N° 663

SÉNAT

SESSION ORDINAIRE DE 2022-2023

Enregistré à la Présidence du Sénat le 31 mai 2023

RAPPORT

FAIT

au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1)
sur la proposition de loi relative
à la **reconnaissance biométrique** *dans l'***espace public***,*

Par M. Philippe BAS,

Sénateur

(1) Cette commission est composée de : M. François-Noël Buffet*, président ;* Mmes Catherine Di Folco, Marie-Pierre de La Gontrie, MM. Christophe-André Frassa, Jérôme Durain, Marc-Philippe Daubresse, Philippe Bonnecarrère, Mme Nathalie Goulet, M. Thani Mohamed Soilihi, Mmes Cécile Cukierman, Maryse Carrère, MM. Alain Marc, Guy Benarroche*, vice-présidents ;* M. André Reichardt, Mmes Laurence Harribey, Muriel Jourda, Agnès Canayer*, secrétaires ;* Mme Éliane Assassi, MM. Philippe Bas, Arnaud de Belenet, Mmes Nadine Bellurot, Catherine Belrhiti, Esther Benbassa, MM. François Bonhomme, Hussein Bourgi, Mme Valérie Boyer, M. Mathieu Darnaud, Mmes Françoise Dumont, Jacqueline Eustache-Brinio, M. Pierre Frogier, Mme Françoise Gatel, MM. Loïc Hervé, Patrick Kanner, Éric Kerrouche, Jean-Yves Leconte, Henri Leroy, Stéphane Le Rudulier, Mme Brigitte Lherbier, MM. Didier Marie, Hervé Marseille, Mme Marie Mercier, MM. Alain Richard, Jean-Yves Roux, Jean-Pierre Sueur, Mme Lana Tetuanui, M. Dominique Théophile, Mmes Claudine Thomas, Dominique Vérien, M. Dany Wattebled.

Voir les numéros :

Sénat : **505** et **664** (2022-2023)

SOMMAIRE

Pages

L'ESSENTIEL

Réunie le 31 mai 2023 sous la présidence de **François-Noël Buffet**, la commission des lois a adopté **avec modifications**, sur le rapport de **Philippe Bas**, la proposition de loi n° 505 (2022-2023) *relative à la reconnaissance biométrique dans l'espace public*.

Déposée par Marc-Philippe Daubresse et Arnaud de Belenet ainsi que plusieurs de leurs collègues, la proposition de loi vise à **traduire les recommandations du rapport d'information, *La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance*, adopté à l'unanimité par la commission des lois le 10 mai 2022**[1].

Faisant le constat d'un **défaut d'encadrement juridique spécifique et de réflexion éthique collective**, la proposition de loi envisage la création d'un cadre juridique spécial pour la reconnaissance biométrique afin de réguler les pratiques et d'éviter le déploiement d'usages parfois contestables de cette technologie fortement intrusive. Est ainsi proposée la **définition de lignes rouges et de grands principes**, sur la base desquels une **autorisation de certains usages de reconnaissance biométrique** dans l'espace public pourrait être envisagée. L'autorisation de ces cas d'usage spécifiques est cependant proposée **à titre expérimental**, avec un régime de redevabilité rigoureux et un contrôle parlementaire élargi.

À l'initiative de son rapporteur, la commission a adopté plusieurs amendements, afin, tout en s'inscrivant dans la logique de la proposition de loi de **fixer en premier lieu des interdits**, de **renforcer les garanties applicables à l'ensemble des cas d'usage proposés** à titre expérimental, en les inscrivant dans un **cadre d'exigences renforcées** permettant de limiter leurs usages à des cas exceptionnels, circonscrits dans le temps et dans l'espace, et justifiés par un intérêt public supérieur.

---

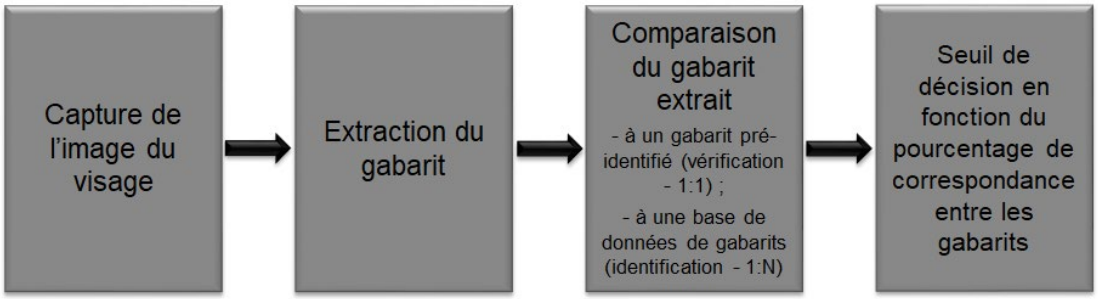
[1] *Rapport d'information n° 627 (2021-2022) fait, au nom de la commission des lois, par Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain. Ce rapport est consultable à l'adresse suivante : https://www.senat.fr/notice-rapport/2021/r21-627-notice.html.*

I. LA RECONNAISSANCE BIOMÉTRIQUE : UNE TECHNOLOGIE DONT L'ENCADREMENT JURIDIQUE FAIT L'OBJET DE NOMBREUSES RÉFLEXIONS

A. LA RECONNAISSANCE BIOMÉTRIQUE : UNE TECHNOLOGIE AUJOURD'HUI ENCADRÉE PAR LE DROIT DES DONNÉES PERSONNELLES

Les technologies de reconnaissance biométrique, qui incluent la reconnaissance faciale, regroupent l'ensemble des procédés automatisés permettant de reconnaître un individu à partir de la quantification de ses caractéristiques physiques, physiologiques ou comportementales[1].

La reconnaissance des personnes à partir de leurs données biométriques s'effectue en deux étapes : les données de la personne sont d'abord **captées et transformées en un modèle informatique dénommé gabarit**, puis ce gabarit est comparé, grâce à **l'intelligence artificielle**, avec un ou plusieurs autres gabarits afin de vérifier qu'il s'agit bien d'une seule et même personne ou de lui attribuer une identité. On parle dans le premier cas **d'authentification** et dans le second **d'identification**. Ainsi, pour la reconnaissance faciale, le processus est le suivant :



Source : Commission des lois du Sénat – Rapport sur la reconnaissance biométrique dans l'espace public

Les cas d'usage de ces technologies sont **potentiellement illimités**. Ainsi, sans que cette liste soit exhaustive, la reconnaissance biométrique peut permettre de contrôler l'accès et le parcours des personnes pour les évènements ou locaux sensibles, d'assurer la sécurité et le bon déroulement d'évènements à forte affluence ou d'aider à la gestion des flux dans les lieux et environnements nécessitant une forte sécurisation.

[1] *L'article 4 du règlement général sur la protection des données (RGPD) définit ainsi les données biométriques comme* « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ».

Or, les techniques de reconnaissance biométrique ne font pas l'objet d'un encadrement *ad hoc*. Elles sont actuellement **exclusivement régies par le droit des données à caractère personnel**. S'agissant de données « sensibles » au sens du règlement général sur la protection des données (RGPD), les données biométriques font l'objet d'une **interdiction de traitement**. Sur la base du RGPD, ces traitements ne peuvent être mis en œuvre que par exception dans certains cas particuliers : avec le **consentement exprès des personnes**, pour protéger leurs **intérêts vitaux** ou sur la base d'un **intérêt public important**. Sur la base de la directive « Police-justice », ces traitements ne peuvent être réalisés par les autorités publiques compétentes qu'en cas de **nécessité absolue** et sous réserve de **garanties appropriées** pour les droits et libertés de la personne concernée.

Ainsi, en France, **les usages pérennes de la reconnaissance biométrique à distance dans les espaces accessibles au public sont extrêmement limités**. Il s'agit pour l'essentiel du dispositif de rapprochement par photographies opéré dans le **Traitement des antécédents judiciaires** (TAJ) et du système Parafe[1] permettant une authentification sur la base des données contenues dans le passeport lors des **passages aux frontières extérieures**. Plusieurs expérimentations ont par ailleurs été menées, par la Ville de Nice ou Aéroports de Paris notamment, mais aucune d'entre elles n'a pour l'instant été pérennisée.

B. UN DÉVELOPPEMENT RAPIDE DE CES TECHNOLOGIES QUI APPELLE UN ENCADREMENT SPÉCIFIQUE

Le développement rapide des technologies de reconnaissance biométrique, grâce aux algorithmes d'apprentissage, **polarise l'opinion publique** entre ceux qui, compte tenu de leur caractère par nature attentatoire aux libertés, **plaident pour un moratoire et ceux qui mettent en exergue leurs importants bénéfices potentiels**.

L'encadrement par le droit des données à caractère personnel ne paraît cependant pas parfaitement adapté. Ses brèches laissent se développer des usages, notamment par les acteurs privés, en-dehors de toute **réflexion collective** sur la spécificité des traitements de données biométriques.

Cette réflexion est pourtant appelée de leurs vœux par plusieurs acteurs, qu'il s'agisse de la Commission nationale de l'informatique et des libertés (CNIL) qui recommandait la fixation de lignes rouges claires[2], du

---

[1] *Passage rapide aux frontières extérieures.*

[2] *Reconnaissance faciale : pour un débat à la hauteur des enjeux, Commission nationale de l'informatique et des libertés (CNIL), 15 novembre 2019. Le rapport est consultable à l'adresse suivante : https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux.*

Conseil de l'Europe[1], du Défenseur des droits[2] ou encore de la Commission nationale consultative des droits de l'homme[3].

Outre celui dont est issue la proposition de loi, trois rapports parlementaires traitent également du sujet :

- note n° 14, *La reconnaissance faciale* (juillet 2019) de Didier Baichère, député, au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST)[4] ;

- rapport au Premier ministre, *Pour un usage responsable et acceptable par la société des technologies de sécurité*, par Jean-Michel Mis, député, remis en septembre 2021[5] ;

- rapport d'information n° 1089 *sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité*, de Philippe Gosselin et Philippe Latombe, députés, déposé le 12 avril 2023[6].

Tous s'accordent sur la nécessité d'un encadrement spécifique des technologies de reconnaissance biométrique afin d'éviter le développement d'usages considérés comme illégitimes ou trop attentatoires aux libertés et aux droits fondamentaux.

C. LE RÈGLEMENT EUROPÉEN SUR L'INTELLIGENCE ARTIFICIELLE : UNE TEMPORALITÉ INADAPTÉE QUI EXIGE DE L'ANTICIPER

Le règlement européen sur l'intelligence artificielle actuellement en cours de discussion s'inscrit dans cette réflexion et a pour ambition d'encadrer le développement des systèmes de reconnaissance biométrique. Le projet présenté par la Commission européenne prévoit notamment une interdiction de la notation sociale basée sur les données biométriques ainsi qu'une interdiction des systèmes d'identification biométrique en temps réel dans les espaces publics à des fins répressives. Il autoriserait toutefois l'utilisation de ces systèmes en temps réel à des fins répressives dans trois cas : pour la recherche de victimes potentielles d'actes criminels, pour faire

---

[1] *Lignes directrices sur la reconnaissance faciale, Conseil de l'Europe, 28 janvier 2021. Le rapport est consultable à l'adresse suivante : https://www.dalloz-actualite.fr/document/conseil-de-l-europe-lignes-directrices-sur-reconnaissance-faciale-28-janv-2021.*

[2] *Technologies biométriques : l'impératif respect des droits fondamentaux, Défenseur des droits, 19 juillet 2021. Le rapport est consultable à l'adresse suivante : https://www.defenseurdesdroits.fr/fr/rapports/2021/07/rapport-technologies-biometriques-limperatif-respect-des-droits-fondamentaux.*

[3] *Intelligence artificielle et droits humains : Pour l'élaboration d'un cadre juridique ambitieux, Commission nationale consultative des droits de l'homme, 7 avril 2022.*
Le rapport est consultable à l'adresse suivante : https://www.cncdh.fr/sites/default/files/a_-_2022_-_6_-_intelligence_artificielle_et_droits_fondamentaux_avril_2022.pdf.

[4] *La note est consultable à l'adresse suivante : https://www.senat.fr/opecst/notes.html.*

[5] *Le rapport est consultable à l'adresse suivante : https://www.vie-publique.fr/rapport/281424-pour-un-usage-responsable-et-acceptable-par-la-societe-des-technologies.*

[6] *Le rapport est consultable à l'adresse suivante : https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information#.*

face à certaines menaces pour la vie ou la sécurité des personnes telles que les attaques terroristes, et pour détecter, localiser, identifier ou engager des poursuites à l'encontre des auteurs de certaines infractions passibles d'une peine de prison d'au moins trois ans[1].

Présenté par la Commission européenne en avril 2021, ce texte pourrait être adopté définitivement au cours de l'année 2023. Son entrée en vigueur n'interviendrait cependant pas avant l'année 2025.

Au vu du développement rapide des technologies liées à l'intelligence artificielle, et plus particulièrement de celles traitant des données biométriques, il est cependant nécessaire de fixer dès maintenant des principes directeurs encadrant leur développement et leurs usages.

II. LA PROPOSITION DE LOI : UN PREMIER ENCADREMENT DE L'USAGE DES TECHNOLOGIES BIOMÉTRIQUES DANS L'ESPACE PUBLIC

A. LA TRADUCTION LÉGISLATIVE DU RAPPORT D'INFORMATION DE LA COMMISSION DES LOIS SUR LA RECONNAISSANCE BIOMÉTRIQUE

Parallèlement aux discussions au niveau européen, les rapporteurs de la mission d'information sur la reconnaissance faciale ont proposé **30 recommandations concernant la reconnaissance biométrique dans l'espace public, avec pour objectif d'écarter le risque d'une société de surveillance**.

Face à un **défaut d'encadrement juridique spécifique et de réflexion éthique collective**, le rapport envisageait la création d'un cadre juridique permettant de réguler les pratiques et d'éviter le déploiement d'usages parfois contestables de cette technique fortement intrusive.

Trois axes étaient proposés :

- la définition collective d'un cadre comprenant des lignes rouges, une méthodologie et un régime de redevabilité ;

- la définition des modalités d'usage de la reconnaissance biométrique suivant une logique de cas d'usage ;

- le renforcement de la souveraineté technologique de la France et de l'Europe.

[1] *Il s'agit des infractions visées dans la décision-cadre du Conseil du 13 juin 2022 relative au mandat d'arrêt européen, parmi lesquelles figurent les actes de terrorisme, la traite d'êtres humains, la corruption, les homicides volontaires, les viols* etc.

Ainsi, les rapporteurs avaient pour objectif la définition de lignes rouges et de grands principes clairs, sur la base desquels une autorisation de certains usages de reconnaissance biométrique dans l'espace public pouvait être discutée par le Parlement. Ils concluaient que l'autorisation de ces cas d'usage spécifiques devrait cependant se faire à titre expérimental, avec un régime de redevabilité fort et un contrôle parlementaire élargi.

La proposition de loi relative à la reconnaissance biométrique dans l'espace public, déposée le 5 avril 2023 par MM. Daubresse et de Belenet, vise à **traduire les recommandations du rapport afin que le Parlement puisse se saisir du sujet**.

B. UN RAISONNEMENT PAR CAS D'USAGE, EN FONCTION DES FINALITÉS POURSUIVIES ET DES RISQUES ENCOURUS

La proposition de loi prévoit, dans son **article premier**, de **fixer dans la loi les lignes rouges définies par le rapport** : seraient ainsi interdites toute catégorisation et notation des personnes physiques sur la base de leurs données biométriques, ainsi que, de manière générale, la reconnaissance des personnes physiques sur la base de leurs données biométriques en temps réel dans l'espace public et dans les espaces accessibles au public.

La proposition de loi définit ensuite, dans ses articles 2 à 6, les **cas d'usage de technologies de reconnaissance biométriques qui pourraient, par dérogation à cet article 1er, être expérimentés**.

Un raisonnement par cas d'usage,
en fonction des finalités poursuivies

Trois distinctions doivent ici être rappelées, car elles conditionnent les risques pour les libertés des différents cas d'usage de la reconnaissance biométrique :

Authentification et identification : l'authentification consiste à vérifier qu'une personne est bien celle qu'elle prétend être, le système comparant un gabarit biométrique préenregistré avec celui extrait de la personne concernée au moment du besoin d'identification, afin de vérifier que les deux gabarits correspondent. Il s'agit donc d'une comparaison « 1 contre 1 ». L'identification vise quant à elle à retrouver une donnée biométrique parmi celles extraites de plusieurs personnes au sein d'une base de données. La comparaison effectuée est une comparaison « 1 contre N », où un gabarit est confronté à une base de données de gabarits. L'authentification est donc par nature moins intrusive que l'identification ;

Exploitation en temps réel et exploitation *a posteriori* : dans le cadre d'une exploitation en temps réel, le processus permet un usage immédiat des résultats pour procéder à un contrôle de la personne concernée ; lors d'une exploitation *a posteriori*, les recherches se font généralement sur des enregistrements ;

Police administrative et police judiciaire : le cadre dans lequel est effectuée la recherche conditionne les contrôles réalisés et l'autorité qui les met en œuvre.

Les risques potentiels des systèmes de reconnaissance biométrique :

La Commission nationale de l'informatique et des libertés[1] liste cinq risques que peuvent engendrer les utilisations de technologies de reconnaissance biométrique, de chaque type d'usage dépendant le degré de risque encouru :

- un risque pour la vie privée des personnes, avec une atteinte au principe d'anonymat sur la voie publique ;

- des risques d'erreurs sur l'identification des personnes ;

- des risques de biais discriminatoires en fonction de la manière dont les systèmes ont été entraînés ;

- un risque d'inhibition dans l'exercice des droits ou des libertés fondamentales ;

- un risque de sécurité informatique, en particulier si les bases de données biométriques sont centralisées.

Ainsi, l'**article 2** prévoit en premier lieu la **possibilité**, tout en conservant le principe d'une interdiction de l'usage de la biométrie pour l'accès à certains lieux sans alternative non biométrique, **de permettre à titre expérimental d'organiser par exception un contrôle exclusivement biométrique de l'accès à tout ou partie d'un grand évènement** qui, par son ampleur ou par ses circonstances, est particulièrement exposé à des risques d'actes de terrorisme ou à des risques d'atteinte grave à la sécurité des personnes et pour lequel l'organisateur a démontré un impératif particulier d'assurer un haut niveau de fiabilité de l'identification des personnes.

Les articles 3 à 6 ouvrent la possibilité d'identifier les personnes sur la base de leurs caractéristiques biométriques.

Les **articles 3 et 4**, qui institueraient à titre expérimental des **possibilités d'utilisation des techniques d'identification biométrique dans l'espace public** ***a posteriori***, concernent respectivement le **cadre judiciaire**, pour la recherche d'auteurs ou de victimes potentielles de certaines infractions, et le **cadre administratif** avec la création d'une nouvelle technique de renseignement.

Les **articles 5 et 6** prévoient le **recours à titre expérimental à ces technologies en temps réel**. L'article 5 vise à permettre un recours ciblé et limité dans le temps dans un **cadre administratif**, tandis que l'article 6 a trait à l'usage de cette technique dans un **cadre judiciaire**.

Les articles 7 et 8 définissent le cadre dans lequel ces expérimentations se dérouleraient.

[1] *Audition par la commission de Louis Dutheillet de Lamothe, Secrétaire général de la CNIL (23 mai 2023).*

L'**article 7** prévoit tout d'abord la **mise en place d'un régime de contrôle renforcé** : un rapport annuel serait remis par le Gouvernement au Parlement, l'Assemblée nationale et le Sénat seraient informés en temps réel des mesures prises dans un cadre administratif, et le Parlement pourrait requérir toute information complémentaire du Gouvernement dans le cadre de l'évaluation de ces mesures.

L'**article 8** indique quant à lui que les mesures définies aux articles 2 à 6 sont prises **à titre expérimental et applicables pour une durée de trois ans** à compter de la promulgation de la loi. Il prévoit également qu'un **comité scientifique et éthique** serait chargé d'évaluer régulièrement l'application de ces mesures et ses rapports, rendus publics, seraient transmis au Parlement. Enfin, un **rapport final d'évaluation** serait réalisé par le Gouvernement, appréciant l'application de ces mesures et l'opportunité de les pérenniser ou de les modifier, notamment au vu de potentielles évolutions du droit de l'Union européenne en la matière.

Enfin, l'**article 9** assure l'application outre-mer de la proposition de loi.

III. LA POSITION DE LA COMMISSION DES LOIS : UNE TECHNOLOGIE DONT LES USAGES EXCEPTIONNELS DOIVENT ÊTRE FORTEMENT ENCADRÉS

A. UNE PROPOSITION DE LOI QUI OUVRE UTILEMENT LE DÉBAT SUR L'USAGE DE LA RECONNAISSANCE BIOMÉTRIQUE DANS L'ESPACE PUBLIC

En réponse à l'appel de la Commission nationale de l'informatique et des libertés (CNIL), dès 2019, d'un débat public sur le sujet, **la proposition de loi a le mérite d'engager le Parlement à se positionner sur l'usage des technologies de reconnaissance biométriques**, du cadre adapté et des garanties nécessaires au cours d'un débat spécifique sur le sujet.

