N° 609
SÉNAT

SESSION ORDINAIRE DE 2025-2026

Enregistré à la Présidence du Sénat le 12 mai 2026

PROPOSITION DE LOI

visant à **généraliser** *la* **vidéoprotection algorithmique**,

PRÉSENTÉE

Par MM. Pierre-Jean VERZELEN, Pierre MÉDEVIELLE, Jean-Pierre GRAND, Cédric CHEVALIER, Marc LAMÉNIE, Pierre Jean ROCHETTE, Mme Corinne BOURCIER, M. Jean-Luc BRAULT, Mme Marie-Pierre BESSIN-GUÉRIN et M. Olivier PACCAUD,

Sénateurs et Sénatrices

(Envoyée à la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, sous réserve de la constitution éventuelle d'une commission spéciale dans les conditions prévues par le Règlement.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

La crainte d'être surpassé voire contrôlé par les machines n'est pas un nouveau débat mais s'accentue avec le développement exponentiel de l'intelligence artificielle. Toutefois, s'il peut inspirer de la méfiance, l'outil numérique peut également être un atout inestimable s'agissant de nombreux usages, notamment, afin d'assurer la protection et la sécurité des personnes et des biens. Malgré cette appréhension, l'usage de l'intelligence artificielle se multiplie au quotidien, que ce soit dans l'espace public, notamment dans les aéroports, mais aussi dans l'espace privé, pour déverrouiller un smartphone ou accéder à des comptes bancaires.

Depuis sa mise en place en 1995, la vidéoprotection dans l'espace public s'est fortement développée en France. Après les métropoles et autres grandes villes, les communes rurales se sont équipées. Le développement de la vidéoprotection s'inscrit dans une période où des évolutions politiques, réglementaires et technologiques ont eu lieu et ont favorisé son essor. Ces caméras étaient installées pour prévenir des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés mais ne recourraient à aucune technologie innovante. Déjà à cette époque, les opposants de la vidéoprotection dénonçaient ces outils. Néanmoins, progressivement, le cadre réglementaire s'est élargi, laissant la place à l'utilisation de dispositifs de plus en plus performants.

La vidéoprotection algorithmique (VPA) est une technologie qui analyse les flux des caméras de vidéoprotection pour détecter certains événements prédéfinis. Cette technologie vise à intégrer des algorithmes d'analyse d'images dans les systèmes de vidéoprotection actuels afin d'augmenter la capacité de traitement des images. Concrètement, la vidéoprotection algorithmique permet de détecter automatiquement des comportements, des objets suspects, des mouvements de foule sans avoir recours à la surveillance biométrique. La mise en œuvre de ces traitements algorithmiques signale en temps réel la réalisation d'un événement que le système a pour mission de détecter. C'est l'expérimentation qui a été mise en place par la loi relative aux Jeux Olympiques 2024 afin de sécuriser les grandes manifestations ayant eu lieu pendant cette période. Aucune dérive n'a été démontrée à l'issue de cette expérimentation, dont l'avantage est

qu’elle préserve d’éventuelles discriminations et qu’elle reste objective. Ce que l’on peut en retenir, c’est qu’afin de produire réellement des effets, la vidéoprotection algorithmique a besoin de davantage de données.

C’est pourquoi la France doit, comme beaucoup de ses voisins déjà, généraliser la vidéoprotection algorithmique. En effet, la vidéoprotection algorithmique est déjà déployée en Belgique, au Royaume-Uni. La France ne peut pas rester à l’écart de cette évolution. Les Jeux Olympiques 2024 l’ont prouvé, nous avons les moyens d’utiliser une technologie au service de la sécurité des citoyens, sous contrôle humain, sans reconnaissance faciale généralisée et sans constitution de fichiers biométriques.

