



N° 2400

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 28 janvier 2026.

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

ANNEXE AU RAPPORT

PROPOSITION DE LOI

*visant à améliorer la protection des commerçants grâce à
l'usage d'outils numériques*

(*Première lecture*)

Article unique

- ① I. – (*Supprimé*)
- ② II (*nouveau*). – À titre expérimental et jusqu’au 31 décembre 2031, à la seule fin de prévenir le vol, les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l’article L. 251-2 du code de la sécurité intérieure dans les lieux et les établissements ouverts au public particulièrement exposés à des risques d’agression ou de vol peuvent faire l’objet de traitements algorithmiques. Ces traitements ont pour unique objet de détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler le risque de vol et de les signaler afin que soient mises en œuvre des mesures appropriées.
- ③ III (*nouveau*). – Les traitements mentionnés au II du présent article 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 de la loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés.
- ④ IV (*nouveau*). – Le public est préalablement informé, par tout moyen approprié, de l’emploi de traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l’article L. 252-1 du code de la sécurité intérieure.
- ⑤ V (*nouveau*). – Les traitements mentionnés au II 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, à aucune interconnexion ni à aucune 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 à 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 VI (*nouveau*). – Par dérogation à l'article 31 de la loi n° 78-17 du 6 janvier 1978 précitée, les modalités de recours à un traitement mentionné au II du présent article sont définies par un décret pris après avis de la Commission nationale de l'informatique et des libertés.
- ⑨ Ce décret détermine les caractéristiques essentielles du traitement. Il indique notamment les événements prédéterminés que le traitement a pour objet de signaler, le cas échéant les spécificités des situations justifiant son emploi, les lieux et les établissements mentionnés au même II susceptibles de le mettre en œuvre et les conditions d'habilitation et de formation des agents pouvant accéder aux signalements du traitement, laquelle porte notamment sur les enjeux liés aux libertés publiques et à l'éthique en lien avec le recours au traitement algorithmique des images. Il désigne l'autorité chargée d'établir l'attestation de conformité mentionnée au dernier alinéa du VII.
- ⑩ VII (*nouveau*). – Le traitement algorithmique doit satisfaire aux exigences suivantes, qui doivent pouvoir être vérifiées pendant toute la durée du fonctionnement du traitement :
- ⑪ 1° Lorsque le traitement algorithmique 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. Leur traitement doit être loyal et éthique, reposer sur des critères objectifs et permettre d'identifier et de prévenir l'occurrence de biais et d'erreurs. Ces données font l'objet de mesures de sécurisation appropriées ;
- ⑫ 2° Le traitement comporte un enregistrement automatique des signalements des événements prédéterminés détectés permettant d'assurer la traçabilité de son fonctionnement ;
- ⑬ 3° Le traitement permet des mesures de contrôle humain et un système de gestion des risques permettant de prévenir et de corriger la survenue de biais éventuels ou de mauvaises utilisations ;
- ⑭ 4° Les modalités selon lesquelles, à tout instant, le traitement peut être interrompu sont précisées ;
- ⑮ 5° Le traitement fait l'objet d'une phase de test conduite dans des conditions analogues à celles de son emploi autorisé par le décret mentionné au VI, attestée par un rapport de validation.

- ⑯ Lorsque le traitement est développé ou fourni par un tiers, celui-ci fournit une documentation technique complète et présente des garanties de compétence, de continuité, d'assistance et de contrôle humain en vue notamment de procéder à la correction d'erreurs ou de biais éventuels lors de sa mise en œuvre et de prévenir leur réitération.
- ⑰ Le respect des exigences énoncées au présent VII 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 II qui demandent l'autorisation de l'utiliser dans les conditions prévues au VIII.
- ⑱ VIII (*nouveau*). – Toute demande d'emploi du traitement doit être accompagnée d'une analyse d'impact relative à la protection des données personnelles, qui expose :
- ⑲ 1° Le bénéfice escompté de l'emploi du traitement au service de la finalité mentionnée au II, au regard des événements prédéterminés donnant lieu à un signalement par le système ;
- ⑳ 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.
- ㉑ Cette analyse réalisée lors de l'autorisation du traitement par décret est adressée à la Commission nationale de l'informatique et des libertés.
- ㉒ L'emploi du traitement est autorisé par le représentant de l'État dans le département ou, à Paris, par le préfet de police. Cette autorisation peut être accordée uniquement lorsque le recours au traitement est proportionné à la finalité poursuivie.
- ㉓ La décision d'autorisation est motivée et publiée. Elle précise :
- ㉔ a) Le responsable du traitement et les services associés à sa mise en œuvre ;
- ㉕ b) Le périmètre géographique concerné par la mise en œuvre du traitement dans les limites mentionnées au même II ;
- ㉖ c) Les modalités d'information du public, notamment sur ses droits ;
- ㉗ d) La durée de l'autorisation. Cette durée ne peut excéder cinq ans.

- (28) IX (*nouveau*). – Le responsable du traitement mentionné au a° du VIII tient un registre des suites apportées aux signalements effectués par le traitement ainsi que des personnes ayant accès aux signalements.
- (29) X (*nouveau*). – Les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l'article L. 252-1 du code de la sécurité intérieure ne peuvent pas être utilisées comme données d'apprentissage.
- (30) XI (*nouveau*). – La Commission nationale de l'informatique et des libertés contrôle l'application du présent article. À cette fin, elle peut faire usage des prérogatives prévues aux sections 2 et 3 du chapitre II du titre I^{er} de la loi n° 78-17 du 6 janvier 1978 précitée.
- (31) XII (*nouveau*). – La Commission nationale de l'informatique et des libertés est informée tous les ans des conditions de mise en œuvre de l'expérimentation mentionnée au II du présent article. Le Gouvernement remet au Parlement, au plus tard le 31 décembre 2029, un rapport d'évaluation de la mise en œuvre de l'expérimentation, établi par un comité d'évaluation présidé par une personnalité indépendante, dans des conditions précisées par un décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. Ce décret définit notamment les modalités de pilotage et d'évaluation pluridisciplinaire et objective de l'expérimentation et les indicateurs utilisés par celle-ci. L'évaluation associe, dans le respect du principe de parité entre les femmes et les hommes, deux députés et deux sénateurs, dont au moins un député et un sénateur appartenant à un groupe d'opposition, désignés respectivement par le président de l'Assemblée nationale et le président du Sénat. Le décret définit les conditions dans lesquelles l'évaluation associe également des personnalités qualifiées indépendantes nommées notamment par le président de la Commission nationale de l'informatique et des libertés et par le ministre de l'intérieur sur proposition du président du comité. Le rapport d'évaluation est également transmis à la Commission nationale de l'informatique et des libertés et rendu public sur internet au même moment.