Un amendement avait en effet été déposé par Marc-Philippe Daubresse, premier signataire de la proposition de loi, à l'occasion de la discussion de la loi n° 2023-380 du 19 mai 2023 *relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions*. Cet amendement avait cependant été retiré avant sa discussion, **un consensus s'étant formé sur la nécessité de débattre de la reconnaissance biométrique dans l'espace public dans un cadre exclusif**, plutôt que d'aborder cette thématique au détour d'une discussion, plus large, sur la sécurisation des jeux Olympiques et Paralympiques. Si le déroulement de cet évènement sportif soulève en effet des interrogations, il est en effet peu plausible que les technologies biométriques visées puissent être pleinement opérationnelles à cette date.

La discussion de la proposition de loi intervient donc à un moment où la plupart des acteurs institutionnels ont déjà eu l'occasion d'étudier le sujet et d'exprimer leurs positions, mêlant lignes rouges, garanties

nécessaires et usages pouvant avoir un intérêt opérationnel. Les dispositifs proposés ont donc vocation à être ajustés au cours de la discussion parlementaire afin de **définir le cadre le plus pertinent pour assurer la protection des droits et libertés de nos concitoyens ainsi que leur sécurité**. C'est ce à quoi s'est attachée la commission des lois.

B. UN RENFORCEMENT NÉCESSAIRE DES LIGNES ROUGES ET GARANTIES ENTOURANT LE DÉPLOIEMENT DE CES TRAITEMENTS POUR FAIRE OBSTACLE À UNE SOCIÉTÉ DE SURVEILLANCE

La commission a en premier lieu souhaité renforcer les lignes rouges et fixer les limites aux utilisations à venir des technologies de reconnaissance biométrique, en les regroupant au sein d'un même premier chapitre de la proposition de loi.

Elle a ainsi modifié la rédaction de l'**article 1er** afin de renforcer l'encadrement des technologies de reconnaissance biométrique tout en ciblant les systèmes les plus sensibles en termes de libertés. À cet effet, la commission a précisé que seuls **les systèmes d'identification biométrique réalisés à distance et sans le consentement des personnes** seraient interdits, ces derniers présentant le plus de risques au regard des droits et libertés. La commission a ensuite fixé **une ligne rouge supplémentaire en interdisant l'identification biométrique *a posteriori***, qu'elle juge tout autant intrusive que l'identification biométrique en temps réel. Elle a aussi ajouté que **les systèmes d'identification biométrique dans l'espace public et dans les espaces accessibles au public ne pourraient être autorisés par voie réglementaire**, même en cas de nécessité absolue : une intervention du législateur sera toujours nécessaire. La commission a ensuite précisé qu'il ne pourrait être dérogé à l'interdiction des systèmes d'identification biométrique dans l'espace public et dans les espaces accessibles au public en dehors des exceptions prévues par la présente loi, de façon à **éviter tout glissement vers une société de surveillance**. Le recours à ces dérogations devrait obéir aux **principes de nécessité et de proportionnalité**.

Par coordination avec l'interdiction de la reconnaissance biométrique *a posteriori* introduite par la commission à l'article 1er, la commission a introduit un **article 4 A** qui vise à permettre aux **services de la police nationale et de la gendarmerie nationale de continuer à recourir *a posteriori* à des dispositifs de reconnaissance biométrique au sein des fichiers d'antécédents judiciaires** dans le cadre de la recherche des auteurs d'infractions à la loi pénale. Autorisée par des dispositions réglementaires depuis 2012, cette possibilité permet aux forces de l'ordre d'utiliser la reconnaissance biométrique pour identifier des personnes fichées dans le Traitement des antécédents judiciaires (TAJ) et constitue un dispositif utile, comme souligné par le Conseil d'État[1].

[1] *CE, 26 avril 2022, n° 442364*

Elle a également, par l'adoption d'un **article additionnel 1er *bis*, défini le cadre expérimental et le régime de contrôle des articles de la proposition de loi**. C'est ainsi que l'ensemble des cas d'usage de la reconnaissance biométrique dans l'espace public et dans les espaces accessibles au public ne serait autorisé qu'**à titre expérimental, pour une durée de trois ans**, pour des finalités précises. Conformément à l'article 5 de la proposition de règlement du Parlement européen et du Conseil relatif à l'intelligence artificielle, ces usages répondraient à une **procédure d'autorisation spécifique**, des magistrats pour les usages judiciaires, et de la commission nationale de contrôle des techniques de renseignement (CNCTR) pour les usages administratifs. Cette expérimentation serait placée sous le contrôle du Parlement, qui pourrait s'adjoindre l'aide de différents experts afin d'assurer un suivi en temps réel et une évaluation forte des mesures prises ou mises en œuvre.

La commission a également inséré un **article 1er *ter*** afin de définir les **conditions auxquelles devraient répondre les traitements de données biométriques développés** dans le cadre des usages proposés à titre expérimental par la proposition de loi. Ainsi, elle a précisé que l'objet de ces traitements sera de **faire apparaître le degré de probabilité** de l'identité d'une personne dont il s'agit de vérifier la présence et que seul apparaîtra aux yeux de l'agent le résultat final, afin de constituer un **outil d'aide à la décision**. Ces traitements ne pourront procéder à aucun rapprochement, interconnexion ou mise en relation automatisés avec d'autres traitements de données à caractère personnel et **demeureront en permanence sous le contrôle des agents chargés de leur mise en œuvre**. Ces agents devront être **individuellement formés et habilités**. La commission a également prévu que les traitements devront être **développés par l'État ou sous son contrôle**, avant d'être **individuellement autorisés par décret en Conseil d'État** pris après avis de la Commission nationale de l'informatique et des libertés ou, le cas échéant, de la Commission nationale de contrôle des techniques de renseignement.

La commission a fait le choix d'appliquer ces multiples et solides garanties à l'ensemble des cas d'usage dont l'expérimentation est proposée. Il s'agit **d'un socle minimal à respecter pour l'utilisation de la reconnaissance biométrique, qu'elle a complété par l'adjonction de garanties supplémentaires pour les cas d'usage les plus problématiques** (*voir infra*).

La commission a inséré un **article 1er *quater*** visant, d'une part, à **consacrer la CNIL en tant que « chef de file » de la régulation de l'intelligence artificielle** et, d'autre part, à **fluidifier la coopération entre les différentes autorités compétentes**. Suivant les recommandations formulées dans le rapport d'information précité des députés Philippe Gosselin et Philippe Latombe, elle a ainsi intégré deux membres supplémentaires au collège de la CNIL : le président de l'Autorité de

régulation de la communication audiovisuelle et numérique ainsi que le président de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP). Par réciprocité, elle a prévu une représentation de la CNIL au sein de ces deux autorités.

C. RÉSERVER LE RECOURS AUX TECHNOLOGIES DE RECONNAISSANCE BIOMÉTRIQUES DANS LE CADRE DES ENQUÊTES JUDICIAIRES AUX INFRACTIONS LES PLUS GRAVES

S'agissant des usages judiciaires, **la commission a estimé que le recours à la reconnaissance biométrique ne devait être expérimenté que dans le cadre des enquêtes et instructions portant sur des infractions d'une exceptionnelle gravité**. En conséquence, **elle a fortement resserré le périmètre de l'expérimentation**, que ce soit :

- dans le cadre de la reconnaissance biométrique *a posteriori* : elle ne pourrait être utilisée que dans le cadre des enquêtes et investigations portant sur des faits de terrorisme, de trafic d'armes, d'atteintes aux personnes punies d'au moins cinq ans de prison ou des procédures des recherche de personnes disparues ou en fuite (**article 3**) ;

- dans le cadre de la reconnaissance biométrique en temps réel : la commission a considéré que cet usage ne pouvait concerner que les cas les plus extrêmes. Suivant les recommandations des députés Philippe Gosselin et Philippe Latombe, elle n'en a autorisé l'expérimentation que pour les enquêtes et investigations portant sur des faits de terrorisme, d'atteintes aux intérêts fondamentaux de la nation, sur des infractions relatives à la criminalité organisée relevant de la compétence de la juridiction nationale chargée de la lutte contre la criminalité organisée ou sur des disparitions de personnes mineures (**article 6**).

La commission a également entendu **renforcer au maximum le régime de contrôle de cette expérimentation ainsi que les garanties associées**. Elle a ainsi soumis l'usage *a posteriori* à une autorisation expresse de l'autorité judiciaire, qui devra préciser l'origine et la nature des données exploitées. Elle a également tiré les conséquences de la jurisprudence du Conseil constitutionnel en la matière, en **interdisant toute mise en commun dans un traitement général des données biométriques exploitées** dans les différentes enquêtes et investigations concernées. S'agissant de l'usage en temps réel, elle a **précisé la finalité du dispositif, a conditionné sa mise en œuvre au respect d'un strict principe de subsidiarité et l'a réservé aux seuls officiers de police judiciaire habilités**. Elle a également confié au **seul juge des libertés et de la détention le soin de procéder au renouvellement de l'autorisation** de recourir aux traitements biométriques en question.

D. INSCRIRE LES USAGES ADMINISTRATIFS DE CES TECHNOLOGIES DANS LE CADRE ROBUSTE D'UNE AUTORISATION AU PLUS HAUT NIVEAU AVEC UN CONTRÔLE D'UNE AUTORITÉ ADMINISTRATIVE INDÉPENDANTE

S'agissant des usages administratifs, la commission a en premier lieu recentré l'article 2, qui prévoit la possibilité, pour les organisateurs de grands événements particulièrement exposés à des risques d'actes de terrorisme ou à des risques d'atteinte grave à la sécurité des personnes, de mettre en place **un système d'authentification biométrique sans consentement** pour l'accès de certaines personnes à tout ou partie des zones accueillant le grand événement. À cet effet, la commission a restreint le champ de l'expérimentation en prévoyant que **le système d'authentification biométrique obligatoire ne pourrait concerner les habitants des zones concernées**. Elle a également précisé que **seul l'État pourrait mettre en œuvre les traitements de données biométriques** utilisés dans le cadre de cette expérimentation. La commission a par ailleurs souhaité ajouter de nouvelles garanties et a instauré **une information préalable obligatoire** des personnes soumises au dispositif d'authentification biométrique sans consentement. Enfin, elle a prévu que l'organisateur d'un grand événement devra démontrer qu'un **haut niveau de fiabilité de l'identification des personnes est requis** pour accéder aux zones faisant l'objet d'une restriction de circulation et d'accès, et pas seulement pour accéder au grand événement.

La commission a ensuite souhaité **inscrire l'identification des personnes sur la base de leurs données biométriques en matière administrative dans le cadre robuste prévu par la loi sur le renseignement,** que cette identification soit réalisée *a posteriori* ou en temps réel.

À l'**article 4**, qui envisageait la **création d'une nouvelle technique de renseignement permettant aux services du premier cercle d'utiliser des logiciels de reconnaissance biométrique *a posteriori***, la commission a ainsi souhaité **clarifier les procédures applicables en fonction de l'origine des données traitées**. Ainsi, s'agissant des renseignements collectés à la suite de la mise en œuvre de techniques de renseignement, elle a prévu que le recours à ce type de logiciels pour en faciliter l'exploitation soit précisé dans la demande d'autorisation de la technique elle-même, afin d'éviter une double demande d'autorisation pour la collecte puis pour l'exploitation des données. La commission a également **recentré la création de cette nouvelle technique de renseignement sur la possibilité, ouverte par l'article** aux services, d'exploiter *a posteriori* les **images de vidéoprotection** par ce type de logiciels après autorisation du Premier ministre donné après avis de la commission nationale de contrôle des techniques de renseignement (CNCTR). Conformément aux finalités de la vidéoprotection, **cette nouvelle possibilité ne serait ouverte que pour la lutte contre le terrorisme**.

L'**article 5** proposait quant à lui de créer un cadre permettant le recours ciblé et limité dans le temps à des systèmes de reconnaissance biométrique **en temps réel, dans un cadre administratif**. Malgré les

nombreuses garanties envisagées, il **souffrait de plusieurs faiblesses** : il réservait d'abord cet usage aux officiers de police judiciaire, alors qu'il s'agissait d'une procédure s'inscrivant dans un cadre administratif. Il attribuait ensuite un pouvoir étendu d'autorisation aux préfets, qui auraient été désarmés pour apprécier la pertinence de recours à ces technologies faute de disposer des éléments suffisants pour évaluer eux-mêmes la situation. Les décisions des préfets étaient en troisième lieu soumises au contrôle des tribunaux administratifs, devant lequel le contradictoire doit entièrement être respecté, ce qui aurait été à l'encontre du secret parfois nécessaire à la protection de la sécurité nationale.

La commission a en conséquence profondément remanié l'article 5, en **inscrivant clairement la procédure dans un cadre administratif et en l'assortissant des garanties maximales**. Pour ce faire, elle a **réservé l'utilisation** de la reconnaissance biométriques en temps réel dans l'espace public en matière administrative **aux services de renseignement du premier cercle en charge de la sécurité intérieure, à la seule fin d'assurer la prévention du terrorisme**. Elle a également choisi d'appliquer à cette utilisation le régime robuste éprouvé depuis maintenant huit ans d'autorisation du Premier ministre après avis de la commission nationale de contrôle des techniques de renseignement (CNCTR), permettant que le déploiement de ces technologies soit **placé en permanence sous le contrôle de la CNCTR et du Conseil d'État**. Enfin, la commission a précisé que le déploiement de ces technologies devait être **strictement subsidiaire**.

*

* *

La commission a adopté la proposition de loi ainsi modifiée.

EXAMEN DES ARTICLES

CHAPITRE IER
FAIRE OBSTACLE À UNE SOCIÉTÉ DE SURVEILLANCE
(Division nouvelle)

Afin d'assurer la clarté du texte, la commission a créé une nouvelle division regroupant les articles de la proposition de loi consacrés aux dispositions s'appliquant aux différents articles de la proposition de loi (**amendement COM-3** du rapporteur).

Article 1er
Fixation de lignes rouges destinées à encadrer l'utilisation de la reconnaissance biométrique

L'article 1er tend à définir des lignes rouges afin de poser des interdits quant à l'utilisation des systèmes de reconnaissance biométrique, et ainsi écarter le risque d'une société de surveillance.

Souscrivant pleinement à l'encadrement des modalités d'utilisation de cette technologie, la commission a adopté cet article en renforçant son dispositif.

1. La reconnaissance biométrique emporte des risques importants pour les libertés publiques

Comme l'a rappelé Louis Dutheillet de Lamothe, secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL) durant son audition[1], l'utilisation des dispositifs de reconnaissance biométrique crée de nombreux risques pour les libertés publiques.

D'abord, la reconnaissance biométrique est susceptible de porter atteinte au **droit au respect de la vie privée** et pourrait conduire à la mise en place d'une **société de surveillance**, en ce qu'elle permet potentiellement de surveiller le comportement et les déplacements des personnes dans l'espace public en permanence.

Les **erreurs** commises par les technologies de reconnaissance biométrique peuvent aussi nuire au respect des libertés fondamentales. Une erreur en matière judiciaire pourrait par exemple entraîner l'interpellation d'un mauvais suspect, dans le cas où il n'y aurait pas de contrôle humain. Ces technologies sont aussi sujettes à des **biais discriminatoires**, ce qui peut conduire à un taux d'erreur plus élevé pour certaines catégories de population.

---

[1] *Cette audition est visible sur le site du Sénat : http://videos.senat.fr/video.3888164_646ac23166e5d.reconnaissance-biometrique--audition-de-la-cnil*

Enfin, l'utilisation de la reconnaissance biométrique peut faire apparaître une **inhibition dans l'exercice de certaines libertés fondamentales**. Si la reconnaissance biométrique se déployait sans cadre, les citoyens pourraient par exemple renoncer à l'exercice de leur droit de manifester par crainte d'un usage détourné de cette technologie.

2. Face à ces risques, des lignes rouges doivent être définies afin d'encadrer l'utilisation des systèmes de reconnaissance biométrique

Les systèmes de reconnaissance biométrique ne font pas l'objet d'un encadrement *ad hoc et* sont à l'heure actuelle régis exclusivement par **le droit des données à caractère personnel**.

Le règlement général sur la protection des données[1] (RGPD) interdit à cet égard le traitement des données biométriques, celles-ci constituant des données sensibles, tout comme les données relatives à la santé ou aux opinions politiques. Par exception, ces traitements sont autorisés par le RGPD avec **le consentement exprès des personnes**, pour **protéger leurs intérêts vitaux** ou sur la base d'un **intérêt public important**. La directive « *Police-Justice*[2] » autorise quant à elle ces traitements en cas de **nécessité absolue** et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée**.**

Face aux risques que comportent les technologies de reconnaissance biométrique, il apparaît toutefois nécessaire de **fixer des lignes rouges spécifiques pour encadrer leur utilisation et éviter la mise en place d'une société de surveillance**, comme recommandé par la Commission nationale de l'informatique et des libertés (CNIL) dans son rapport de 2019[3] ainsi que par les sénateurs Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain dans leur rapport d'information de 2022[4].

---

[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] *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.

[3] « Reconnaissance faciale : pour un débat à la hauteurs des enjeux », *CNIL, 15 novembre 2019.*

[4] La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance, *rapport d'information n° 627 (2021-2022) de Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, déposé le 10 mai 2022, p.81. Ce rapport est consultable à l'adresse suivante : https://www.senat.fr/notice-rapport/2021/r21-627-notice.html.*

Reprenant cette recommandation, l'article 1er de la proposition de loi complèterait l'article 95 de la loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés* pour fixer plusieurs lignes rouges afin d'encadrer l'utilisation des systèmes de reconnaissance biométrique.

L'article 1er interdirait ainsi :

- la catégorisation des personnes physiques sur la base de leurs données biométriques ;

- la notation des personnes physiques sur la base de leurs données biométriques. La notation sociale est définie par la Commission européenne comme « *étudiant ou classant la fiabilité des personnes physiques en fonction de leur comportement social dans plusieurs contextes ou de caractéristiques personnelles ou de personnalité connues ou prédites* ». Un système de crédit social a par exemple été instauré en Chine où les citoyens sont surveillés en permanence dans l'espace public grâce à des dispositifs de reconnaissance faciale. Chaque citoyen se voit attribuer une note en fonction de son comportement dans l'espace public et peut voir son accès aux transports tels que le train ou l'avion restreint en fonction de sa note ;

- les systèmes de reconnaissance biométrique en temps réel dans l'espace public et dans les espaces accessibles au public.

Ce faisant, l'article 1er s'inscrit dans la lignée du projet de règlement européen sur l'intelligence artificielle dévoilé par la Commission européenne en avril 2021. Celui-ci prévoit en effet l'interdiction de la notation sociale basée sur les données biométriques ainsi que des systèmes d'identification biométrique en temps réel dans les espaces publics à des fins répressives, sauf dans trois cas : pour la recherche de victimes potentielles d'actes criminels ; pour faire face à certaines menaces pour la vie ou la sécurité des personnes telles que les attaques terroristes ; et pour détecter, localiser, identifier ou engager des poursuites à l'encontre des auteurs de certaines infractions passibles d'une peine de prison d'au moins trois ans[1].

3. La position de la commission : des lignes rouges qu'il convient de renforcer et dont les dérogations doivent être encadrées

La commission est **favorable à la définition de lignes rouges** afin d'encadrer l'usage de la reconnaissance biométrique et d'éviter la mise en place d'une société de surveillance.

---

[1] *Il s'agit des infractions visées dans la décision-cadre du Conseil du 13 juin 2022* relative au mandat d'arrêt européen*, parmi lesquelles figurent les actes de terrorisme, la traite d'êtres humains, la corruption, les homicides volontaires, les viols* etc.

La commission souscrit donc pleinement à l'interdiction de la catégorisation et de la notation des personnes physiques sur la base de leurs données biométriques ainsi qu'à l'interdiction de la reconnaissance biométrique en temps réel dans l'espace public et dans les espaces accessibles au public.

Par l'adoption d'un **amendement COM-4** de son rapporteur, elle a toutefois modifié cet article de façon à **renforcer les lignes rouges relatives à la reconnaissance biométrique.**

D'une part, la commission s'est efforcée de cibler les systèmes de reconnaissance biométrique les plus sensibles en termes de libertés. S'agissant de l'interdiction de la reconnaissance biométrique dans l'espace public et dans les espaces accessibles au public, elle a estimé que **cette interdiction devait être centrée sur les systèmes d'identification biométrique réalisés à distance et sans le consentement de la personne**, qui présentent le plus de risques au regard des libertés publiques. Elle a donc exclu de cette interdiction les systèmes d'authentification biométrique tels que le système Parafe[1], fondé sur le consentement explicite de l'usager et dont l'utilisation a été jugée légitime et proportionnée par la CNIL.