Selon un rapport de l’Assemblée nationale de 2023, on estime à environ 100 000 le nombre de caméras installées dans l’espace public. Si on comptabilise les caméras présentes dans des lieux privés ouverts au public comme des commerces ou des banques, ce nombre est encore plus important. Les caméras existantes sont déjà pourvues de la technologie algorithmique. En pratique, cette modalité est simplement désactivée lors de l’installation des caméras. Autrement dit, il n’existe ni frein technologique ni frein technique à la généralisation de la vidéoprotection algorithmique. Son déploiement ne générera pas de coûts exorbitants. Toutefois, il est nécessaire de développer des logiciels français et européens pour ne pas se laisser dépasser par l’innovation chinoise ou asiatique et garantir la souveraineté numérique de la France. Si la position française demeure si stricte sur ces technologies pourvues d’intelligence artificielle, la France n’aura aucune innovation dans ce domaine. C’est pourquoi nous devons collectivement créer ce cadre législatif pour permettre aux entreprises françaises et européennes de demeurer des acteurs incontournables de l’innovation de demain.

Par ailleurs, la vidéoprotection algorithmique participera à l’amélioration de l’efficacité des moyens dont disposent les forces de l’ordre pour accomplir leurs missions. Ces caméras constitueraient un soutien non négligeable dans l’assistance de leurs fonctions. En effet, on estime qu’une personne peut regarder six écrans pendant vingt minutes avant d’avoir besoin d’une pause. Les caméras permettraient d’avertir l’agent de la détection d’un événement prédéterminé et donc d’agir plus rapidement et efficacement. Cette technologie permet ainsi une baisse de la charge de travail tout en mettant le point sur ce qui est potentiellement problématique. Elle compense ainsi une capacité de concentration amoindrie après des heures consécutives sur des écrans.

Enfin, la vidéoprotection est un outil plébiscité par les citoyens et les maires, la sécurité s'imposant comme un thème incontournable du débat public. Ainsi, 72 % des Français estiment que le thème de la vidéoprotection et de l'intelligence artificielle doit être démocratiquement débattu. La vidéoprotection permet également aux élus de s'appuyer sur un outil fiable et efficace. Ainsi, les mairies financent un dispositif qui est mis à disposition des policiers et des gendarmes afin d'assurer la protection de chacun. Cette association doit se poursuivre et pouvoir être perfectionnée grâce à l'algorithme.

Cette proposition de loi vise à autoriser l'utilisation de traitements algorithmiques permettant d'identifier sur les images captées par des dispositifs de vidéoprotection, des événements révélant un risque pour la sécurité des personnes.

La présente proposition de loi reprend, dans son article unique, les dispositions adoptées dans le cadre des Jeux Olympiques 2024. Elle prévoit la généralisation de la vidéoprotection algorithmique dans des conditions strictement encadrées. Des événements prédéterminés préfigureront les modalités d'utilisation de la vidéoprotection algorithmique. Plusieurs événements pourront être retenus afin de protéger la population : bris de glace, animal errant, personnes au sol (malaise ou chute), explosion, départ de feu, accidents… Ces détections visent à protéger l'intégrité des personnes et l'ordre public. Ils seront déterminés par décret. Ainsi, lorsque la caméra identifiera ces événements, une alerte sera émise et permettra l'intervention humaine afin de déterminer l'opportunité à agir ou non. La vidéoprotection algorithmique en elle-même ne sera à l'origine d'aucune action : elle ne pourra fonder aucune décision individuelle ou aucun acte de poursuite. Le contrôle humain primera toujours. Ces caméras permettront une intervention plus rapide des forces de l'ordre mais aussi des services de secours et d'urgence.

L'emploi du traitement algorithmique est autorisé par le représentant de l'État dans le département ou par le Préfet de police à Paris qui s'assure de son caractère nécessaire et proportionnel. La décision doit être motivée et comprendre le périmètre géographique, les modalités d'information du public, qui pourra s'effectuer, comme en Belgique par un pictogramme, ainsi que le responsable du traitement.

