles de Gaulle

- **Groupe ADP**
  — Mme Alexandra Locquet, directrice audit, sécurités et maîtrise des risques
  — M. Bastien Bernard, directeur des opérations aéroportuaires
  — M. Mathieu Cuip, directeur des affaires publiques
  — M. Paul Beyou, chargé des affaires publiques nationales
- **Police aux frontières**
  — Mme Valérie Minne, directrice centrale adjointe

Mercredi 18 janvier et jeudi 19 janvier 2023 : Monaco, Cannes, Nice

- **Direction de la Sûreté publique de Monaco**
  — M. Richard Marangoni, contrôleur général
  — M. Régis Bastide, directeur adjoint
- **Ambassade de France à Monaco**
  — M. Laurent Stefanini, ambassadeur
  — M. Mathieu Schuster, premier conseiller
- **Mairie de Cannes**
  — M. David Lisnard, maire
  — M. Thierry Migoule, directeur de cabinet
- **Conférence nationale des procureurs**
  — M. Xavier Bonhomme, procureur de la République près le tribunal judiciaire de Nice
  — M. Damien Savarzeix, procureur de la République près le tribunal judiciaire de Grasse
- **Commission départementale de vidéoprotection**
  — M. Hicham Melhem, président
  — M. Bertrand Gasiglia, membre
  — M. Gérald Vivier, membre
- **Préfecture des Alpes-Maritimes**
  — M. Bernard Gonzalez, préfet
  — M. Benoît Huber, directeur de cabinet
- **Mairie de Nice**

— Mme Véronique Borre, directrice générale adjointe Sécurité – Proximité.

— M. Jérôme Marcenac, directeur de la police municipale de Nice

— M. Christophe Gardon, responsable adjoint de la police municipale de Nice

— M. Nicolas Maillan, directeur des systèmes d'information

— M. Grégory Petzet, responsable du Centre de supervision urbain

— Mme Manuela Grossi, chargée de mission

— M. Jean-François Ona, chargé de mission

Lundi 13 mars au mercredi 15 mars 2023 : Israël

- **Centre de supervision de la police nationale à Tel-Aviv**
- **Ambassade de France en Israël**

  — M. Éric Danon, ambassadeur

  — Mme Margaux Bergeon-Dars, première conseillère

  — Mme Joëlle Conte, attachée de sécurité intérieure

  — M. Uriel Gadessaud, attaché politique
- **Centre du Magen David Adom**
- **Entreprises israéliennes**

  — Oosto

  — Viisights

  — Sigtech

  — Atlas