L'authentification biométrique
et l'identification biométrique

L'authentification biométrique consiste à vérifier qu'une personne est bien celle qu'elle prétend être. Le système compare un gabarit biométrique préenregistré avec celui extrait du visage de la personne qui se présente à un point de contrôle. Il s'agit d'une comparaison « *1 contre 1* ». Cette technique est par exemple utilisée dans les sas Parafe installés dans les aéroports.

L'identification biométrique vise à retrouver une personne au sein d'un groupe d'individus filmés dans un lieu ou figurant sur une image. Le système extrait le gabarit de chaque personne du groupe et vérifie si ce gabarit correspond à une personne connue au sein d'une base de données. Il s'agit d'une comparaison « *1 contre N* », qui permet par exemple de lier un état civil à un visage ou de suivre la trajectoire d'une personne dans une foule.

D'autre part, la commission a jugé nécessaire de renforcer l'encadrement des systèmes de reconnaissance biométrique.

À cet effet, la commission a d'abord fixé une ligne rouge supplémentaire en **interdisant l'identification biométrique *a posteriori***, qui présente le même caractère intrusif que l'identification biométrique en temps réel puisqu'elle permet de traquer des personnes longtemps après la survenue d'un événement.

[1] *Passage rapide aux frontières extérieures*

Elle a ensuite précisé que les systèmes d'identification biométrique dans l'espace public et dans les espaces accessibles au public **ne pourraient être autorisés par voie réglementaire, même en cas de nécessité absolue**, contrairement à ce qui est prévu pour les traitements de données sensibles aux articles 31 et 88 de la loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*.

Elle a également décidé qu'**il ne pourrait être dérogé à l'interdiction des systèmes d'identification biométrique dans l'espace public et dans les espaces accessibles au public en dehors des cas prévus par la présente loi**, de façon à éviter tout glissement vers une société de surveillance. La commission a ainsi indiqué qu'il ne pourrait être dérogé à l'interdiction de principe posée dans l'article 1er que pour des motifs d'une exceptionnelle gravité, pour des finalités limitativement énumérées et selon un régime d'autorisations préalables. L'exécution de ces dérogations devra être assortie de contrôles exercés par des autorités indépendantes du service habilité à mettre en œuvre ces exceptions. Enfin, le recours aux dérogations devra obéir aux principes de nécessité et de proportionnalité, appréciés notamment au regard des finalités poursuivies et des circonstances de leur mise en œuvre, ainsi que du caractère limité des images traités et de leur durée de conservation.

Enfin, la commission a jugé que les dispositions relatives aux lignes rouges devraient être insérées dans **un nouvel article 6 *bis*** dans la loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés* plutôt qu'à l'article 95 de la même loi. En effet, l'intégration de ces dispositions au sein de l'article 95 limiterait leur application aux traitements de données à caractère personnel soumis au titre III de cette loi, qui transpose la directive « *Police-Justice* », c'est-à-dire aux traitements de données à caractère personnel 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.

La commission a adopté l'article 1er **ainsi modifié**.

Article 1er bis *(nouveau)*
Cadre expérimental et régime de contrôle des cas d'usage de la reconnaissance biométrique prévus par la proposition de loi

Introduit par la commission à la suite de l'adoption d'un amendement du rapporteur, l'article 1er *bis* vise à définir le cadre expérimental et le régime de contrôle des dispositifs ouverts par la proposition de loi.

Il prévoit ainsi que l'ensemble des cas d'usage de la reconnaissance biométrique dans l'espace public et dans les espaces accessibles au public ne soient autorisés qu'à titre expérimental, pour une durée de trois ans, pour des finalités précises. Ces usages feraient l'objet d'une procédure d'autorisation spécifique, des magistrats pour les usages judiciaires, et de la commission nationale de contrôle des techniques de renseignement (CNCTR) pour les usages administratifs. Cette expérimentation serait placée sous le contrôle du Parlement, qui pourrait s'adjoindre l'aide de différents experts afin d'assurer un suivi en temps réel et une évaluation forte des mesures prises ou mises en œuvre.

Introduit par la commission des lois par l'adoption de l'**amendement COM-5** du rapporteur, l'article 1er *bis* prévoit de définir le cadre expérimental et le régime de contrôle des cas d'usage de la reconnaissance biométrique dans l'espace public et les espaces accessibles au public définis par les articles de la proposition de loi. Ce faisant, il rassemble le contenu des articles 7 et 8 de la proposition de loi – avec quelques modifications – ces articles étant en conséquence supprimés.

2. La définition du caractère expérimental des cas d'usage de la reconnaissance biométrique prévus par la proposition de loi

Conformément à ce qu'envisageait l'article 8 de la proposition de loi, l'article 1er *bis* prévoit que **les mesures définies aux articles 2 à 6 sont prises à titre expérimental, pour une durée de 3 ans à compter de la promulgation de la loi**.

Si de nombreux acteurs appellent en effet à un encadrement de l'utilisation de la reconnaissance biométrique par les personnes publiques, tous semblent s'accorder sur la nécessité de la mise en place d'une phase d'expérimentation.

Comme le soulignaient les sénateurs Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain dans leur rapport d'information intitulé *La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance* : « ***Cette phase d'expérimentation semble faire consensus***. *Le coordonnateur national pour l'intelligence artificielle, Renaud Vedel, a ainsi estimé qu'*"une loi d'expérimentation pourrait, après avis de la CNIL, définir temporairement les conditions d'expérimentation et de

déploiement progressif de ces outils. **La clause de revoyure garantirait à la CNIL, au Conseil d'État et éventuellement au Parlement, qu'un débat démocratique global et exhaustif, éclairé par l'expérimentation, aurait lieu sur ces enjeux, après la phase de déploiement embryonnaire initial**". *Les représentants du secrétariat général de la défense et la sécurité nationale (SGDSN) exposent que* "le rôle de l'expérimentation est justement de fournir les éléments clefs de cette évaluation en matière opérationnelle, technique et juridique. **L'apport de la reconnaissance faciale reste à évaluer en conditions opérationnelles**, une solution mixte pouvant potentiellement présenter le meilleur compromis". *Le directeur général de la sécurité intérieure (DGSI) a pour sa part indiqué aux rapporteurs que* "pour la reconnaissance de visages sur la voie publique, la mise en place d'un cadre expérimental apparaît pertinent tant pour tester et s'assurer de la performance technique des solutions envisagées que pour **vérifier l'intérêt effectif des usages opérationnels envisagés**. Il s'agirait, ce faisant, de vérifier les différentes hypothèses de travail formulées par les services opérationnels et de s'assurer que le cadre législatif finalement mis en place sera non seulement adapté d'un point de vue des nécessités opérationnelles, mais également sur le plan de la protection des libertés publiques et individuelles" »[1].

Le recours à une expérimentation, dans les conditions prévues par l'article 37-1 de la Constitution, obligerait les différents acteurs – qu'il s'agisse du Parlement, du Gouvernement ou des services utilisateurs – **à se positionner ultérieurement sur les usages de la reconnaissance biométrique qui s'avèreraient les plus pertinents sur la base de l'expérience passée.**

La phase expérimentale permettrait au débat de se nouer, dépassant ce faisant les positions de principe des uns et des autres. Au terme de la durée de trois ans prévue pour l'expérimentation, les dispositifs autorisés par la proposition de loi ne seraient plus applicables. S'il s'avère qu'ils sont inutiles, mal ajustés aux besoins, ou insuffisamment protecteurs des libertés, il reviendrait au Parlement de se prononcer sur leur suppression, une réévaluation des besoins ou une modification des dispositifs en fonction des résultats obtenus.

[1] La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance, *rapport d'information n° 627 (2021-2022) de Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, déposé le 10 mai 2022, p.79. Ce rapport est consultable à l'adresse suivante : https://www.senat.fr/notice-rapport/2021/r21-627-notice.html*.

2. La mise en place d'un régime de contrôle des dispositifs de la proposition de loi

1.1. La création d'un comité scientifique et éthique : un affaiblissement du rôle du Parlement ?

L'article 8 de la proposition de loi prévoyait la **mise en place d'un comité scientifique et éthique qui serait chargé d'évaluer régulièrement l'application des dispositifs prévus par la proposition de loi**. Ses rapports seraient rendus publics et transmis aux présidents de la commission des lois de l'Assemblée nationale et du Sénat.

L'objectif poursuivi par les auteurs de la proposition de loi, explicité par leur rapport d'information, **était que l'expérimentation prévue soit une « "démarche sincèrement expérimentale"** *selon les termes de la CNIL car* "les expérimentations ne sauraient éthiquement avoir pour objet ou pour effet d'accoutumer les personnes à des techniques de surveillance intrusive, en ayant pour but plus ou moins explicite de préparer le terrain à un déploiement plus poussé"[1] » Pour ce faire, les auteurs de la proposition de loi ont souhaité la mise en place d'une « ***évaluation publique et indépendante*** *de l'efficacité de la technologie employée par un* ***comité composé de scientifiques et de personnes qualifiées en matière d'éthique*** *pour vérifier au cas par cas l'apport de la technologie de reconnaissance biométrique, sa proportionnalité, l'explicabilité de ses résultats,* etc. *Le comité pourrait* ***également formuler toute proposition de nature à améliorer le respect des principes juridiques et éthiques qui fondent les expérimentations*** *, veiller à la transparence du recours à cette technique auprès des personnes concernées, émettre un avis sur les évolutions souhaitables ou évaluer les choix techniques et l'efficacité du recours à la reconnaissance faciale.* ***Ce dispositif exige que le comité soit informé de chaque expérimentation et que lui soient transmises les données nécessaires à sa mission d'évaluation*** **»**[2].

L'article 8 prévoit cependant que la composition, l'organisation et les modalités de fonctionnement de ce comité soient fixées par décret, **ce qui ne permet pas de garantir son indépendance**.

L'externalisation du contrôle de l'expérimentation à un organisme extérieur au Parlement constitue également un affaiblissement du rôle de ce dernier, chargé par la Constitution de contrôler et d'évaluer l'action du Gouvernement, en particulier lorsqu'il l'autorise à mettre en place des dispositifs à titre expérimental. **L'article 1er *bis* n'a donc pas repris la création de ce nouveau comité**, la commission préférant s'en tenir à l'exercice par le Parlement de ses prérogatives.

---

[1] *« Reconnaissance faciale : pour un débat à la hauteurs des enjeux », CNIL, 15 novembre 2019.*

[2] La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance, *rapport d'information n° 627 (2021-2022) de Marc Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, déposé le 10 mai 2022, p.81. Ce rapport est consultable à l'adresse suivante : https://www.senat.fr/notice-rapport/2021/r21-627-notice.html.*

1.2. Un régime parlementaire de contrôle renforcé

Reprenant la majeure partie de l'article 7 de la proposition de loi, l'article 1er *bis* prévoit en **conséquence du caractère expérimental des dispositions de la proposition de loi et du caractère particulièrement novateur et intrusif des technologies qu'il est proposé d'expérimenter** la mise en place d'un **régime renforcé de contrôle parlementaire**.

L'article 7 prévoyait ainsi la mise en place de trois dispositifs d'information :

- l'information sans délai des mesures prises ou mises en œuvre par les autorités administratives en application des articles 2, 4 et 5 de la proposition de loi ;

- la transmission sans délai de la copie de tous les actes pris en application de ces dispositions ;

- la remise d'un rapport annuel du Gouvernement au Parlement qui concernerait tant les mesures prises en matière administrative (en application des articles 2, 4 et 5 de la proposition de loi) que celles prises en matière judiciaire (en application des articles 3 et 6 de la proposition de loi).

L'article prévoyait également que l'Assemblée nationale et le Sénat pouvaient requérir toute information complémentaire dans le cadre du contrôle et de l'évaluation de ces mesures.

La commission a considéré qu'un tel régime de contrôle renforcé se justifiait par le caractère très dérogatoire au droit commun de l'usage de la reconnaissance biométrique et par les **nombreuses inquiétudes** que ces technologies soulèvent dans la société. Elle s'est cependant interrogée sur le caractère indispensable de la mention selon laquelle les deux assemblées parlementaires pourraient requérir toute information complémentaire dans le cadre du contrôle et de l'évaluation des mesures. Il s'agit en effet d'une **prérogative découlant de la mission constitutionnelle du Parlement, chargé par l'article 24 de la Constitution de contrôler l'action du Gouvernement et d'évaluer les politiques publiques**. L'amendement portant article additionnel a en conséquence supprimé cette mention.

Par l'adoption de ce même amendement, la commission n'a **pas repris l'exigence de rapports annuels du Gouvernement au Parlement**, conformément à sa jurisprudence constante selon laquelle le Parlement peut, dans l'exercice de ses missions, réaliser des évaluations régulières des prérogatives qu'il accorde au Gouvernement et à l'autorité judiciaire.

S'agissant enfin de l'information en temps réel du Parlement, la commission a fait le choix de la **recentrer**, par cohérence avec l'adoption des autres amendements aux articles 4 et 5 inscrivant ces dispositifs dans un cadre de renseignement, **sur les mesures prises en application de l'article 2**. Afin de garantir un bon niveau d'information du Parlement, elle a par contre prévu que le **rapport annuel de la commission nationale de contrôle des techniques de renseignements devrait contenir une évaluation des mesures**

prises en application des articles 4 et 5, dans le respect du secret de la défense nationale et sans révéler des procédures ou des méthodes opérationnelles.

Enfin, et de manière classique pour une expérimentation, **le Gouvernement remettrait au Parlement un rapport évaluant l'application des mesures** prises en application de la proposition de loi **et appréciant l'opportunité de les pérenniser ou de les modifier**, notamment au vu de l'évolution du droit de l'Union européenne en la matière. Le règlement européen sur l'intelligence européenne devrait en effet, à cette date, avoir été définitivement adopté et il conviendra d'en tirer toutes les conséquences dans le droit national.

La commission a adopté l'article 1er *bis* **ainsi rédigé**.

Article 1er ter *(nouveau)*
Encadrement des traitements de données biométriques

Introduit par la commission à l'initiative du rapporteur, l'article 1er *ter* vise à définir les garanties que les traitements de données biométriques utilisés dans le cadre de la proposition de loi devront respecter.

Introduit par la commission par l'adoption de l'**amendement COM-6** du rapporteur, l'article 1er *ter* vise à **définir les conditions auxquelles devraient répondre les traitements de données biométriques développés** dans le cadre des usages proposés à titre expérimental par la proposition de loi, et ce afin de favoriser la protection des données dès la conception et par défaut (*privacy by design*). Ce concept signifie, selon la définition qu'en donne la commission nationale de l'informatique et des libertés (CNIL), que « *les responsables de traitements doivent mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. Concrètement, ils doivent veiller à limiter la quantité de données traitée dès le départ (principe dit de "minimisation")* ».

L'objectif poursuivi par la commission en intégrant à la proposition de loi cet article additionnel est que les garanties de protection des données personnelles soient intégrées dans la conception des traitements, et ne dépendent ainsi pas uniquement de l'usage qui en est fait.

L'article prévoit en conséquences **plusieurs exigences auxquelles les traitements de données biométriques développés pour répondre aux usages prévus par la proposition de loi devront répondre** :

- les traitements devront faire **apparaître le degré de probabilité qu'une personne apparaissant sur les images exploitées corresponde effectivement à la personne dont la présence est recherchée**. Les technologies de reconnaissance biométrique étant des technologies probabilistes, elles ne peuvent aboutir à la reconnaissance d'une personne de manière certaine à chaque fois. L'article 1er *ter* permet en conséquence d'afficher le taux de concordance entre le gabarit recherché et le gabarit extrait de l'image, afin que l'agent chargé de la surveillance du traitement puisse en tirer les conséquences nécessaires ;

- les traitements ne devront faire apparaître aux yeux de l'agent que le résultat final, et non pas le travail réalisé en arrière-plan, afin de constituer un **outil d'aide à la décision**, tout en protégeant les données personnelles des personnes qui ne sont pas recherchées ;

- les traitements ne pourront procéder à **aucun rapprochement, interconnexion ou mise en relation automatisés** avec d'autres traitements de données à caractère personnel ;

- ils demeureront en permanence sous **contrôle humain**. Cette garantie est essentielle. Elle permet d'exiger une interprétation humaine systématique des données produites par le traitement ;

- les **agents utilisant ces traitements devront être individuellement formés et habilités**.

L'article prévoit ensuite des garanti**es en matière de développement des traitements**. Ceux-ci seront développés par l'État et sous son contrôle, dans les conditions prévues pour le développement des traitements algorithmiques prévus par l'article 10 de la loi n° 2023-380 du 19 mai 2023 *relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions*.

Les traitements seraient autorisés par un décret en Conseil d'État pris après **avis de la Commission nationale de l'informatique et des libertés ou**, le cas échéant, **de la Commission nationale de contrôle des techniques de renseignement**, le décret devant être accompagné d'une analyse d'impact relative à la protection des données personnelles.

Enfin, **un échantillon de données pertinentes, adéquates et représentatives pourrait être collecté par l'État et sous sa responsabilité afin de servir en tant que données d'apprentissage** pour une durée strictement nécessaire et maximale de quatre mois à compter de l'enregistrement des images. Ces images seraient détruites, en tout état de cause, à la fin de l'expérimentation.

La commission a adopté l'article 1er *ter* **ainsi rédigé**.

Article 1er quater *(nouveau)*
Élargissement du collège de la Commission nationale de l'informatique et des libertés

Introduit par un amendement du rapporteur, l'article 1er *quater* intègre deux membres supplémentaires au collège de la Commission nationale de l'informatique et des libertés (CNIL) : le président de l'Autorité de régulation de la communication audiovisuelle et numérique ainsi que le président de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP). Par réciprocité, il est prévu une représentation de la CNIL au sein de ces deux autorités.

Dans un rapport d'information en date d'avril 2023 relatif aux *enjeux de l'utilisation d'images de sécurité dans le domaine public*[1], les députés Philippe Gosselin et Philippe Latombe décrivent la CNIL comme « ***l'organisme public idoine afin de relever les défis que posent les progrès de l'intelligence artificielle*** » et recommandent de lui confier le rôle de « chef de file » de la régulation de l'intelligence artificielle. Pour ce faire, ils préconisent, d'une part, de renforcer les moyens humains et techniques à sa disposition et, d'autre part, **d'intégrer à son collège les présidents de l'ARCEP et de l'ARCOM**.

Par l'adoption d'un **amendement COM-7** du rapporteur, la commission a traduit cette seconde recommandation au niveau législatif. Elle a estimé que **cet élargissement du collège de la CNIL renforcerait sa crédibilité en tant que première autorité régulatrice de l'intelligence artificielle et fluidifierait le dialogue avec les autres institutions compétentes en matière de régulation du numérique**. Réciproquement, elle a prévu que le président de la CNIL, ou l'un de ses représentants, siège au sein de chacune de ces autorités. Veillant à ce que cette nouvelle mission ne détourne pas le président de la CNIL de ses missions propres, la commission a toutefois prévu que, dans le cas de l'ARCEP, il ne siège qu'au sein de la formation plénière. Au cours de son audition par la commission des lois le 23 mai 2023, le secrétaire général de la CNIL s'était par ailleurs montré

[1] *Les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité, Assemblée nationale, rapport d'information n° 1089 (2022-2023) de Philippe Gosselin et Philippe Latombe, déposé le 12 avril 2023. Ce rapport est consultable à l'adresse suivante :*
https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information#_Toc256000052

personnellement[1] plutôt favorable à une évolution de cette nature, estimant que « ***l'interrégulation est de plus en plus nécessaire*** »[2].

Du reste, **une organisation de cette nature a déjà été mise en place avec succès** entre la CNIL et la Commission d'accès aux documents administratifs par les articles 25 et 27 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. Au cours de son audition précitée, le secrétaire général de la CNIL a ainsi tiré un bilan très positif de cette évolution dont il relevait qu'elle « [créait] *une remarquable fluidité entre les deux exigences que sont la protection des données personnelles et la bonne communication des documents administratifs* »[3].

La commission a adopté l'article 1er *quater* **ainsi rédigé**.

[1] *Sous les réserves d'usage, dans la mesure où cette question n'a pas fait l'objet d'une délibération du collège de la CNIL et cette analyse ne présume pas de la position officielle que pourrait adopter l'institution.*

[2] *Audition de Louis Dutheillet de Lamothe, secrétaire général de la CNIL, par la commission des lois le 23 mai 2023. La vidéo de l'audition est disponible à cette adresse : https://www.senat.fr/travaux-parlementaires/commissions/commission-des-lois/actualite/audition-de-louis-dutheillet-de-lamothe-secretaire-general-de-la-cnil-862.html.*

[3] *Sous les réserves d'usage, dans la mesure où cette question n'a pas fait l'objet d'une délibération du collège de la CNIL et cette analyse ne présume pas de la position officielle que pourrait adopter l'institution.*

CHAPITRE II
EXPÉRIMENTATION DE DISPOSITIFS D'AUTHENTIFICATION BIOMÉTRIQUE SANS CONSENTEMENT POUR L'ACCÈS À CERTAINS GRANDS ÉVÈNEMENTS
(Division nouvelle)

Afin d'assurer la clarté du texte, la commission a créé une nouvelle division relative à l'expérimentation de dispositifs d'authentification biométrique sans consentement pour l'accès à certains grands évènements, en adoptant l'**amendement COM-8** du rapporteur.