Afin d'apporter les garanties nécessaires, il est précisé que cette généralisation n'implique aucune utilisation de la reconnaissance faciale. La proposition de loi rappelle également l'interdiction de tout rapprochement, de toute interconnexion ou mise en relation avec d'autres traitements de données à caractère personnel.

L’idée n’est pas de surpasser la protection des données ou les libertés individuelles, il s’agit au contraire de les imbriquer afin d’aboutir à une solution équilibrée dans l’intérêt général. Ainsi, cette proposition de loi respecte l’article 23 du règlement général sur la protection des données (RGPD) qui autorise, par voie législative, la limitation de ces droits par une mesure nécessaire et proportionnée. En effet, l’autorisation est délivrée par le préfet qui pourra apprécier avec vigilance, et en fonction des spécificités locales, de son opportunité.

Proposition de loi visant à généraliser la vidéoprotection algorithmique

Article unique

① I. – Après l'article L. 251-1 du code de la sécurité intérieure, il est inséré un article L. 251-1-1 ainsi rédigé :

② « *Art. L. 251-1-1*. – I. – Afin de protéger la sécurité des personnes et des biens et de prévenir toute atteinte à l'ordre public, les images collectées au moyen de systèmes de vidéoprotection autorisés en application de l'article L. 252-1 peuvent faire l'objet de traitements comprenant un système d'intelligence artificielle.

③ « Ces traitements sont strictement nécessaires et proportionnés et ont pour unique objet de détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler des risques d'atteinte à la sécurité des personnes et des biens et à l'ordre public et de les signaler en vue de la mise en œuvre des mesures nécessaires, par les services de la police et de la gendarmerie nationales, les services d'incendie et de secours, les services de police municipale et les services internes de sécurité de la société nationale SNCF et de la Régie autonome des transports parisiens.

④ « II. – Les traitements mentionnés au I sont régis 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

⑤ « III. – Les traitements mentionnés au I du présent article n'utilisent aucun système d'identification biométrique, ne traitent aucune donnée biométrique et ne mettent en œuvre aucune technique de reconnaissance faciale. Ils ne peuvent procéder à aucun rapprochement, interconnexion ou mise en relation automatisée avec d'autres traitements de données à caractère personnel.

⑥ « Ils procèdent exclusivement à un signalement d'attention, strictement limité à l'indication du ou des événements prédéterminés qu'ils ont été programmés pour détecter. Ils ne produisent aucun autre résultat et ne peuvent fonder, par eux-mêmes, aucune décision individuelle, ni aucun acte de poursuite.

⑦ « Ils demeurent en permanence sous le contrôle des personnes chargées de leur mise en œuvre.

⑧ « IV. – Le recours à un traitement mentionné au I est, par dérogation à l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, autorisé par un décret pris après avis de la Commission nationale de l'informatique et des libertés.

⑨ « Ce décret fixe les caractéristiques essentielles du traitement. Il indique notamment les événements prédéterminés que le traitement a pour objet de signaler et, le cas échéant, les spécificités des situations justifiant son emploi, les services mentionnés au second alinéa du I du présent article 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. Il désigne l'autorité chargée d'établir l'attestation de conformité mentionnée au dernier alinéa du V.

⑩ « Le décret est accompagné d'une analyse d'impact relative à la protection des données personnelles qui expose :

⑪ « 1° Le bénéfice escompté de l'emploi du traitement au service de la finalité mentionnée au I, au regard des événements prédéterminés donnant lieu à signalement par le système ;

⑫ « 2° L'ensemble des risques éventuellement créés par le système et les mesures envisagées afin de les minimiser et de les rendre acceptables au cours de son fonctionnement.