Article 2
Authentification biométrique sans consentement pour l'accès à certains grands événements

L'article 1er tend à autoriser à titre expérimental les organisateurs de certains grands événements à mettre en place un système d'authentification biométrique obligatoire pour l'accès de certaines personnes à tout ou partie des zones accueillant le grand événement.

La commission a adopté cet article avec modifications, afin d'exclure les riverains du dispositif et d'en réserver la mise en œuvre à l'État.

1. L'authentification biométrique est aujourd'hui autorisée de manière encadrée

À l'heure actuelle, les systèmes d'authentification biométrique ne sont autorisés que dans deux hypothèses très encadrées.

D'une part, l'authentification biométrique est autorisée lorsque le consentement de la personne a été recueilli. Le consentement de la personne doit cependant être donné de manière libre et éclairée, ce qui implique l'existence d'une alternative ainsi que l'absence de subordination[1]. Cette hypothèse correspond par exemple au système « Parafe » utilisé dans certains aéroports, qui permet aux voyageurs de franchir rapidement la frontière sans contrôle manuel, en passant par un sas automatisé où le gabarit du passeport est comparé au gabarit de la personne filmée dans le sas, ou encore aux systèmes d'authentification permettant aux usagers de déverrouiller leur téléphone grâce à leur visage.

[1] *Tribunal administratif de Marseille, 27 février 2020, n° 1901249.*

D'autre part, des dispositifs d'authentification biométrique sans alternative peuvent être mis en place sur les lieux de travail, de manière très encadrée.

Le 4° de l'article 44 de la loi n° 78-17 du 6 janvier ***1978 relative à l'informatique, aux fichiers et aux libertés*** prévoit ainsi que les employeurs et administrations peuvent mettre en place un système d'authentification biométrique pour l'accès des salariés, agents, stagiaires et prestataires aux lieux de travail ainsi qu'aux appareils et applications utilisés dans le cadre de leurs missions.

Les dispositifs d'authentification biométrique mis en place dans ce cadre doivent cependant répondre à plusieurs exigences spécifiques fixées par un règlement type de la Commission nationale de l'informatique et des libertés[1]. Celui-ci précise par exemple que l'employeur doit expliquer pourquoi les systèmes classiques tels que le contrôle par badge sont insuffisants et réaliser une analyse d'impact préalable.

2. Le dispositif proposé : la mise en place d'un système d'authentification biométrique obligatoire pour l'accès à certains grands événements

Reprenant une recommandation de la mission d'information sur la reconnaissance biométrique dans l'espace public conduite par les sénateurs Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, l'article 2 de la proposition de loi insèrerait un 4° *bis* à l'article 44 de la loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés* et tend à permettre aux organisateurs de certains grands événements au sens de l'article L. 211-11-1 du code de la sécurité intérieure, à titre expérimental, de mettre en place un système d'authentification biométrique obligatoire.

Les grands événements

Les **grands événements** sont régis par l'article L. 211-11-1 du code de la sécurité intérieure. Il s'agit d'événements exposés à **un risque d'actes de terrorisme** en raison de leur nature et de l'ampleur de leur fréquentation. Ces grands événements sont désignés par décret.

La qualification de grand événement permet de soumettre l'accès de toute personne, à un autre titre que celui de spectateur ou de participant, à tout ou partie des établissements et installations désignés par le décret précité, à **une autorisation de l'organisateur**. L'organisateur recueille au préalable l'avis de l'autorité administrative, lequel est rendu à la suite d'une **enquête administrative**.

[1] *Délibération de la CNIL n° 2019-001 du 10 janvier 2019* portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail.

Ont notamment été qualifiés de grand événement les Jeux Olympiques et Paralympiques de 2024 organisés à Paris, le salon international de l'aéronautique et de l'espace du Bourget ou encore la fête du citron de Menton.

Plusieurs garanties entoureraient cette expérimentation. En premier lieu, seuls certains grands événements, ceux **particulièrement exposés à des risques d'actes de terrorisme ou à des risques d'atteinte grave à la sécurité des personnes**, seraient concernés par cette possibilité. L'objectif est de cibler les grands événements les plus sensibles, tels que les sommets de chefs d'État et de gouvernement.

En deuxième lieu, s'agissant des **personnes concernées**, seules celles participant à un autre titre que celui de spectateur ou de participant seraient soumises à ce dispositif d'authentification biométrique obligatoire. Aux termes de l'article R. 211-33 du code de la sécurité intérieure, cette obligation s'appliquerait notamment aux personnes contribuant au soutien technique et logistique de l'événement, à celles assurant la surveillance des installations et espaces concernés par le dispositif ou encore à celles exerçant une activité professionnelle ou bénévole au sein des zones concernées. Les résidents dans la zone concernée seraient aussi soumis à cette obligation.

En troisième lieu, conformément au droit commun, la mise en place de ce dispositif s'effectuerait sous **le contrôle plein et entier de la CNIL** et le traitement de données biométriques devrait répondre aux exigences fixées par un **règlement type établi par la CNIL**, comme c'est déjà le cas pour le contrôle de l'accès aux lieux de travail évoqué ***supra.***

3. La position de la commission : une expérimentation justifiée dont l'encadrement doit être renforcé

La commission est favorable à la mise en place de cette expérimentation, justifiée par le fait que les grands événements sont exposés à davantage de menaces.

Par l'adoption d'un **amendement COM-9** de son rapporteur, la commission a cependant souhaité mieux encadrer ce dispositif.

À cet effet, la commission a d'abord souhaité restreindre le champ de l'expérimentation. Pour cela, elle a d'une part prévu que les traitements de données biométriques utilisés à des fins d'authentification biométrique lors des grands événements **ne pourront être mis en œuvre que par l'État**, et pas directement par l'organisateur du grand événement. Ce dernier peut en effet être une personne privée. À titre d'exemple, le salon international de l'aéronautique et de l'espace, qui est un grand événement, est organisé par une filiale du Groupement des industries françaises aéronautiques et spatiales (GIFAS).

D'autre part, la commission a précisé que **les dispositifs d'authentification biométrique obligatoire ne pourront concerner les habitants des zones concernées par la mise en place de ce système**. Ceux-ci devront disposer d'un moyen alternatif pour rejoindre leur domicile.

Par ailleurs, la commission a souhaité ajouter de nouvelles garanties. Elle a ainsi précisé que les personnes concernées par le système d'authentification biométrique obligatoire, tels que les employés ou les bénévoles, devront avoir été **informés au préalable** de la mise en place de ce système.

Elle a en outre prévu que pour mettre en place un tel système, **l'organisateur d'un grand événement devra démontrer qu'un haut niveau de fiabilité de l'identification des personnes est requis pour accéder aux établissements et installations faisant l'objet d'une restriction de circulation et d'accès**, et pas seulement pour accéder au grand événement.

La commission a adopté l'article 2 **ainsi modifié**.

CHAPITRE III
EXPÉRIMENTATION DE TRAITEMENTS DE DONNÉES BIOMÉTRIQUES *A POSTERIORI* DANS LE CADRE D'ENQUÊTES JUDICIAIRES OU EN MATIÈRE DE RENSEIGNEMENT
(Division nouvelle)

Afin d'assurer la clarté du texte, la commission a créé une nouvelle division regroupant trois articles consacrés à l'utilisation de traitements de données biométriques *a posteriori* dans le cadre d'enquêtes judiciaires et en matière de renseignement (**amendement COM-10** du rapporteur).

Article 3
Expérimentation de logiciels de reconnaissance biométrique d'identification *a posteriori* dans le cadre d'enquêtes judiciaires

L'article 3 autorise, à titre expérimental, l'utilisation de logiciels de reconnaissance biométrique *a posteriori* dans le cadre de certaines enquêtes judiciaires. Adoptant cet article, la commission a limité cette possibilité aux seules enquêtes portant sur des faits de terrorisme, de trafic d'armes, d'atteintes aux personnes punies d'au moins cinq ans de prison ainsi qu'aux procédures de recherche de personnes disparues ou en fuite. Elle a également explicitement prévu une autorisation préalable de l'autorité judiciaire, précisant la nature et l'origine des données, ainsi que l'interdiction de rassembler dans un traitement unique les données exploitées selon cette méthode.

1. L'état du droit : une extension du recours à l'utilisation de la reconnaissance biométrique *a posteriori* dans un cadre judiciaire qui requiert un fondement législatif spécifique

1.1. Une utilisation actuellement très limitée de la reconnaissance biométrique a posteriori

La reconnaissance biométrique n'est aujourd'hui utilisée dans un cadre judiciaire qu'*a posteriori* et à partir d'un unique traitement de données à caractère personnel. Il s'agit du **traitement des antécédents judiciaires (TAJ)**, créé par le décret n° 2012-652 du 4 mai 2012 et régi par les articles 230-6 à 230-11 du code de procédure pénale, qui a pour finalités de « *faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs* »[1]. Concrètement, ce fichier rassemble des données recueillies dans le cadre des procédures établies par la police et la gendarmerie nationales, ainsi que par les agents des douanes habilités à

[1] *Article 230-6 du code de procédure pénale.*

exercer des missions de police judiciaire. Aux termes de l'article R. 40-26 du code de procédure pénale, peuvent notamment être enregistrées **les photographies des personnes mises en cause** dans les procédures d'enquêtes et d'instruction conduites par ces services[1] et **à partir desquelles des logiciels de reconnaissance faciale peuvent être utilisés**. Dans leur rapport d'information de mai 2022[2], les sénateurs Marc-Philippe Daubresse, Arnaud De Belenet et Jérôme Durain y voient un « *outil d'aide à l'enquête, qui peut par exemple permettre à un enquêteur qui dispose d'une photographie de l'auteur des faits d'orienter ses recherches vers une personne déjà connue du TAJ* ».

Sur un plan juridique, **les dispositions relatives à l'usage de la reconnaissance faciale de l'article R. 40-26 du code de procédure pénale ont été validées par le Conseil d'État**. Statuant en 2022 sur un recours intenté par l'association La Quadrature du net[3], il a estimé que, d'une part, **le recours à ces logiciels relevait bien d'une « nécessité absolue »** au sens de l'article 88[4] de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. L'arrêt mentionne ainsi le fait qu'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* », et ce alors que les rapprochements opérés par cette voie « *peuvent s'avérer absolument nécessaires à la recherche des auteurs d'infractions et à la prévention des atteintes à l'ordre public* ». D'autre part, le Conseil d'État a considéré que le code de procédure pénale **assortissait le recours à la reconnaissance faciale de « garanties appropriées »**[5], eu égard notamment aux modalités de recueil des données contenues dans le fichier et au contrôle soutenu de l'autorité judiciaire.

Sur un plan pratique, **l'apport de l'usage de logiciels de reconnaissance faciale sur les données contenues dans le TAJ est unanimement apprécié.** Selon les données figurant dans le rapport de Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain précité, les services de la police nationale les ont utilisés à 498 871 reprises en 2021 et ceux de la gendarmerie nationale environ 117 000. Il s'agit néanmoins d'une part marginale du total des consultations du TAJ, estimée à environ 3,2 %[6].

---

[1] *Cette possibilité peut également être utilisée pour des finalités de renseignement, selon les conditions définies à l'article L. 234-4 du code de la sécurité intérieure.*

[2] La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance, *rapport d'information n° 627 (2021-2022) de Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, déposé le 10 mai 2022. Ce rapport est consultable à l'adresse suivante : https://www.senat.fr/notice-rapport/2021/r21-627-notice.html.*

[3] *Conseil d'État, 10ème chambre, 26 avril 2022, n° 442364, La Quadrature du Net.*

[4] *Pris pour l'application de la directive 2016/680 (UE) du Parlement européen et du Conseil du 27 avril 2016, dite « directive Police Justice ».*

[5] *Au sens du même article 88 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*

[6] *Sur un total de 15 341 000 consultations en 2021.*

1.2. Des dispositifs de reconnaissance biométriques potentiellement déterminants pour le succès des enquêtes judiciaires

Les bénéfices potentiels d'une extension du recours à la reconnaissance faciale dans un cadre judiciaire font consensus. À titre d'exemple, les éléments transmis par la Conférence nationale des procureurs de la République rappellent que « *les opérations de recherche a posteriori dans des flux d'images multiples sont particulièrement lourdes et fastidieuses, de sorte que de telles investigations s'inscrivent dans des délais longs, peu compatibles avec les durées de garde à vue et l'exigence de célérité de l'action judiciaire* ».

Le recours à cette technologie apparaît, en outre, **particulièrement adapté dans le cadre de certaines enquêtes**. C'est par exemple le cas pour la recherche d'une personne disparue ou en fuite, dont la présence pourrait être détectée instantanément sur les images recueillies et le parcours reconstitué, et ce quel que soit le volume d'images. Cet appui serait d'autant plus précieux que ces enquêtes se caractérisent par un degré d'urgence important.

1.3 La nécessité d'un fondement législatif spécifique pour étendre cet usage de la reconnaissance biométrique a posteriori

Le niveau de norme approprié pour étendre le recours à la reconnaissance biométrique *a posteriori* dans un cadre judiciaire, en particulier sur des enregistrements issus de la vidéoprotection et recueillies au cours des enquêtes, **a fait débat au cours des travaux du rapporteur**. La question s'est notamment posée de savoir si les articles 230-20 à 230-27 du code de procédure pénale régissant les logiciels de rapprochement judiciaire pouvaient être interprétés comme autorisant une telle extension de l'usage de la reconnaissance faciale, sous réserve des modifications règlementaires correspondantes.

La commission a confirmé l'interprétation des auteurs de la proposition de loi, selon laquelle un fondement législatif spécifique est nécessaire. De fait, ces logiciels procèdent exclusivement à « *l'exploitation et au rapprochement d'informations sur les modes opératoires* »[1] et les données exploitées n'ont pas de caractère biométrique. Il s'agit, pour l'essentiel, des traitements automatisés d'exploitation de relevés bancaires et de documents téléphoniques[2] dénommés « ANACRIM-ATRT » dans le cas de la gendarmerie nationale et MERCURE dans le cas de la police nationale. Au cours de son audition, la direction des affaires criminelles et des grâces (DACG) a précisé que le premier était utilisé par environ 20 000 enquêteurs par an, tandis que l'utilisation du second est particulièrement fréquente.

[1] *Article 230-20 du code de procédure pénale.*
[2] *Pour* « Application de traitement des relations transactionnelles ».

Si le recours à un dispositif de reconnaissance faciale sur les données contenues dans le TAJ a ensuite été validé par le Conseil d'État, celui-ci a expressément pris en compte le fait que les dispositions règlementaires correspondantes n'avaient « *pas pour objet de définir les conditions de collecte d'images de personnes circulant dans l'espace public ou mises en ligne sur les réseaux sociaux* ***ni d'autoriser la confrontation systématique ou à grande échelle de telles images avec les gabarits biométriques enregistrés dans ce traitement*** ». Cette réserve **exclut la possibilité de confronter des enregistrements issus de la vidéoprotection à l'intégralité des images contenues dans un fichier, en l'espèce le TAJ,** et suscite *a minima* des doutes sur la légalité d'un potentiel usage de logiciels de reconnaissance faciale pour repérer la présence d'une seule personne préalablement identifiée sur un enregistrement vidéo. Dans un rapport d'information publié en avril 2023, les députés Philippe Gosselin et Philippe Latombe vont même plus loin et relèvent que « ***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*** »[1].

Le rapport d'information de Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain précité évoque par ailleurs un avis rendu le 12 octobre 2021 par le Conseil d'État, non publié, où celui-ci estimerait que, « ***compte tenu du changement d'échelle qu'ils impliquent dans la capacité d'exploitation des images de surveillance de la voie publique*** **», les traitements de données ayant recours à l'intelligence artificielle sur des images issues de l'espace public devraient être autorisés par le législateur**. Il convient par ailleurs de relever que les services ne procèdent pas à un tel usage aujourd'hui, en partie en raison de ces incertitudes juridiques.

Du reste, dans le cadre de la présente proposition de loi, **la commission a fait le choix de trancher définitivement ce débat** en interdisant explicitement « *le traitement de données biométriques aux fins d'identifier une personne à distance dans l'espace public et dans les espaces accessibles au public* », sauf lorsque la personne a donné son consentement ou dans les cas et selon les conditions déterminées par la loi[2]. **Tirant les conséquences de cette interdiction, elle a également créé un fondement législatif spécifique à l'usage de la reconnaissance faciale sur les données contenues dans le TAJ**[3].

---

[1] *Les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité, Assemblée nationale, rapport d'information n° 1089 (2022-2023) de Philippe Gosselin et Philippe Latombe, déposé le 12 avril 2023. Ce rapport est consultable à l'adresse suivante :*
https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information#_Toc256000052

[2] *Voir le commentaire de l'article 1er.*

[3] *Voir le commentaire de l'article 4A.*

2. L'article 3 : expérimenter le recours *a posteriori* à cette technologie pour certaines enquêtes judiciaires

L'article 3 propose d'insérer un chapitre III *bis* au sein du chapitre III du titre IV du livre Ier du code de procédure pénale, à la suite du chapitre consacré à l'utilisation de logiciels de rapprochement judiciaires. Ce chapitre vise à **autoriser, à titre expérimental, l'usage de la reconnaissance faciale *a posteriori*,** aux seules fins de « *faciliter le rassemblement des preuves des infractions* [visées] *et l'identification de leurs auteurs ou la recherche d'une personne disparue* », sur les images recueillies au cours d'enquêtes et d'instructions portant sur **des crimes et délits punis d'une peine d'emprisonnement de trois ans ou plus ainsi que dans le cadre de procédures de recherche d'une personne en fuite ou des causes de la mort ou de la disparition.**

Le dispositif est construit selon le même modèle que celui applicable aux logiciels de rapprochement judiciaire et avec des garanties similaires.

Ces logiciels de reconnaissance faciale ne pourraient être mis en œuvre que par des agents qualifiés et habilités de la police et de la gendarmerie nationales, ainsi que des services des douanes, et sous le contrôle de l'autorité judiciaire.

S'agissant des données biométriques exploitées, il est précisé que celles-ci ne pourraient provenir que des pièces déjà détenues dans le cadre de l'enquête judiciaire. Elles seraient effacées à la clôture de l'enquête et, en tout état de cause, à l'issue d'un délai de trois ans[1].

S'agissant des dispositifs de contrôle prévus, le procureur de la République compétent pourrait demander à tout moment que les données soient effacées, complétées ou rectifiées. Un magistrat désigné à cet effet par le ministre de la justice serait par ailleurs chargé de contrôler la mise en œuvre de ces logiciels, et notamment de la mise à jour des données. En outre, les pouvoirs de contrôle de la Commission nationale de l'informatique et des libertés s'appliqueraient dans les conditions du droit commun.

Enfin, l'usage de ces logiciels à des fins d'enquêtes administratives est explicitement exclu et ils devraient être autorisés par décret en Conseil d'État pris après avis de la CNIL.

3. La position de la commission : autoriser l'expérimentation uniquement pour les enquêtes portant sur des infractions d'une exceptionnelle gravité et en renforçant les garanties associées

La commission a **accueilli positivement la démarche des auteurs de la proposition de loi** d'expérimenter plus largement le recours à des logiciels de d'identification biométrique *a posteriori* dans le cadre d'enquêtes

[1] *Ce délai est porté à 20 ans dans le cas des procédures de recherche des causes de la disparition.*

judiciaires. Compte tenu des risques importants qu'elle engendre pour l'exercice des libertés publiques, elle s'est néanmoins attachée à **maximiser les garanties associées.**

Elle a donc veillé à ce que les traitements concernés se voient appliquer **l'ensemble des garanties communes aux logiciels de reconnaissance qu'elle a entendu mettre en place**[1]. Il en résulte notamment **qu'aucune interconnexion ne pourrait être effectuée avec d'autres traitements de données**. Concrètement, il ne serait par exemple pas autorisé de comparer « à la volée » les images contenues dans le TAJ avec l'ensemble des personnes apparaissant sur les enregistrements, afin de détecter d'éventuelles correspondances. Il s'agirait principalement de **vérifier la présence d'une personne déterminée** et, le cas échéant, de reconstituer son parcours.

En outre, la commission a **restreint le champ de l'expérimentation aux seules enquêtes et instructions portant sur des infractions d'une exceptionnelle gravité**. Par l'adoption d'un **amendement COM-11** du rapporteur, elle a donc limité l'usage de la reconnaissance biométrique a posteriori :

- aux seules enquêtes et instructions portant sur des faits de **terrorisme, de trafic d'armes ou sur des atteintes aux personnes punies d'au moins cinq ans d'emprisonnement** ;

- aux procédures de recherche de la cause de la mort ou de la disparition ou d'une personne en fuite.

Par l'adoption du même **amendement COM-11**, la commission a soumis explicitement l'usage de ces logiciels à une **autorisation préalable de l'autorité judiciaire**, laquelle devrait préciser **la nature et l'origine des données exploitées**. Afin de tirer les conséquences d'une réserve émise par le Conseil constitutionnel dans sa décision n° 2011-625 DC du 10 mars 2011 relative aux logiciels de rapprochement judiciaire, elle a également précisé que le dispositif ne pourrait « ***conduire qu'à la mise en œuvre de traitements de données à caractère personnel particuliers****, dans le cadre d'une enquête ou d'une procédure déterminée portant sur une série de faits et pour les seuls besoins de ces investigations* ».

La commission a adopté l'article 3 **ainsi modifié**.

---

[1] *Voir commentaire de l'article 1er ter. Il en résulte que les garanties relatives à ce que l'apparition de l'identité des intéressés ne puisse apparaître qu'à l'issue des opérations de rapprochement et à l'exigence d'une autorisation par décret en Conseil d'État pris après avis de la CNIL, ont été déplacées vers cet article.*

Article 4 A (nouveau)
Reconnaissance biométrique dans le cadre des fichiers d'antécédents judiciaires

Introduit par la commission à l'initiative de son rapporteur, l'article 4 A vise à permettre aux forces de sécurité intérieure de continuer à utiliser des systèmes de reconnaissance biométrique *a posteriori* au sein des fichiers d'antécédents judiciaires dans le cadre de la recherche des auteurs d'infractions à la loi pénale.

Introduit par **l'amendement COM-12** adopté par la commission à l'initiative de son rapporteur, l'article 4 A vise à permettre aux **services de la police et de la gendarmerie nationales de continuer à recourir a posteriori à des dispositifs de reconnaissance biométrique dans le cadre de la recherche des auteurs d'infractions à la loi pénale**, afin d'identifier des personnes mises en cause, faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou de la disparition, au sein des fichiers d'antécédents judiciaire comme le « **traitement des antécédents judiciaires** » (TAJ).

Depuis 2012, l'article R. 40-26 du code de procédure pénale autorise en effet les forces de sécurité intérieure à utiliser **la reconnaissance biométrique pour identifier les personnes fichées dans le TAJ**. Dans ce fichier, les photographies des visages des personnes mises en causes ou disparues ainsi que des corps non identifiées peuvent être enregistrées.

Cette possibilité est entourée de **nombreuses garanties**, puisque les informations ne peuvent être recueillies que dans le cadre des procédures établies par les services de sécurité intérieure[1]. Par ailleurs, le TAJ est utilisé sous le contrôle du procureur de la République territorialement compétent, qui peut effacer, compléter ou rectifier les données personnelles inscrites dans le fichier, d'office ou à la demande de la personne concernée. Un magistrat désigné par le ministre de la justice est chargé de suivre la mise en œuvre du fichier et dispose des mêmes prérogatives que le procureur de la République. Enfin, seuls des personnels spécialement habilités peuvent accéder aux données contenues dans le TAJ. D'autres garanties, relatives par exemple à la durée de conservation des données personnelles, sont également prévues par des dispositions réglementaires.

Par coordination avec l'article 1er, qui interdit la reconnaissance biométrique dans l'espace public *a posteriori*, cet article vise à conserver la possibilité pour les forces de sécurité intérieure de recourir à cette modalité de recherche des personnes.

[1] *Au cours des enquêtes concernant tout crime ou délit ainsi que les contraventions de cinquième classe sanctionnant un trouble à l'ordre public ou une atteinte aux personnes, aux biens ou à l'autorité de l'État ou au cours des procédures de recherches des causes de la mort ou de recherche des causes d'une disparition.*

Le recours à la reconnaissance biométrique dans le TAJ est en effet un dispositif utile dans la conduite des enquêtes, dont la proportionnalité a été validée par le Conseil d'État[1]. À cette occasion, ce dernier a souligné qu'« *une telle identification à partir du visage d'une personne et le rapprochement avec les données enregistrées […] peuvent s'avérer absolument nécessaires à la recherche des auteurs d'infractions et à la prévention des atteintes à l'ordre public, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle* ».

La commission a adopté l'article 4 A **ainsi rédigé**.

Article 4

Création d'une nouvelle technique de renseignement permettant aux services du premier cercle d'utiliser des logiciels de reconnaissance biométrique *a posteriori*

L'article 4 instituerait une nouvelle technique de renseignement permettant aux services du premier cercle d'utiliser des logiciels de reconnaissance biométrique *a posteriori*, dans un cadre administratif.

La commission a clarifié les procédures applicables en fonction de l'origine des données traitées, en ciblant la création de la nouvelle technique de renseignement sur la nouvelle possibilité ouverte par l'article, permettant aux services d'exploiter *a posteriori* les images de vidéoprotection par ce type de logiciels après autorisation du Premier ministre donnée après avis de la commission nationale de contrôle des techniques de renseignement (CNCTR).

1. L'exploitation des images recueillies par les services de renseignement : une possibilité limitée mais peu encadrée d'utiliser des traitements de données biométriques

L'exploitation des images et des sons recueillis par les services de renseignement est d'une grande importance dans l'exercice de leur mission. Au regard du volume des données collectées, l'apport de logiciels d'intelligence artificielle dans ce cadre est indéniable.

Les données utilisées par les services de renseignement peuvent provenir de **deux sources principales** :

- le **déploiement de différentes techniques de recueil de renseignements** par les services de renseignement, conditionné à l'autorisation du Premier ministre délivrée après avis de la

[1] *CE, 26 avril 2022, n° 442364.*

Commission nationale de contrôle des techniques de renseignement[1]. Ces techniques, décrites au titre V du livre VIII du code de la sécurité intérieure, comprennent les accès administratifs aux données de connexion, les interceptions de sécurité, la sonorisation de certains lieux et véhicules et la captation d'images et de données informatiques, les mesures de surveillance des communications électroniques internationales, et les mesures de surveillance de certaines communications hertziennes ;

- les **images issues de la voie publique**, notamment provenant des systèmes de vidéoprotection existants.

S'agissant des renseignements collectés par le biais des techniques de renseignement, la loi n° 2015-912 du 24 juillet 2015 *relative au renseignement* a prévu que l'autorisation de déploiement de la technique valait autorisation de l'exploitation des renseignements collectés. Comme le soulignaient les sénateurs Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain dans leur rapport sur *La reconnaissance biométrique dans l'espace public*[2], « *Au regard du volume des données collectées par ce biais, le développement d'outils d'aide à l'enquête, y compris utilisant l'intelligence artificielle, constitue un enjeu majeur* ». Les services de renseignement, et plus particulièrement la direction générale de la sécurité intérieure (DGSI), ont ainsi initié des programmes de recherche afin de développer des outils d'analyse d'images, y compris des outils comportant des systèmes de reconnaissance faciale. Ces outils ont deux objectifs : soit rechercher le visage d'une cible particulière dans un flux vidéo ou une base de visages, soit regrouper des visages similaires dans un silo de données afin de détecter d'éventuelles relations.

Depuis la loi n° 2021-998 du 30 juillet 2021 *relative à la prévention d'actes de terrorisme et au renseignement*, les services de renseignement peuvent conserver les données pendant une durée plus longue à des fins de recherche et développement[3]. Cet allongement de la durée de conservation devrait permettre l'amélioration de la performance de ces outils.

L'exploitation des images issues de la voie publique par les services de renseignement se rapporte quant à elle au cadre classique d'exploitation de ces images par les services de police et de gendarmerie. Ainsi, selon les informations recueillies par les sénateurs Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain au cours de leurs travaux sur la reconnaissance biométrique dans l'espace public, « *le Conseil d'État aurait […], dans un avis rendu le 12 octobre 2021, non publié, estimé que* ***les traitements des images issues de la vidéoprotection par le biais***

---

[1] *Suivant la procédure d'autorisation prévue au chapitre Ier du livre VIII du titre II du code de la sécurité intérieure (articles L. 821-1 et suivants).*

[2] La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance*, rapport d'information n° 627 (2021-2022) de Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, déposé le 10 mai 2022. Ce rapport est consultable à l'adresse suivante : https://www.senat.fr/notice-rapport/2021/r21-627-notice.html.*

[3] *Article L. 822-2 du code de la sécurité intérieure.*

d'un logiciel d'intelligence artificielle constituent des traitements de données personnelles distincts de ceux des images issus de la vidéoprotection *et que ceux-ci, compte tenu du* ***changement d'échelle*** *qu'ils impliquent* ***dans la capacité d'exploitation des images de surveillance de la voie publique****, sont susceptibles de porter une atteinte telle à la liberté individuelle qu'elle affecterait les garanties fondamentales apportées aux citoyens pour l'exercice des libertés publiques au sens de l'article 34 de la Constitution du 4 octobre 1958. Le Conseil d'État en [a déduit] qu'une* ***base législative explicite [était] nécessaire pour encadrer le recours à l'intelligence artificielle sur des images issues de l'espace public, y compris sans utilisation de données biométriques*** »[1]. À ce jour donc, à l'exception des possibilités ouvertes par l'article 10 de la loi n° 2023-380 du 19 mai 2023 *relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions*[2], une exploitation de ces images par des logiciels d'intelligence artificielle, *a fortiori* traitant des données biométriques, est interdite.

2. L'article 4 de la proposition de loi : la création d'une nouvelle technique de renseignement encadrant l'usage *a posteriori* de logiciels de reconnaissance biométrique par les services du premier cercle

1.1. L'article 4 de la proposition de loi : la création d'une nouvelle technique s'appliquant tant aux renseignements collectés par le biais des techniques de renseignement qu'aux images issues de la vidéoprotection

L'article 4 de la proposition de loi instituerait une nouvelle technique de renseignement encadrant l'usage *a posteriori* de logiciels de reconnaissance biométrique par les services de renseignement du premier cercle.

Il est ainsi proposé que les services du premier cercle[3] puissent être autorisés par le Premier ministre, après avis de la commission nationale de

---

[1] La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance, *rapport d'information n° 627 (2021-2022) de Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, déposé le 10 mai 2022. Ce rapport est consultable à l'adresse suivante : https://www.senat.fr/notice-rapport/2021/r21-627-notice.html*.

[2] *Qui autorise, à titre expérimental jusqu'au 30 mars 2023, l'utilisation de traitements algorithmiques sur les images captées par des dispositifs de vidéoprotection ou des aéronefs afin de détecter et de signaler en temps réel des évènements prédéterminés susceptibles de menacer la sécurité des personnes.*

[3] *Les services spécialisés de renseignement, dits du* « premier cercle »*, sont la direction générale de la sécurité extérieure (DGSE) ; la direction du renseignement et de la sécurité de la défense (DRSD) ; la direction du renseignement militaire (DRM) ; la direction générale de la sécurité intérieure (DGSI) ; le service à compétence nationale dénommé* « direction nationale du renseignement et des enquêtes douanières » *(DNRED) ; le service à compétence nationale dénommé* « traitement du renseignement et action contre les circuits financiers clandestins » *(Tracfin). À l'exception de la DRM et de Tracfin, les services du premier cercle ont la faculté de recourir à l'ensemble des techniques de renseignement.*

contrôle des techniques de renseignement (CNCTR), à utiliser des logiciels de traitement de données biométriques ***a posteriori*** afin de **retrouver une personne préalablement identifiée susceptible d'être en lien avec une menace**. Lorsqu'il existerait des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée seraient susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci pourrait également être accordée individuellement pour chacune de ces personnes.

Les **finalités** pour lesquelles cette nouvelle technique de renseignement pourrait être utilisée sont limitativement énumérées. Il s'agirait de la promotion de l'indépendance nationale, l'intégrité du territoire et la défense nationale, la prévention du terrorisme et la prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique.

L'article prévoit plusieurs garanties qui s'appliqueraient à cette nouvelle technique de renseignement :

- **la durée d'autorisation de mise en œuvre serait limitée à un mois**, alors qu'elle est de quatre mois pour la plupart des autres techniques de renseignement ;

- **le caractère d'urgence**, permettant la mise en place de la technique en cas d'avis défavorable de la CNCTR avant la décision du Conseil d'État, **ne pourrait être invoquée que si l'autorisation a été délivrée au titre de la promotion de l'indépendance nationale, de l'intégrité du territoire ou de la défense nationale, de la prévention du terrorisme ou de la prévention des atteintes à la forme républicaine des institutions** ;

- **un nombre maximal d'autorisations serait défini** par arrêté du Premier ministre et celles-ci seraient réparties entre les ministres de tutelle des différents services du premier cercle concernés par la mise en œuvre de la technique.

Enfin, comme pour les autres techniques de renseignement, le service autorisé à recourir à la technique rendrait compte de sa mise en œuvre à **la CNCTR, qui disposerait d'un accès permanent, complet, direct et immédiat aux informations ou aux documents collectés**. Celle-ci pourrait à tout moment adresser une recommandation tendant à ce que les opérations soient interrompues et que les renseignements collectés soient détruits.

1.2. La position de la commission : clarifier les procédures applicables en fonction de l'origine des données traitées

La nouvelle technique de renseignement prévue par l'article 4 de la proposition de loi concernerait les images déjà détenues par les services**, provenant tant des systèmes de vidéoprotection** – les agents des services de renseignement peuvent en effet en être rendus destinataires en application

de l'article L. 252-3 du code de la sécurité intérieure –, **que de la mise en œuvre éventuelle d'autres techniques de renseignement**. La commission a considéré que la rédaction initiale de l'article 4 laissait place à l'ambiguïté, et qu'il convenait de la corriger. Ainsi, l'article poursuit deux objectifs :

- **ouvrir la possibilité d'utiliser *a posteriori* des logiciels de traitement de données biométriques sur les images issues de la vidéoprotection** ;

- **renforcer les exigences pesant sur l'exploitation *a posteriori* des images issues des techniques de renseignement** par le biais de ces mêmes logiciels.

La commission a estimé que **les procédures applicables pour permettre aux services spécialisés de renseignement d'utiliser des logiciels de traitement de données biométriques devaient être distinguées en fonction de la provenance des données**.

S'agissant en premier lieu des **renseignements collectés à la suite de la mise en œuvre de techniques de renseignement**, la commission a prévu, par l'adoption de l'**amendement COM-13** du rapporteur, que **le recours à des logiciels de traitement de données biométriques pour en faciliter l'exploitation devrait être précisé dans la demande d'autorisation de la technique elle-même**, et ce afin d'éviter une double demande d'autorisation pour la collecte puis pour l'exploitation des mêmes données.

S'agissant en second lieu des **images provenant des systèmes de vidéoprotection** dont les agents des services de renseignement peuvent en être rendus destinataires en application de l'article L. 252-3 du code de la sécurité intérieure, la commission a prévu, par l'adoption du **même amendement COM-13**, que les services devront demander l'autorisation au Premier ministre après avis de la commission nationale de contrôle des techniques de renseignement (CNCTR) pour les exploiter grâce à des logiciels d'analyse biométrique, dans le cadre de la nouvelle technique de renseignement prévue par l'article 4. Conformément aux finalités de la vidéoprotection, **cette nouvelle possibilité ne serait ouverte que pour la lutte contre le terrorisme**.

Par l'adoption du **même amendement COM-13**, la commission a également précisé que **les traitements utilisés, que ce soit pour exploiter les renseignements collectés par les techniques de renseignement ou les images issues de la vidéoprotection, devraient répondre aux exigences prévues par l'article 1er *ter* de la proposition de loi**.

La commission a adopté l'article 4 **ainsi modifié**.

CHAPITRE IV
EXPÉRIMENTATION DE TRAITEMENTS DE DONNÉES BIOMÉTRIQUES EN TEMPS RÉEL POUR LUTTER CONTRE LE TERRORISME ET LA GRANDE CRIMINALITÉ
(Division nouvelle)

Afin d'assurer la clarté du texte, la commission a créé une nouvelle division regroupant deux articles consacrés à l'expérimentation de traitements de données biométriques en temps réel pour lutter contre le terrorisme et la grande criminalité (**amendement COM-14** du rapporteur).

Article 5
Recours à des systèmes de reconnaissance biométrique en temps réel, dans un cadre administratif

L'article 5 permettrait de créer un cadre autorisant le recours ciblé et limité dans le temps à des systèmes de reconnaissance biométrique en temps réel, dans un cadre administratif. De fortes garanties entourent le dispositif, puisqu'il ne pourrait être déployé que sur la base d'une menace préalablement identifiée, à des fins de sécurisation des grands évènements face à un risque terroriste ou des risques d'atteinte grave à la sécurité des personnes, sur un nombre limité de caméras dédiées et distinctes de celles des systèmes de vidéoprotection.

Considérant que l'article souffrait de nombreuses faiblesses, la commission l'a profondément remanié, en inscrivant clairement la procédure prévue dans un système robuste ayant fait ses preuves et en l'assortissant des garanties maximales. C'est ainsi que le recours à ces technologies en temps réel serait réservé aux services de renseignement du premier cercle en charge de la sécurité intérieure, afin de lutter contre le terrorisme. Une autorisation du Premier ministre devrait être obtenue, après avis de la commission nationale de contrôle des techniques de renseignement. Cette dernière serait également chargée de contrôler la mise en œuvre de ces technologies et bénéficierait d'un accès permanent, complet, direct et immédiat aux informations ou aux documents collectés ainsi qu'aux signalements générés par les traitements.

1. L'article 5 de la proposition de loi : la création d'une possibilité de recours à des traitements de reconnaissance biométriques dans l'espace public en temps réel pour prévenir des attentats ou des atteintes graves aux personnes

Reprenant une recommandation de la mission d'information sur la reconnaissance biométrique dans l'espace public conduite par les sénateurs Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, l'article 5 de la proposition de loi ouvre une faculté d'utilisation de la reconnaissance biométrique sur la voie publique en temps réel dans un cadre administratif. Les rapporteurs de la mission d'information envisageaient le déploiement de

ce type de dispositif à titre d'exception, « *en vue de* ***sécuriser de grands évènements présentant une sensibilité particulière ou les sites particulièrement sensibles***[1]*. Ces déploiements auraient pour objectif de détecter des personnes d'intérêt afin soit de les écarter si elles font l'objet d'une interdiction de paraître dans le périmètre concerné, soit d'enclencher un dispositif de vigilance si leur présence dans le lieu constitue un motif d'inquiétude* »[2].

Les auteurs de la proposition de loi se sont inspirés pour la rédaction de l'article 5 des dispositifs mis en œuvre au Royaume-Uni par les polices du Pays de Galles et de Londres, où des traitements de données biométriques sont utilisés pour détecter des personnes d'intérêt sur un périmètre géographique limité et pour une période précisément déterminée.

Ainsi, cet article propose de permettre le déploiement, à titre expérimental, de traitements de données biométriques en temps réel dans l'espace public. Il entoure cette possibilité de nombreuses garanties :

- **les finalités seraient précisément définies** : il s'agirait d'assurer la sécurité de grands évènements sportifs, récréatifs et culturels qui, par leur ampleur ou les circonstances de leur déroulement, sont particulièrement exposés à des risques d'actes de terrorisme ou à des risques d'atteintes graves à la sécurité des personnes ;

- les **personnes qu'il s'agirait d'identifier** devraient être « *limitativement et préalablement énumérés* » et faire peser une « *menace grave et immédiate sur l'ordre public* » ;

- ces traitements devraient être déployés sur des images issues de **caméras mobiles distinctes de celles des systèmes de vidéoprotection**, et ce afin de matérialiser le caractère limité du déploiement du dispositif et de garantir la confidentialité de la liste des personnes recherchées, qui ne serait pas transmise aux opérateurs de vidéoprotection. Les personnes pouvant être recherchées dans ce cadre devraient être intégrées au cas par cas pour chaque déploiement, sur la base de la probabilité qu'elles se trouvent sur le lieu concerné ;

- le **périmètre géographique du déploiement du traitement** serait également précisément défini, puisqu'il s'agirait des lieux accueillant les évènements concernés par la menace, de leurs abords, ou sur les voies ou véhicules de transports publics les desservant.

---

[1] ***Plusieurs acteurs demandent un déploiement plus conséquent des dispositifs de reconnaissance faciale en temps réel dans l'espace public****, par exemple en les reliant directement aux dispositifs de vidéoprotection ou encore en les déployant dans d'autres contextes, comme en matière sportive aux abords des stades afin de contribuer à la lutte contre les violences dans le sport et d'améliorer les conditions de sécurité dans les enceintes sportives.* ***Les rapporteurs considèrent cependant qu'un tel déploiement serait à la fois prématuré et disproportionné****.*

[2] La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance, *rapport d'information n° 627 (2021-2022) de Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, déposé le 10 mai 2022. Ce rapport est consultable à l'adresse suivante : https://www.senat.fr/notice-rapport/2021/r21-627-notice.html.*

Le public devrait être informé de l'emploi de ce type de traitements, sauf lorsque les circonstances l'interdiraient ou que l'information entrerait en contradiction avec les objectifs poursuivis. Une information générale du public sur l'emploi de ces traitements devrait être réalisée par le ministère de l'intérieur.