⑬ « V. – Le traitement satisfait aux caractéristiques suivantes :

⑭ « 1° Lorsque le système d'intelligence artificielle employé repose sur un apprentissage, des garanties sont apportées afin que les données d'apprentissage, de validation et de test choisies soient pertinentes, adéquates et représentatives et que leur traitement soit loyal, objectif et de nature à identifier et prévenir l'occurrence de biais et d'erreurs. Ces données demeurent accessibles et protégées tout au long du fonctionnement du traitement ;

⑮ « 2° Le traitement comporte un enregistrement automatique des évènements permettant d'assurer la traçabilité de son fonctionnement ;

⑯ « 3° Les modalités selon lesquelles, à tout instant, le traitement peut être arrêté sont précisées ;

⑰ « 4° Le traitement fait l'objet d'une phase de test conduite dans des conditions analogues à celles de son emploi tel qu'autorisé par le décret mentionné au IV. Cette phase de test est attestée par un rapport de validation.

⑱ « Lorsque le traitement est développé ou fourni par un tiers, celui-ci présente des garanties de compétences et de continuité et fournit une documentation technique complète.

⑲ « Le respect des caractéristiques définies au présent V fait l'objet d'une attestation de conformité établie par l'autorité administrative compétente. Cette attestation est publiée avant que le traitement soit mis à la disposition des services mentionnés au second alinéa du I qui demandent l'autorisation de l'utiliser dans les conditions prévues au VI.

⑳ « VI. – L'emploi du traitement est autorisé par le représentant de l'État dans le département ou à Paris, le préfet de police, qui s'assure de sa stricte nécessité et de son caractère proportionné pour garantir la sécurité publique et la prévention et la détection d'infractions pénales.

㉑ « La demande qui lui est adressée par un services mentionné au second alinéa du I comprend, en tant que de besoin, l'actualisation de l'analyse d'impact réalisée lors de l'autorisation délivrée par décret, adaptée aux circonstances du déploiement. Cette analyse actualisée est transmise à la Commission nationale de l'informatique et des libertés.

㉒ « La décision d'autorisation est publiée et motivée. Elle précise :

㉓ « 1° Le responsable du traitement et les services associés à sa mise en œuvre ;

㉔ « 2° Les motifs de cette mise en œuvre au regard de la finalité mentionnée au I ;

㉕ « 3° Le périmètre géographique concerné par cette mise en œuvre ;

㉖ « 4° Les modalités d'information du public, notamment sur ses droits ou, lorsque cette information entre en contradiction avec la finalité poursuivie, les motifs pour lesquels le responsable du traitement en est dispensé ;

㉗ « 5° La durée d'autorisation. Cette durée ne peut excéder cinq ans, renouvelable selon les mêmes modalités lorsque les conditions demeurent réunies.

㉘ « VII. – L'autorité responsable tient un registre des suites apportées aux signalements effectués par le traitement.

㉙ « Le représentant de l'État dans le département ou, à Paris, le préfet de police est tenu régulièrement informé des conditions dans lesquelles le traitement est mis en œuvre, en tient informée, en tant que de besoin, la Commission nationale de l'informatique et des libertés et peut suspendre l'autorisation délivrée par décret ou y mettre fin à tout moment, s'il constate que les conditions ayant justifié sa délivrance ne sont plus réunies.

⑳ « VIII. – Les images mentionnées au I dont la durée de conservation, prévue par les articles L. 252-5 et L. 242-4, n’est pas expirée peuvent être utilisées comme données d’apprentissage dans les conditions prévues au 1° du V du présent article. »

㉑ II. – La Commission nationale de l’informatique et des libertés est régulièrement informée des conditions de mise en œuvre du I. Le Gouvernement remet au Parlement, au plus tard six mois après l’entrée en vigueur de la présente loi, un rapport d’évaluation de sa mise en œuvre, dont le contenu est déterminé par décret en Conseil d’État après avis de la Commission nationale de l’informatique et des libertés. Ce décret détermine notamment les modalités de pilotage et d’évaluation pluridisciplinaire et objective de la mise en œuvre du I et les indicateurs utilisés par celle-ci. Il précise également les modalités selon lesquelles le public et les agents concernés sont informés et associés à l’évaluation.