L'article définit ensuite la **procédure d'autorisation de déploiement de ces traitements** : il **réserverait cette possibilité aux officiers de police judicaire, sur autorisation du préfet**, sur la base d'une demande précisant le service responsable des opérations, le ou les motifs de mise en œuvre du traitement, la liste des personnes recherchées, les modalités d'établissement de cette liste ainsi que la justification de la menace pour l'ordre public que les personnes représentent, la justification de la nécessité de recourir au dispositif, permettant notamment d'apprécier la proportionnalité de son usage au regard de la finalité poursuivie, le périmètre géographique concerné, la durée souhaitée de l'autorisation et, le cas échéant, les modalités d'information du public.

La décision d'autorisation devrait être délivrée par le préfet, et préciser :

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

- la manifestation sportive, récréative ou culturelle concernée et les motifs de la mise en œuvre du traitement ;

- le périmètre géographique concerné par la mise en œuvre du traitement, qui **ne pourrait inclure les abords des lieux de culte ou l'itinéraire d'une manifestation déclarée** ;

- les modalités d'information du public, notamment sur ses droits ou, lorsque cette information entre en contradiction avec les finalités poursuivies, les motifs pour lesquels le responsable du traitement en est dispensé ;

- la durée d'autorisation, qui **ne pourrait excéder quarante-huit heures**, renouvelable selon les mêmes modalités lorsque les conditions de sa délivrance continuent d'être réunies.

En sus de cette demande et de cette autorisation très détaillées, l'article prévoit une garantie supplémentaire permettant de limiter le périmètre géographique du traitement : **le nombre maximal de caméras sur lesquels pourraient être mis en œuvre ces traitements de manière simultanée serait fixé par département, par arrêté du ministre de l'intérieur**.

Enfin, l'article prévoit un **régime de traçabilité des signalements** et de **redevabilité des services mettant en œuvre le traitement au préfet et du préfet à la CNIL**.

2. La position de la commission : un dispositif intéressant qu'il convient d'inscrire clairement dans un cadre administratif en l'assortissant de garanties maximales

La commission est favorable à l'introduction d'un dispositif de d'identification biométrique dans l'espace public en temps réel dans un cadre administratif de manière exceptionnelle car, bien que consciente qu'il s'agit du cas d'usage soulevant le plus d'interrogations, il s'agit du cas potentiellement le plus utile pour sécuriser un grand évènement face à un risque grave et imminent d'attentat.

Elle a cependant considéré que **l'article 5, tel que rédigé par les auteurs de la proposition de loi, souffrait de plusieurs faiblesses** :

- en premier lieu, **l'article n'inscrit pas clairement le dispositif dans un cadre administratif** puisqu'il réserve son utilisation aux officiers de police judiciaire ;

- en deuxième lieu, il attribue un **pouvoir étendu d'autorisation aux préfets**, qui seront cependant démunis pour apprécier la pertinence de recours à ces technologies faute de disposer des éléments suffisants pour évaluer eux-mêmes la situation. Par ailleurs, certains services de renseignement pourraient être réticents à leur transmettre la liste des personnes qu'ils veulent suivre. De même, l'information prévue du public irait nécessairement à l'encontre des objectifs poursuivis, dès lors que l'usage de ce type de traitement serait réservé aux cas les plus graves ;

- ce d'autant plus qu'en troisième lieu, **les décisions des préfets sont soumises au contrôle des tribunaux administratifs**, devant lesquels le principe du contradictoire doit être entièrement respecté – et ce alors que l'action des services de renseignement relève habituellement du contrôle d'une formation spécifique du Conseil d'État, habilité au secret de la défense nationale.

La commission a en conséquence, par l'adoption de **l'amendement COM-15** du rapporteur, profondément remanié l'article 5, en **inscrivant clairement la procédure prévue dans un cadre administratif et en l'assortissant des garanties maximales**.

Pour ce faire, la commission a d'abord **réservé l'utilisation** de la reconnaissance biométrique en temps réel dans l'espace public en matière administrative **aux services de renseignement du premier cercle en charge de la sécurité intérieure, à la seule fin d'assurer la prévention du terrorisme**.

Elle a également choisi d'appliquer à cette utilisation le régime robuste éprouvé depuis maintenant huit ans d'autorisation du Premier ministre après avis de la commission nationale de contrôle des techniques de renseignement (CNCTR), permettant que le déploiement de ces technologies soit **placé en permanence sous le contrôle de la CNCTR et du Conseil d'État**.

La commission a également précisé que le déploiement de ces technologies devait être **strictement subsidiaire**, l'autorisation ne pouvant être accordée que si le service ne peut employer d'autres moyens moins intrusifs ou que l'utilisation de ces autres moyens serait susceptible d'entraîner des menaces graves pour l'intégrité des agents.

Ainsi, le déploiement de ces traitements devrait faire l'objet d'une autorisation du Premier ministre pris après avis de la CNCTR. Le recours à cette technique ne pourrait être autorisé que pour une **durée de 48 heures**, renouvelable dans les mêmes conditions de durée s'il est établi que le recours à ces traitements demeure le seul moyen d'atteindre la finalité poursuivie.

Un **nombre maximal d'autorisations** pouvant être en vigueur simultanément serait défini par le Premier ministre, après avis de la CNCTR.

Le champ géographique du déploiement n'a pas été modifié par la commission, de même que le **recours à des caméras distinctes de celles des systèmes de vidéoprotection**, ce qui constitue deux garanties complémentaires importantes.

Par l'adoption du **même amendement COM-15** du rapporteur, la commission a également précisé que **les traitements utilisés devraient répondre aux exigences prévues par l'article 1er *ter* de la proposition de loi**.

La commission a adopté l'article 5 **ainsi modifié**.

Article 6

Expérimentation de logiciels de reconnaissance biométrique en temps réel dans le cadre d'enquêtes judiciaires

L'article 6 propose d'autoriser l'utilisation, à titre expérimental, de traitements de reconnaissance biométriques en temps réel dans le cadre de certaines enquêtes judiciaires. Compte tenu des risques élevés induits par l'usage en temps réel de cette technologie pour les libertés publiques, la commission l'a adopté mais limité aux enquêtes portant sur des infractions limitées et d'une extrême gravité : les actes de terrorisme, les atteintes aux intérêts fondamentaux de la nation, les crimes et délits relatifs à la grande criminalité organisée et les disparitions de personnes mineures. Elle l'a également assorti d'un niveau maximal de garantie, en particulier en réservant son usage aux officiers de police judiciaire et en confiant au seul juge des libertés et de la détention le soin de procéder au renouvellement des autorisations d'utilisation accordées.

1. L'article 6 de la proposition de loi : l'expérimentation de logiciels de reconnaissance biométrique en temps réel pour certaines enquêtes judiciaires

Dans un rapport d'information de mai 2022, Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain[1], ont **ouvert la voie à une expérimentation de l'usage de traitements d'identification biométrique en temps réel dans l'espace public**. Ils ont notamment relevé le bénéfice que pouvait apporter cette technologie pour certaines enquêtes déterminées, tout en insistant sur les risques associés pour l'exercice des libertés publiques et la nécessité d'accompagner son utilisation d'un haut niveau de garanties. Ils relevaient ainsi que « *le déploiement de tels dispositifs pourrait permettre, d'une part, le suivi d'une personne venant de commettre une infraction grave en temps réel sur la base de ses données biométriques à partir des images issues de la vidéoprotection afin d'en faciliter l'interpellation et, d'autre part, la recherche dans un périmètre géographique et temporel limité, des auteurs d'infractions graves recherchés par la justice ou des personnes victimes d'une disparition inquiétante* ».

L'article 6 de la proposition de loi est la traduction législative de cette recommandation. Il **autorise, à titre expérimental, le recours à des traitements de reconnaissance biométrique en temps réel par des officiers ou des agents de police judiciaire, sous le contrôle d'un magistrat, dans des situations limitativement énumérées**. Il s'agit des cas où une telle opération est exigée par les nécessités :

- d'une enquête ou d'une instruction portant sur **un acte de terrorisme, des faits de trafic d'armes ou d'explosifs, ou relative à une atteinte à l'intégrité des personnes punies d'au moins trois ans d'emprisonnement** ;

- d'une procédure d'enquête ou d'instruction de **recherche d'une personne en fuite ou des causes de la mort ou de la disparition**.

Les auteurs de la proposition de loi ont assorti cette expérimentation d'un **nombre significatif de garanties** tenant tout d'abord à l'origine des données exploitées. Il est prévu que les images utilisées soient collectées « *au moyen de **caméras dédiées et distinctes de celles des systèmes de vidéoprotection*** ». Une garantie significative tient également au fait que la reconnaissance faciale ne pourrait être utilisée qu'aux fins d'identifier « ***des personnes limitativement et préalablement énumérées*** », ce qui interdit explicitement toute identification « à la volée » des personnes apparaissant sur les images collectées.

---

[1] La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance, *rapport d'information n° 627 (2021-2022) de Marc Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, déposé le 10 mai 2022. Ce rapport est consultable à l'adresse suivante : https://www.senat.fr/notice-rapport/2021/r21-627-notice.html*.

L'utilisation des logiciels de reconnaissance biométrique est ensuite soumise à **un strict régime d'autorisation**. Celle-ci serait accordée, selon les cas, par le procureur de la République chargé du dossier pour une durée maximale de **24 heures**, ou, dans le cas de procédures d'instruction ou d'information pour recherche des causes de la mort ou de la disparition, par le juge d'instruction chargé du dossier pour une durée maximale de **48 heures**. Dans les deux cas, la décision d'autorisation devrait mentionner « *tous les éléments permettant d'identifier les lieux et les personnes concernées* », ainsi que la durée de l'autorisation. Son renouvellement supposerait une décision expresse et motivée. Cette décision, qui n'aurait pas de caractère juridictionnel, serait par ailleurs versée au dossier de la procédure.

Ces traitements seraient également **mis en œuvre sous l'autorité et le contrôle du magistrat qui les a autorisés**, lequel pourrait ordonner à tout moment leur interruption. Les correspondances éventuellement signalées entre la personne recherchée et une personne présente sur les images ne pourraient fonder, en elles-mêmes, aucune décision individuelle ni poursuites automatisées. Les signalements seraient ainsi systématiquement suivis d'un **contrôle humain par des agents qualifiés et habilités de la police et de la gendarmerie nationales**.

L'utilisation de ces traitements serait ensuite indissociable de « ***l'existence et de la robustesse d'un système de contrôle humain*** » ainsi que de la mise en place d'un **système de gestion des risques** visant notamment à détecter ou corriger les éventuels biais de l'algorithme.

La traçabilité des opérations effectuées serait quant à elle assurée par la rédaction d'un procès-verbal[1] mentionnant les signalements générés et les suites leur ayant été apportées, ainsi que la date et l'heure du début et de la fin des opérations. Par ailleurs, les enregistrements seraient placés sous scellés fermés, tandis qu'un second procès-verbal, versé au dossier, décrirait les données utiles à la manifestation de la vérité. La conservation de séquences relatives à la vie privée étrangères au dossier est par ailleurs explicitement prohibée.

Les données collectées seraient effacées à la clôture de l'enquête et, en tout état de cause, à l'issue d'une période de trois ans. Par exception, elles seraient concernées 20 ans pour les procédures de recherche des causes de la disparition n'ayant pas abouti. Les opérations de destruction correspondantes feraient l'objet d'un procès-verbal.

S'agissant du fonctionnement du traitement, il est prévu que celui-ci ne puisse signaler la probabilité d'une correspondance qu'une fois les opérations de rapprochement achevées.

---

[1] *Par* « le procureur de la République, le juge d'instruction ou l'officier de police judiciaire commis par lui ou requis par le procureur de la République, ou l'agent de police judiciaire agissant sous sa responsabilité ».

Enfin, ces traitements devraient être autorisés par décret en Conseil d'État pris après avis de la CNIL.

2. La position de la commission : réserver l'expérimentation aux infractions d'une extrême gravité et prévoir un niveau maximal de garanties

Alors que le Gouvernement a officiellement fermé la porte à toute expérimentation de l'usage de la reconnaissance faciale dans l'immédiat, en particulier s'agissant des usages en temps réel, **la commission a estimé qu'il était utile d'ouvrir ce débat.**

Le progrès technologique est par nature ambivalent et ne pas légiférer exposerait au risque de subir le développement anarchique d'une technologie dont les bénéfices potentiels sont réels, à la condition que son usage soit rigoureusement encadré. Comme le mentionnaient les députés Philippe Gosselin et Philippe Latombe dans un rapport d'information d'avril 2023[1], « *la création d'un cadre juridique qui autorise la reconnaissance faciale apparaît* [d'une part] ***indispensable afin de ne pas se priver d'un outil essentiel pour améliorer la sécurité de nos concitoyens*** » ledit cadre doit, d'autre part, « ***comporter des garanties juridiques solides pour tenir compte des fortes réticences exprimées par une partie de la société*** ».

La commission a donc **souscrit à la démarche des auteurs de la proposition de loi, tout en s'attachant**, par l'adoption d'un **amendement COM-16** du rapporteur, **à combler les angles morts de l'article 6 et à renforcer encore davantage les garanties proposées**[2].

La commission a tout d'abord limité le champ de l'expérimentation de traitements d'identification biométriques en temps réel dans un cadre judiciaire aux enquêtes et instructions portant sur **des faits d'une extrême gravité**. Suivant les préconisations formulées par les députés Philippe Gosselin et Philippe Latombe dans leur rapport précité, elle n'a ainsi autorisé le recours à ces dispositifs que dans le cadre des investigations relatives :

- à des actes de **terrorisme** ;

- à des **atteintes aux intérêts fondamentaux de la nation** ;

---

[1] *Les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité, Assemblée nationale, rapport d'information n° 1089 (2022-2023) de Philippe Gosselin et Philippe Latombe, déposé le 12 avril 2023. Ce rapport est consultable à l'adresse suivante :*
https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information#_Toc256000052

[2] *La commission ayant fait le choix d'appliquer un certain nombre de garanties à l'ensemble des traitements expérimentés, les dispositions prévoyant que l'identité des personnes ne peut apparaître qu'à l'issue des opérations de rapprochement, l'existence d'un système de contrôle humain et de gestion des risques, l'impossibilité de fonder une décision individuelle sur le seul signalement d'une correspondance ou le recours à un décret en Conseil d'État pris après avis de la CNIL pour autoriser les traitements ont été transférées à l'article 1er ter de la proposition de loi (voir commentaire) mais demeurent applicables aux traitements régis par l'article 6.*

- à des infractions relatives à la **grande criminalité organisée** et relevant de la compétence de la juridiction nationale chargée de la lutte contre la criminalité organisée ;

- à la **disparition d'une personne mineure**.

La commission n'a en revanche pas retenu la proposition selon laquelle l'autorisation d'utiliser ces traitements biométriques devrait être requise par un magistrat du parquet et accordée par un magistrat du siège. Alors que les enquêtes et instruction visées sont caractérisées par des degrés élevés d'urgence, ce dispositif aurait en effet pu porter amoindrir l'opérationnalité du dispositif. Cet impératif de célérité disparaissant une fois le dispositif déployé, la commission a en revanche **considéré qu'il revenait au seul juge des libertés et de la détention de se prononcer sur un éventuel renouvellement de l'autorisation initiale.**

La commission a également **clarifié les finalités du dispositif** en alignant celles-ci sur les autres cas d'usage expérimentés, à savoir le rassemblement des preuves des infractions et l'identification de leurs auteurs ou la recherche d'une personne mineure disparue. La mise en œuvre de ces traitements biométriques a également été conditionnée à **l'application d'un strict principe de subsidiarité**. Enfin, la commission a limité le champ des utilisateurs de ces traitements de reconnaissance biométriques aux **seuls officiers de police judiciaire.**

La commission a adopté l'article 6 **ainsi modifié**.

Article 7 (supprimé)

Mise en place d'un régime parlementaire de contrôle renforcé

L'article 7 prévoyait la mise en place d'un régime de contrôle renforcé par le Parlement : un rapport annuel devait lui être remis par le Gouvernement, l'Assemblée nationale et le Sénat devaient être informés en temps réel des mesures prises dans un cadre administratif, et le Parlement devait pouvoir requérir toute information complémentaire du Gouvernement dans le cadre de l'évaluation de ces mesures.

Par coordination avec l'intégration du contenu de cet article dans le nouvel article 1er *bis* de la proposition de loi, **la commission a supprimé cet article** par l'adoption de l'**amendement COM-17** du rapporteur.

La commission a **supprimé** l'article 7.

Article 8 (supprimé)
Définition du cadre de l'expérimentation

L'article 8 prévoyait que les mesures définies aux articles 2 à 6 soient prises à titre expérimental, pour une durée de 3 ans à compter de la promulgation de la loi. Il prévoyait également qu'un comité scientifique et éthique serait chargé d'évaluer régulièrement l'application de ces mesures et ses rapports, rendus publics, seraient transmis au Parlement. Enfin, un rapport final d'évaluation devait être réalisé par le Gouvernement, appréciant l'application des mesures prévues par la proposition de loi et l'opportunité de les pérenniser ou de les modifier, notamment au vu de l'évolution du droit de l'Union européenne en la matière

Par coordination avec l'intégration du contenu de cet article dans le nouvel article 1er *bis* de la proposition de loi, **la commission a supprimé cet article** par l'adoption de l'**amendement COM-18** du rapporteur.

La commission a **supprimé** l'article 8.

CHAPITRE V
DISPOSITIONS RELATIVES À L'OUTRE-MER
(Division nouvelle)

Afin d'assurer la clarté du texte, la commission a créé une nouvelle division relative à l'application de la proposition de loi dans les territoires ultramarins, en adoptant un **amendement COM-19** du rapporteur.

Article 9
Application de la proposition de loi dans les territoires ultramarins

L'article 9 prévoit que l'ensemble des dispositions de la proposition de loi seront applicables sur l'ensemble du territoire national, qu'il s'agisse des dispositions insérées dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, soit les articles 1er et 2 (deux premiers alinéas de l'article), de celles insérées dans le code de la sécurité intérieure, soit l'article 4 (alinéa 3 de l'article 9), de celles insérées dans le code de procédure pénale, soit l'article 3 (alinéas 4 et 5), et de celles non codifiées, soit les articles 1er *bis*, 1er *ter*, 5 et 6 (alinéa 6).

La commission a adopté l'article 9 **sans modification**.

EXAMEN EN COMMISSION

_____

MERCREDI 31 MAI 2023

M. François-Noël Buffet, président. – Nous examinons la proposition de loi relative à la reconnaissance biométrique dans l'espace public, déposée par Marc-Philippe Daubresse, Arnaud de Belenet et plusieurs de leurs collègues.

M. Philippe Bas, rapporteur. – La reconnaissance faciale sans consentement dans l'espace public est un sujet difficile. Nul besoin de s'attarder sur les dangers réels de cette technologie en matière d'atteinte à la vie privée, sur les risques de développement d'une société de surveillance à la chinoise ou encore sur les erreurs possibles d'identification. Pourtant, cette technologie présente des avantages dont il serait dommage de se priver définitivement. Elle permet notamment de prévenir des attentats ou encore de retrouver des criminels.

Un régime d'interdiction absolue serait vain : les usages privés se développent sur les téléphones portables, les frontières sont ouvertes et nous subirions une perte de chances pour atteindre les objectifs précités. À l'inverse, une liberté totale serait synonyme de contrôle social, voire d'un système de crédit social, comme on le voit en Chine, mais aussi d'abus de pouvoir par une utilisation non réglementée du dispositif.

Cette proposition de loi fait suite au très intéressant rapport d'information de Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, que nous avons adopté à l'unanimité en mai 2022. Il visait à éviter tout développement anarchique de la technologie en posant un principe général d'interdiction, tout en l'expérimentant pour des finalités précises et en l'encadrant par des procédures inscrites dans la loi.

Nous disposons sur cette thématique d'un rapport de la Commission nationale de l'informatique et des libertés (CNIL) de 2019, d'un projet de règlement européen en cours d'examen par le Parlement européen, d'un rapport remis au Premier ministre en septembre 2021 par le député Jean-Michel Mis et, plus récemment, d'un rapport d'information des députés Philippe Gosselin et Philippe Latombe.

Il y a donc une effervescence autour de ce sujet, que nous avons abordé lors de l'examen du texte relatif aux jeux Olympiques et Paralympiques de 2024. Nous avions alors adopté une seule disposition faisant appel à l'intelligence artificielle : celle qui permet de détecter par vidéosurveillance un mouvement de foule, l'abandon d'un objet ou d'un colis ou encore l'irruption de personnes masquées dans une manifestation, sans traitement de données biométriques. À l'époque, nous n'avons pas

souhaité instaurer un dispositif de reconnaissance faciale. Après des échanges entre le président du Sénat et la CNIL, mais aussi en séance publique avec le Gouvernement, il a été jugé préférable de traiter la question globalement, et non à l'occasion de la discussion d'un autre texte. Tel est l'objet de cette proposition de loi.

En tant que rapporteur, je salue l'accompagnement que m'ont offert les auteurs de la proposition de loi dans ma découverte de l'étendue des implications de ce dossier. Je leur ai par ailleurs soumis tous mes amendements, pour m'assurer que nous travaillions dans le même sens.

J'ai souhaité répartir différemment les dispositions du texte, afin de créer un bloc précisant l'ensemble des garanties que nous voulons apporter et l'ensemble des interdits que nous voulons poser. Ainsi, nous refusons que la reconnaissance faciale soit utilisée à des fins de notation des individus, par exemple ceux qui traversent toujours dans les clous et qui, comme on le voit en Chine, pourraient réserver des chambres d'hôtel sans dépôt de garantie. Non à la catégorisation de nos concitoyens, à la création de groupes et de sous-ensembles !

Nous voulons interdire l'identification à distance sans consentement. L'utilisation de la reconnaissance faciale doit passer exclusivement par des dispositions législatives et non réglementaires. Nous demandons que chaque logiciel d'intelligence artificielle permettant de procéder à une reconnaissance faciale soit calibré très précisément par décret et que ce décret soit précédé d'un avis de la CNIL ou de la Commission nationale de contrôle des techniques de renseignement (CNCTR) et passe devant le Conseil d'État. Par ailleurs, nous exigeons que l'exploitation des données issues de la reconnaissance faciale donne lieu à une intervention humaine et qu'il n'y ait pas d'automatisme. L'interpellation d'un individu pour acte de terrorisme, par exemple, est, par nature, potentiellement musclée. Il ne faudrait pas qu'elle ne soit due qu'au résultat d'un logiciel…

Après ce socle minimal de garanties, le régime de contrôle et d'autorisation ou encore le rôle du Parlement, nous définissons les usages possibles de cette technologie. Comme nous n'en avons pas encore l'expérience, nous jugeons qu'une expérimentation est nécessaire. Sauf intervention nouvelle du législateur, l'expérimentation cessera au bout de trois ans, suivant une clause « d'autodestruction » que nous connaissons bien. Nous demandons naturellement que le Parlement soit précisément informé des résultats de cette expérimentation.

J'ai ensuite proposé de distinguer, d'une part, les usages en matière de renseignement pour l'action des services spéciaux et, d'autre part, les usages dans le cadre des enquêtes judiciaires. Deux types de démarche sont à noter : l'utilisation des images *a posteriori* et leur utilisation en temps réel, la seconde posant davantage d'interrogations.

En matière de renseignement, une disposition prévoyait, dans le texte initial, que les auxiliaires de l'organisation de grands événements puissent faire l'objet, lorsqu'ils vont dans des endroits précis, d'un accès au site contrôlé sur la base de leurs données biométriques. Je propose de confier cette responsabilité non pas à l'organisateur de l'événement, mais à l'État. Par ailleurs, les riverains ne seraient pas soumis à cette modalité d'accès sans leur accord.

Je propose par ailleurs de clarifier que l'utilisation *a posteriori* par les services de renseignement du premier cercle de logiciels de reconnaissance biométrique sur des images de voie publique issues de la vidéoprotection, en vue de repérer la présence de personnes dangereuses, sera circonscrite à la prévention d'attentats terroristes.

Enfin, pour le cas où les services de sécurité souhaiteraient appliquer en temps réel, sur des caméras dédiées, un logiciel de reconnaissance faciale, je souhaite que le régime de la décision et de la garantie relève du Premier ministre. Pour que la garantie soit maximale, je propose d'appliquer le régime robuste et reconnu des techniques de renseignement, tout en réservant cet usage à la direction générale de la sécurité intérieure (DGSI).

La reconnaissance faciale doit bénéficier d'un régime semblable à celui qui s'applique lorsque l'on pose une balise sous une voiture ou un micro dans un appartement, ou que l'on saisit en temps réel des données figurant dans un ordinateur. Pour rappel, ce régime prévoit l'avis de la CNCTR ; le Premier ministre prend la décision, et si l'avis n'est pas conforme, le Conseil d'État se prononce en formation non publique. Pour la mise en œuvre en temps réel de ces logiciels, je propose donc d'adopter ce régime de protection maximal.

Nous avons également posé le principe de subsidiarité : la technique de reconnaissance faciale ne saurait être utilisée qu'après épuisement de toutes les chances d'identifier quelqu'un par d'autres moyens ou technologies.

Pour les enquêtes judiciaires, j'ai raisonné par analogie et vous propose de réserver l'utilisation de la reconnaissance faciale à la lutte contre le terrorisme, aux crimes les plus graves, pour rechercher un enfant enlevé ou encore un criminel en fuite. Il faut qu'une autorisation expresse de l'autorité judiciaire soit requise, que le principe de subsidiarité soit appliqué, que les officiers de police judiciaire soient spécialement formés et habilités à utiliser cette technologie et que, pour l'utilisation en temps réel, le juge des libertés et de la détention se prononce en cas de renouvellement au-delà de quarante-huit heures.

En application du vade-mecum sur l'application des irrecevabilités au titre de l'article 45 de la Constitution, le périmètre indicatif de la proposition de loi pourrait comprendre les modalités d'utilisation des dispositifs de reconnaissance biométrique à des fins d'authentification,

d'identification dans un cadre judiciaire et d'identification dans un cadre administratif.

Il en est ainsi décidé.

M. Marc-Philippe Daubresse. – En vous remerciant de nous avoir confié cette mission l'an dernier, je dois vous dire, après trente et un ans de mandat parlementaire, que ce dispositif législatif est le plus compliqué auquel j'ai eu à faire face.

Avec mes deux corapporteurs, nous avons ajouté à notre rapport d'information le sous-titre « Trente propositions pour écarter le risque d'une société de surveillance ». C'est donc à juste titre que, lorsque j'ai présenté un amendement à l'occasion de la loi relative aux jeux Olympiques et Paralympiques de 2024, mes collègues ont suggéré qu'une proposition de loi serait préférable pour aller au fond de ce sujet. J'ai donc retiré mon amendement et nous avons associé Jérôme Durain à notre travail d'élaboration de la proposition de loi.

Dans notre rapport très fouillé, nous étions arrivés à la conclusion que, compte tenu du changement d'échelle des technologies biométriques, un encadrement législatif était nécessaire. Nous ne disposions alors, comme cadre juridique, que du règlement général sur la protection des données (RGPD) et d'un projet de directive européenne. Nous risquions d'être soumis, à l'insu de notre plein gré et sans avoir notre mot à dire, à des législations supranationales, comme nous le sommes sur d'autres sujets d'ailleurs.

C'est donc dans cet état d'esprit que nous avons abordé la rédaction de cette proposition de loi, en posant quatre interdictions et trois principes généraux. Nous avons commencé par édicter les lignes rouges, considérant qu'on ne pouvait raisonner, pour les exceptions, qu'usage par usage. De fait, la version initiale de la proposition de loi pouvait donner l'impression que l'on donnait une place égale au principe des lignes rouges et à leurs exceptions.

Les amendements du rapporteur, auxquels nous avons été associés, bouleversent l'architecture formelle du texte, mais ne modifient pas la logique dans laquelle nous avons souhaité nous inscrire. Les choses sont remises à leur place : les lignes rouges et les interdits sont posés en premier, selon une démarche dont nous devrons nous inspirer dans le prochain examen du texte sur l'intelligence artificielle.

La reconnaissance biométrique sert à l'identification et à l'authentification. Elle peut s'appliquer en temps différé et en temps réel. Tout cela nécessite une présence humaine. Quant à l'utilisation en temps réel, exception parmi les exceptions, elle ne peut se concevoir que si elle est assortie de garanties extrêmement renforcées.

Les propositions du rapporteur respectent complètement la logique de notre rapport. Elles améliorent nettement notre texte en posant beaucoup plus clairement les interdits et en prévoyant des exceptions, usage par usage, avec des garanties renforcées.

La souveraineté française en matière numérique est en danger. Deux des leaders du marché mondial, Thales et Idemia, sont en effet français. Or faute de législation claire en France, toute une série de technologies est en train de partir à l'étranger. À terme, nous risquons une perte de souveraineté numérique, comme nous en avons connu dans d'autres domaines.

En conclusion, nous soutiendrons les amendements du rapporteur, y compris les dispositions relatives à l'expérimentation. Ils s'inscrivent totalement dans la philosophie de notre proposition.

M. Arnaud de Belenet. – Permettez-moi d'exprimer ma gratitude à l'égard des membres de la commission qui nous ont confié cette mission, ainsi qu'à l'égard du rapporteur. En repositionnant de manière très explicite un interdit majeur, ce dernier nous permet de faire un grand pas législatif : nous ne voulons pas d'une société de surveillance. Le rapporteur a par ailleurs rehaussé les garanties relatives à l'expérimentation.

J'adresse également ma gratitude à Marc-Philippe Daubresse et Jérôme Durain pour notre travail en commun. Cette mission restera pour moi l'un des grands souvenirs de ce mandat et me donne le sentiment d'avoir été utile. Cranter cet interdit et l'écrire dans la loi de manière durable n'est pas seulement nécessaire, cela constitue un marqueur civilisationnel. C'est le signe d'un choix politique de société comme nous en faisons rarement. Habituellement, nous excellons dans la technique juridique ; là, nous faisons un choix politique très clair. J'espère que ce texte pourra prospérer à l'Assemblée nationale.

Sur le fond, tout a été dit. En matière d'expertise, nos entreprises doivent être au rendez-vous. Il faut aussi que l'État maîtrise ces technologies pour pouvoir exercer son contrôle légitime et protéger nos libertés publiques.

M. Jérôme Durain. – Je voudrais saluer le compagnonnage amical qui m'a uni à mes deux corapporteurs Marc-Philippe Daubresse et Arnaud de Belenet dans l'élaboration du rapport d'information, ainsi que le travail du rapporteur Philippe Bas sur cette proposition de loi, qui améliore encore le texte. Pour autant, le groupe Socialiste, Écologiste et Républicain ne votera pas en faveur de la proposition de loi, non pas que je m'oppose à la nécessité de dresser l'inventaire des garanties et de les renforcer, mais pour des raisons de calendrier et d'agenda politique.

Nous sommes en effet dans une forme d'entre-deux, entre un rapport qui a été remis en amont des jeux Olympiques et au sortir d'un débat sur la préparation de cet événement au cours duquel les uns et les autres, y compris des ministres, ont renoncé à la reconnaissance faciale, jugeant

qu'elle n'était pas nécessaire. Des réactions dans l'opinion nous font sentir également à quel point le débat opposant liberté et sécurité est permanent. À Dijon, un système de vidéosurveillance a permis d'envoyer au domicile de chaque « délinquant » une amende pour avoir osé taper sur une casserole, tandis qu'à Matignon, une personne chargée de mettre en œuvre les techniques de renseignement validait inopinément 300 techniques de renseignement…

Nos libertés sont toujours fragiles. J'ai trop de respect pour le travail, l'honnêteté intellectuelle et la rigueur de mes collègues pour dire que nous allons verser dans le capitalisme de surveillance ou dans le contrôle social à la chinoise. Malgré tout, alors que des oppositions se sont exprimées, alors que nous aurons très prochainement un débat sur la réglementation européenne sur l'intelligence artificielle, alors que les crispations dans la société sont importantes sur ces sujets, le vecteur de la proposition de loi ne nous paraît pas être le meilleur.

J'avoue avoir été touché par l'intervention du secrétaire général de la CNIL lors de son audition devant notre commission. Ce dernier, se montrant peu favorable au développement de la reconnaissance faciale, a utilisé des termes assez forts, pointant la différence entre le moment où les systèmes n'existent pas et le moment où ils existent, ou en rappelant que choisir d'expérimenter, c'est choisir de créer. En résumé, prenons garde à l'effet cliquet.

Nous devrons aller au bout de nos réflexions sur la reconnaissance faciale, sans exagérer sur l'indignité de la technique – tout le monde devrait sinon renoncer à utiliser son téléphone – ni sur son éloge immodéré, certains services de renseignement reconnaissant eux-mêmes que ce n'est pas de la reconnaissance faciale dont ils ont besoin.

N'oublions pas non plus que le sujet dépasse le domaine strictement régalien. À la fin des fins, la reconnaissance faciale est aussi faite pour vendre du chocolat dans les aéroports ! Tenons compte aussi de la dimension commerciale. Il faut une large appropriation citoyenne de ce sujet éminemment complexe.

Mme Agnès Canayer. – Je me félicite de cette proposition de loi, que je soutiendrai et qui me paraît d'autant plus équilibrée après les apports du rapporteur. Le sujet était déjà sous-jacent lors de l'examen de la loi sur le renseignement et le terrorisme ou, plus récemment, de la loi sur les jeux Olympiques et Paralympiques. Il avait alors été considéré que ce n'était ni le bon moment ni le bon texte et qu'il fallait se recentrer sur la vidéoprotection intelligente en vue de l'organisation de grands événements à venir.

Je me félicite de ce débat. La menace existe et les techniques évoluent. Il faut trouver le juste équilibre entre les moyens à donner à la sécurisation et la garantie des libertés individuelles.

EXAMEN DES ARTICLES

Division additionnelle avant l'article 1er

M. Philippe Bas, rapporteur. – L'amendement COM-3 introduit un nouveau chapitre relatif aux garanties permettant de faire obstacle à une société de surveillance.

L'amendement COM-3 est adopté.

Article 1er

M. Philippe Bas, rapporteur. – Cet article fondamental pose l'interdit du traitement des données biométriques aux fins d'identifier une personne à distance dans l'espace public.

L'amendement COM-4 prévoit qu'il ne peut être dérogé à cet interdit que pour des motifs d'une exceptionnelle gravité, dans des conditions expérimentales, pour des finalités limitativement énumérées et selon un régime d'autorisation préalable, dont l'exécution est assortie d'un contrôle par des autorités indépendantes du service habilité à l'exploitation de la technologie. Le recours à ces dérogations doit aussi obéir aux principes de nécessité et de proportionnalité.

L'amendement COM-4 est adopté.

L'article 1er est adopté dans la rédaction issue des travaux de la commission.

Après l'article 1er

M. Philippe Bas, rapporteur. – L'amendement COM-5 tend à fixer le régime de l'expérimentation : au terme d'une durée de trois ans, les dispositions deviennent caduques. L'Assemblée nationale et le Sénat sont régulièrement informés. La CNCTR publie chaque année les éléments relatifs à l'utilisation de la technologie de reconnaissance faciale par les services de renseignement. Enfin, comme c'est l'usage, le Gouvernement nous saisit d'un bilan, six mois avant la fin de l'expérimentation.

L'amendement COM-5 est adopté et devient article additionnel.

M. Philippe Bas, rapporteur. – L'amendement COM-6 vise à encadrer les logiciels qui seront mis en œuvre pour le traitement des images par reconnaissance biométrique. Le traitement doit indiquer le degré de probabilité de l'identification d'une personne. Il ne peut fonder par lui-même aucune décision individuelle – une intervention humaine est requise – et ne peut faire l'objet de rapprochements ou d'interconnexions avec d'autres traitements de données à caractère personnel. Cela va mieux en le disant.

Les logiciels de traitement devront être développés par l'État ou sous son contrôle, dans les conditions définies dans la loi du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses

autres dispositions. Ils sont autorisés par des décrets en Conseil d'État, pris après avis de la CNIL ou de la CNCTR et accompagnés d'une analyse d'impact, dont le contenu est clairement défini. Enfin, les images sont détruites à l'expiration d'un certain délai.

L'amendement COM-6 est adopté et devient article additionnel.

M. Philippe Bas, rapporteur. – L'amendement COM-7 vise à améliorer le degré de connaissance réciproque sur ces technologies entre l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) et la CNIL. Il est proposé qu'un membre de la CNIL siège au sein de chacune de ces deux autorités et qu'un membre de chacune de ces deux autorités siège au sein de la CNIL.

L'amendement COM-7 est adopté et devient article additionnel.

Division additionnelle avant l'article 2

M. Philippe Bas, rapporteur. – L'amendement COM-8 vise à introduire un nouveau chapitre relatif à l'expérimentation de dispositifs d'authentification biométrique sans consentement pour l'accès à certains grands évènements.

L'amendement COM-8 est adopté.

Article 2

M. Philippe Bas, rapporteur. – L'amendement COM-9 tend à encadrer les systèmes d'authentification biométrique sans consentement mis en place à l'article 2 lors de certains grands événements. Cette disposition permet de contrôler l'accès des auxiliaires de l'organisation au moyen de la reconnaissance biométrique. Les personnes concernées seraient informées, au moment de leur recrutement, de cette modalité.

L'amendement COM-9 est adopté.

L'article 2 est adopté dans la rédaction issue des travaux de la commission.

Division additionnelle avant l'article 3

M. Philippe Bas, rapporteur. – L'amendement COM-10 vise à introduire un nouveau chapitre relatif à l'utilisation de traitements de données biométriques *a posteriori* dans le cadre d'enquêtes judiciaires ou en matière de renseignement.

L'amendement COM-10 est adopté.

Article 3

M. Philippe Bas, rapporteur. – L'amendement COM-11 limite l'usage de logiciels de reconnaissance biométriques *a posteriori* dans un cadre judiciaire aux seules enquêtes portant sur des infractions particulièrement

graves. Il prévoit également que l'usage de ces logiciels devra être explicitement et préalablement autorisé par le magistrat en charge de l'enquête.

L'amendement COM-11 est adopté.

L'article 3 est adopté dans la rédaction issue des travaux de la commission.

Avant l'article 4

M. Philippe Bas, rapporteur. – L'amendement COM-12 tend à autoriser les services de la police nationale et de la gendarmerie nationale à avoir recours *a posteriori* à un module de reconnaissance biométrique afin d'identifier des personnes mises en cause, faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou disparues, au sein de fichiers d'antécédents judiciaires.

L'amendement COM-12 est adopté et devient article additionnel.

Article 4

M. Philippe Bas, rapporteur. – L'amendement COM-13 prévoit que, lorsque l'exploitation des données issues de la mise en œuvre d'une technique de renseignement peut faire appel à la technologie de reconnaissance biométrique, la demande d'autorisation mentionne expressément cette possibilité. Il s'agit d'éviter la double autorisation.

L'amendement réserve en conséquence la nouvelle technique de renseignement créée, permettant d'utiliser *a posteriori* des logiciels de reconnaissance biométrique sur les images issues de la vidéoprotection, à la lutte contre le terrorisme.

L'amendement COM-13 est adopté.

L'article 4 est adopté dans la rédaction issue des travaux de la commission.

Division additionnelle avant l'article 5

M. Philippe Bas, rapporteur. – L'amendement COM-14 vise à introduire un chapitre IV relatif à l'expérimentation de traitements de données biométriques en temps réel pour lutter contre le terrorisme et la grande criminalité.

L'amendement COM-14 est adopté.

Article 5

M. Philippe Bas, rapporteur. – L'amendement COM-15 tend à ouvrir, au titre des techniques de renseignement, une autorisation spéciale pour la reconnaissance biométrique en temps réel dans l'espace public par la DGSI à la seule fin de prévention du terrorisme.

Pour la première fois, le système actuel robuste et efficace d'autorisations délivrées par le Premier ministre sur avis de la CNCTR serait élargi non plus seulement au recueil d'informations, mais à leur analyse.

L'amendement COM-15 est adopté. En conséquence, les amendements COM-1 et COM-2 *deviennent sans objet.*

L'article 5 est adopté dans la rédaction issue des travaux de la commission.

Article 6

M. Philippe Bas, rapporteur. – L'amendement COM-16 porte sur l'utilisation subsidiaire de la biométrie en temps réel pour des enquêtes judiciaires. Il prévoit de limiter ce dispositif aux seules investigations relatives à des actes de terrorisme, à des atteintes aux intérêts fondamentaux de la nation, à la grande criminalité ou à des disparitions d'enfants.

Le juge des libertés et de la détention devra être saisi après quarante-huit heures pour tout renouvellement de l'utilisation de cette technologie. Seuls des officiers de police judiciaire habilités, à l'exclusion des agents de police judiciaire, pourront la mettre en œuvre.

L'amendement COM-16 est adopté.

L'article 6 est adopté dans la rédaction issue des travaux de la commission.

Article 7

M. Philippe Bas, rapporteur. – L'amendement COM-17 tend à supprimer l'article 7, dont les dispositions ont été introduites à l'article 1er *bis*.

L'amendement COM-17 est adopté.

L'article 7 est supprimé.

Article 8

M. Philippe Bas, rapporteur. – L'amendement COM-18 tend à supprimer l'article 8, pour les mêmes raisons.

L'amendement COM-18 est adopté.

L'article 8 est supprimé.

Division additionnelle avant l'article 9

M. Philippe Bas, rapporteur. – L'amendement COM-19 tend à introduire un nouveau chapitre relatif à l'application de la proposition de loi dans les territoires ultramarins.

L'amendement COM-19 est adopté.

Article 9

L'article 9 est adopté sans modification.

La proposition de loi est adoptée dans la rédaction issue des travaux de la commission.

Le sort des amendements examinés par la commission est retracé dans le tableau suivant :

Auteur	N°	Objet	Sort de l'amendement
Division(s) additionnelle(s) avant l'article 1er			
M. BAS, rapporteur	3	Introduction d'un nouveau chapitre relatif aux garanties permettant de faire obstacle à une société de surveillance	**Adopté**
Article 1er			
M. BAS, rapporteur	4	Clarification des lignes rouges relatives à la reconnaissance biométrique	**Adopté**
Article(s) additionnel(s) après l'article 1er			
M. BAS, rapporteur	5	Caractère expérimental des dispositions de la proposition de loi	**Adopté**
M. BAS, rapporteur	6	Caractéristiques des traitements de reconnaissance biométriques mis en œuvre à titre expérimental	**Adopté**
M. BAS, rapporteur	7	Intégration de représentants de l'ARCOM et de l'ARCEP au collège de la CNIL et, par réciprocité, de représentants de la CNIL au sein de ces deux autorités	**Adopté**
Division(s) additionnelle(s) avant l'article 2			
M. BAS, rapporteur	8	Introduction d'un nouveau chapitre relatif à l'expérimentation d'un dispositif d'authentification biométrique sans consentement pour l'accès à certains grands évènements	**Adopté**
Article 2			
M. BAS, rapporteur	9	Renforcement de l'encadrement des systèmes d'authentification biométrique sans consentement mis en place lors de certains grands événements	**Adopté**
Division(s) additionnelle(s) avant l'article 3			
M. BAS, rapporteur	10	Introduction d'un nouveau chapitre relatif à l'expérimentation de traitements de données biométriques *a posteriori* dans le cadre d'enquêtes judiciaires ou en matière de renseignement	**Adopté**
Article 3			
M. BAS, rapporteur	11	Garanties supplémentaires pour l'expérimentation de la reconnaissance biométrique *a posteriori* dans un cadre judiciaire	**Adopté**

Auteur	N°	Objet	Sort de l'amendement
Article(s) additionnel(s) avant l'article 4			
M. BAS, rapporteur	12	Maintien de la possibilité pour les forces de sécurité intérieure de recourir à des modules de reconnaissance biométrique au sein des fichiers d'antécédents judiciaires dans le cadre de la recherche des auteurs d'infractions à la loi pénale	**Adopté**
Article 4			
M. BAS, rapporteur	13	Clarification en fonction de la provenance des données des procédures applicables pour permettre aux services de renseignement d'utiliser des logiciels de traitement de données biométriques	**Adopté**
Division(s) additionnelle(s) avant l'article 5			
M. BAS, rapporteur	14	Introduction d'un nouveau chapitre relatif à l'expérimentation de traitements de données biométriques en temps réel pour lutter contre le terrorisme et la grande criminalité	**Adopté**
Article 5			
M. BAS, rapporteur	15	Inscription de l'expérimentation de traitements biométriques en temps réel en matière administratif dans le modèle d'autorisation et de contrôle des robuste des techniques de renseignement	**Adopté**
M. REICHARDT	1	Amendement d'ordre rédactionnel	**Rejeté**
M. REICHARDT	2	Saisine pour avis de la Haute autorité pour la transparence de la vie publique en cas de doute sur la compatibilité des fonctions envisagées avec les intérêts détenus et les fonctions exercées au cours des cinq dernières années dans le cadre du développement des traitements	**Rejeté**
Article 6			
M. BAS, rapporteur	16	Garanties supplémentaires pour l'expérimentation de la reconnaissance biométrique en temps réel dans un cadre judiciaire	**Adopté**
Article 7			
M. BAS, rapporteur	17	Amendement de suppression	**Adopté**
Article 8			
M. BAS, rapporteur	18	Amendement de suppression	**Adopté**

Auteur	N°	Objet	Sort de l'amendement
Division(s) additionnelle(s) avant l'article 9			
M. BAS, rapporteur	19	Introduction d'un nouveau chapitre relatif aux dispositions d'application de la proposition de loi dans les territoires ultramarins	**Adopté**

RÈGLES RELATIVES À L'APPLICATION DE L'ARTICLE 45 DE LA CONSTITUTION ET DE L'ARTICLE 44 *BIS* DU RÈGLEMENT DU SÉNAT (« CAVALIERS »)

Si le premier alinéa de l'article 45 de la Constitution, depuis la révision du 23 juillet 2008, dispose que « *tout amendement est recevable en première lecture dès lors qu'il présente un lien, même indirect, avec le texte déposé ou transmis* », le Conseil constitutionnel estime que cette mention a eu pour effet de consolider, dans la Constitution, sa jurisprudence antérieure, reposant en particulier sur « *la nécessité pour un amendement de ne pas être dépourvu de tout lien avec l'objet du texte déposé sur le bureau de la première assemblée saisie* » [1].

De jurisprudence constante et en dépit de la mention du texte « transmis » dans la Constitution, le Conseil constitutionnel apprécie ainsi l'existence du lien par rapport au contenu précis des dispositions du texte initial, déposé sur le bureau de la première assemblée saisie[2]. Pour les lois ordinaires, le seul critère d'analyse est le lien matériel entre le texte initial et l'amendement, la modification de l'intitulé au cours de la navette restant sans effet sur la présence de « cavaliers » dans le texte[3]. Pour les lois organiques, le Conseil constitutionnel ajoute un second critère : il considère comme un « cavalier » toute disposition organique prise sur un fondement constitutionnel différent de celui sur lequel a été pris le texte initial[4].

En application des articles 17 *bis* et 44 *bis* du Règlement du Sénat, il revient à la commission saisie au fond de se prononcer sur les irrecevabilités résultant de l'article 45 de la Constitution, étant précisé que le Conseil constitutionnel les soulève d'office lorsqu'il est saisi d'un texte de loi avant sa promulgation.

---

[1] Cf. *commentaire de la décision n° 2010-617 DC du 9 novembre 2010 - Loi portant réforme des retraites.*

[2] Cf. *par exemple les décisions n° 2015-719 DC du 13 août 2015 - Loi portant adaptation de la procédure pénale au droit de l'Union européenne et n° 2016-738 DC du 10 novembre 2016 - Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias.*

[3] *Décision n° 2007-546 DC du 25 janvier 2007 - Loi ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique.*

[4] *Décision n° 2020-802 DC du 30 juillet 2020 - Loi organique portant report de l'élection de six sénateurs représentant les Français établis hors de France et des élections partielles pour les députés et les sénateurs représentant les Français établis hors de France.*

En application du *vademecum* sur l'application des irrecevabilités au titre de l'article 45 de la Constitution, adopté par la Conférence des Présidents, la commission des lois **a arrêté,** lors de sa réunion du mercredi 31 mai 2023, **le périmètre indicatif de la proposition de loi n° 505 (2022-2023) relative à la reconnaissance biométrique dans l'espace public.**

Elle a considéré que **ce périmètre incluait** les dispositions relatives :

- aux modalités d'utilisation des dispositifs de reconnaissance biométrique à des fins d'authentification ;

- aux modalités d'utilisation des dispositifs de reconnaissance biométrique à des fins d'identification dans un cadre judiciaire ;

- aux modalités d'utilisation des dispositifs de reconnaissance biométrique à des fins d'identification dans un cadre administratif.

COMPTE RENDU DE L'AUDITION DE M. LOUIS DUTHEILLET DE LAMOTHE, SECRÉTAIRE GÉNÉRAL DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

(Mardi 23 mai 2023)

M. François-Noël Buffet, président. – Nous recevons cet après-midi Louis Dutheillet de Lamothe, secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL).

Monsieur le secrétaire général, j'ai souhaité l'organisation de cette audition afin que vous nous présentiez le rapport d'activité pour 2022 de la CNIL. Nous aimerions aussi connaître la position de la CNIL sur le sujet particulier de la reconnaissance biométrique, dans la perspective de l'examen la semaine prochaine en commission de la proposition de loi relative à la reconnaissance biométrique dans l'espace public, déposée par nos collègues Marc-Philippe Daubresse et Arnaud de Belenet, qui fait suite à la mission d'information qu'ils ont conduite de février à mai 2022 avec Jérôme Durain. Philippe Bas, rapporteur de ce texte, aura certainement à cœur de vous questionner de façon précise sur le sujet.

M. Louis Dutheillet de Lamothe, secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL). – Je vous prie tout d'abord de bien vouloir excuser Marie-Laure Denis, présidente de la CNIL, qui ne pouvait être présente cet après-midi, retenue par le colloque sur les 45 ans de la CNIL et qui devra se rendre demain à Bruxelles.

Je commencerai par vous présenter en quelques mots le rapport d'activité de la CNIL, avant d'évoquer la proposition de loi.

L'accompagnement est une activité toujours plus soutenue pour la CNIL : le règlement général sur la protection des données (RGPD), qui a remplacé le système de déclaration par un système de responsabilité des entreprises, assorti de lourdes sanctions, a créé une demande de sécurité juridique. Nous avons ainsi adopté une quinzaine d'actes de droit souple – guides, référentiels, recommandations, *etc*. – et répondu à 1 500 demandes de conseil de la part d'entreprises, nombre qui se maintient à un niveau constant. Nous avons reconduit pour la deuxième année nos actions d'accompagnement individualisé de projets innovants, selon notre dispositif de « bac à sable ». Nous avons choisi en 2022 le thème des technologies innovantes en matière d'éducation et procédé à un appel à projets. Comme ce programme a eu beaucoup de succès, nous poursuivrons en 2023, avec un nouveau programme d'accompagnement renforcé, qui, lui, ne sera pas thématique. Nous avons donc enrichi la palette de nos actions pour

permettre aux entreprises innovantes de lancer des produits en étant sûres de leur conformité avec le RGPD.

Mme Karin Kiefer, directrice de la protection des droits et des sanctions de la CNIL. – Notre activité de contrôle et de sanction se divise en trois grands ensembles : le traitement des demandes des usagers, le contrôle des acteurs et l'édiction de mesures correctrices.

En ce qui concerne la relation aux usagers, nous avons reçu plus de 12 000 plaintes en 2022, ainsi que 7 400 demandes d'exercice de droits indirects, qui portent notamment sur le fichier national des comptes bancaires et assimilés (Ficoba), chiffre en hausse de 27 %. Pour la première fois depuis l'entrée en vigueur du RGPD, nous avons réussi à traiter plus de plaintes que nous n'en avons reçu, ce qui nous a permis de réduire le stock d'affaires en attente – une première depuis 2018 ! Nous avons créé un portail internet dédié aux usagers, pour que les plaignants puissent ouvrir un compte en ligne et nous solliciter par ce biais ; nous avons aussi ouvert un téléservice pour les demandes d'exercice de droits indirects.

Nous avons effectué 3 500 contrôles, majoritairement sur place, comme nous le faisions avant l'épidémie liée à la covid-19 – on peut se réjouir d'un retour à la normale en la matière. Beaucoup de ces contrôles font suite à des plaintes des citoyens.

S'agissant de l'activité répressive, la CNIL a adopté 147 mises en demeure en 2022, notamment, dans la moitié des cas, pour des manquements relatifs à la sécurité des données. Elle a prononcé 21 décisions de sanctions, dont 13 publiques. Une avancée a été la création d'une procédure simplifiée qui permet au président de la formation restreinte ou à un membre qu'il désigne de prendre seul une sanction dans des dossiers d'importance mineure ou ne présentant pas de difficulté particulière, ce qui permet d'agir plus vite. Parmi les sanctions emblématiques, je citerai celle rendue à l'encontre de la société Clearview, dans une affaire liée à la reconnaissance faciale. Beaucoup de sanctions, comme celles à l'encontre de Microsoft, Apple ou TikTok, concernent l'usage des cookies. Nous avons aussi participé à des décisions européennes, en examinant des projets de décisions de nos homologues, à l'image de la décision récente du régulateur irlandais contre Meta d'1,2 milliard d'euros.

M. Louis Dutheillet de Lamothe. – La CNIL a vu le taux de plaintes augmenter de 30 % par an depuis la mise en œuvre du RGPD. Dans ces conditions, être capable de traiter plus de plaintes que nous n'en recevons constitue un défi quotidien pour les services de la CNIL.

J'en viens maintenant à la proposition de loi relative à la reconnaissance biométrique dans l'espace public. En 2019, la CNIL a publié une position de principe, soulignant les risques particuliers que la reconnaissance faciale comporte. Elle appelait à un débat public démocratique. Nous y sommes !

La CNIL a toujours considéré les données biométriques comme des données particulières, même si ce n'est que le RGPD qui en a fait des données « sensibles », c'est-à-dire dont le traitement est interdit sans le consentement de la personne, à moins qu'une loi ou un texte réglementaire ne l'autorise. Les données biométriques permettent en effet l'identification des personnes, de manière unique et quasi certaine, et ne peuvent jamais être modifiées, ce qui peut être problématique si leur sécurité est compromise.

Il faut s'interroger sur les différents usages de la reconnaissance biométrique, et sur les risques associés. Certains usages avec le consentement des personnes ne posent pas de problème, comme l'authentification de l'usager d'un téléphone par exemple. Beaucoup d'entreprises sollicitent la CNIL pour développer de tels services d'identification par biométrie avec le consentement de la personne. La CNIL vérifie comment le service est sécurisé techniquement, les modalités de recueil du consentement de la personne, si les données sont stockées en local, à la main de la personne, sans base centralisée. Il faut en effet partir du principe qu'une base centralisée peut toujours être victime d'une cyberattaque un jour ou l'autre et que la sécurité des données centralisées peut toujours être compromise. Nous demandons que le stockage soit décentralisé – une empreinte par téléphone, par exemple –, de telle sorte qu'il ne soit pas possible de récupérer l'ensemble des données en une seule attaque.

D'autres usages sont de police. Il peut s'agir de vérifier, à partir d'une photographie, si une personne figure dans le fichier de traitement d'antécédents judiciaires (TAJ) ou dans n'importe quel fichier. Un autre usage plus intrusif consiste à rechercher *a posteriori* dans des vidéos un ou plusieurs visages. Ce n'est à ce jour pas autorisé dans le droit français, même s'il s'agit du prolongement de l'usage précédent.

L'usage de la reconnaissance en temps réel par une caméra, d'une personne dans la rue, ou ailleurs, constitue un changement de nature. Nous identifions cinq risques.

Le premier consiste en une menace pour le respect de la vie privée, car, avec ce système, il devient possible d'identifier toute personne sur une photographie ou une vidéo ; or notre droit protège notre capacité à circuler dans l'espace public de manière anonyme.

Il existe aussi des risques d'erreurs sur l'identification, comme on le constate dans les pays qui ont commencé à expérimenter ces systèmes : il arrive que les personnes appréhendées ne soient pas les bonnes.

Ensuite, ces systèmes peuvent comporter des biais discriminatoires, en fonction de la manière dont ils ont été entraînés, et ils peuvent commettre plus d'erreurs sur telle ou telle catégorie de population.

Le quatrième risque est lié à l'apparition d'une inhibition dans l'exercice de ses droits ou libertés fondamentales : on peut hésiter à manifester si l'on sait que l'on est filmé et potentiellement reconnu !

Enfin, il y a un risque de sécurité informatique : toute base centralisée de données biométriques est une cible pour une cyberattaque malveillante. La question n'étant pas de savoir si une attaque aura lieu, mais quand ! Les cyberattaques sont de plus en plus sophistiquées et nul ne peut garantir la sécurité des données.

Le collège de la CNIL ne s'est pas prononcé sur la proposition de loi. Mes propos ne refléteront donc que l'analyse des services de la CNIL au regard de sa doctrine plus générale.

Il découle des délibérations du collège de la CNIL qu'il ne faut expérimenter ces technologies, notamment celles permettant une analyse temps réel, qu'avec une extrême prudence et de manière progressive.

Or la proposition de loi élargit de manière considérable et d'un seul coup les cas d'usage. On peut les distinguer en trois grands ensembles.

Tout d'abord, l'authentification. C'est l'usage qui pose le moins de difficultés. Il convient de procéder avec un stockage des données en local, qui ne soit pas centralisé et qui reste à la main des personnes. Il me semble que ces usages sont déjà permis par le droit actuel. Le règlement type de la CNIL permet d'installer des systèmes d'authentification des personnes employées par quelqu'un ; cette possibilité vaut aussi pour l'organisation d'un événement. Il suffit donc d'élargir et d'affiner ce qui existe déjà. Ces systèmes d'authentification biométriques sont faillibles. Les sociétés qui assurent la sécurité d'événements refusent en général de s'en remettre uniquement à la biométrie. Il faut conjuguer ces dispositifs avec du contrôle humain et d'autres dispositifs, adaptés au cas par cas. Le règlement type de la CNIL, qui prévoit trois niveaux de dispositifs possibles, peut constituer un point de référence utile.

Le deuxième cas d'usage visé par la proposition de loi est nouveau : il s'agit de l'identification *a posteriori*, soit dans le cadre d'enquêtes judiciaires, soit dans le cadre d'enquêtes par les services de renseignement lorsque les intérêts fondamentaux de la Nation sont en jeu. La relecture *a posteriori* de documents, de photographies ou de vidéos, dans le cadre d'une enquête déjà ouverte, pour y identifier des personnes est moins attentatoire que la reconnaissance en temps réel, dans la rue des personnes qui passent. Cette capacité de recherche dans une vidéo est inédite. Il importe de s'interroger sur la nécessité et sur le caractère proportionné du recours à ce type de méthodes. Dans ce cas, il convient de prévoir des garanties, à commencer par l'existence d'un contrôle humain approfondi.

Le périmètre retenu par le texte semble très large. L'exposé des motifs vise les infractions les plus graves, mais en fait tous les délits passibles d'une peine d'emprisonnement de trois ans, donc tous les vols, pourraient faire l'objet de ce type d'enquête selon le texte de l'article 3.

Nous vous demandons de mettre en avant le principe de subsidiarité, qui figurait dans le rapport de votre commission sur la

reconnaissance biométrique dans l'espace public. Cette technique de recherche automatique de visages dans des vidéos ne devrait être que subsidiaire par rapport aux techniques habituelles d'enquête.

Enfin et surtout, il faut, nous semble-t-il, préciser et encadrer de manière stricte l'identité des personnes que l'on va rechercher dans une vidéo : est-ce que l'on recherche une personne bien identifiée ? ou bien s'agit-il d'identifier toutes les personnes présentes sur une scène, par exemple pour trouver des témoins, ce qui est intrusif et ne devrait être possible que dans des cas d'une extrême gravité ?

En ce qui concerne l'usage par les services de renseignement, le texte prévoit déjà un encadrement, mais celui-ci pourrait encore être précisé. Il permet le recours à la biométrie pour « retrouver une personne préalablement identifiée susceptible d'être en lien avec une menace ». On comprend qu'il s'agit d'une menace pour les intérêts fondamentaux de la Nation, mais il faudrait l'expliciter ; de même, la notion d'« entourage » est trop large.

Le troisième et dernier cas d'usage est l'identification en temps réel dans l'espace public, pour sécuriser de grands événements ou pour les enquêtes judiciaires les plus graves. Il s'agit pour nous du point le plus délicat et le plus novateur. Le risque d'atteinte à la vie privée est d'une tout autre ampleur et nature que dans les cas précédents. La surveillance et l'identification ont lieu en temps réel, au moment où les personnes passent devant la caméra. Or c'est dans ces cas que le contrôle humain est le plus faible, car à la différence d'une enquête de long cours, le fait divers appelle une réaction dans l'urgence, en temps réel. C'est aussi dans ces circonstances que les risques d'erreur sur la personne ou d'intervention d'un biais discriminatoire sont les plus élevés, avec des conséquences concrètes potentiellement importantes. En outre, la mise en œuvre de ce type de système suppose techniquement de créer une dérivation des images vers les lieux où serait effectuée la reconnaissance faciale en temps réel par comparaison avec les bases de données biométriques mises à disposition. Comme il n'existe pas de système de vidéosurveillance centralisée en France, il faudrait installer ce dispositif dans chaque endroit où l'on voudrait l'utiliser. Cela accroît le risque de sécurité et de compromission des bases et des données. Enfin, ce système est aussi le plus inhibant pour les personnes pour exercer leurs libertés dans l'espace public.

La création de ce dispositif, fût-ce à titre expérimental, serait une rupture fondamentale pour l'exercice de nos libertés publiques alors que n'avons pas encore de recul sur l'efficacité et l'utilité de la biométrie dans les autres cas d'usage. L'exploitation en temps réel des vidéos ne se limite pas à la reconnaissance faciale, elle comporte aussi le recours à l'intelligence artificielle. Une réflexion a eu lieu depuis deux ans sur les caméras augmentées ou intelligentes. Le Parlement vient de décider, dans la loi relative aux jeux Olympiques et Paralympiques (JOP) de 2024, de tester cette

technologie, dans un cadre dont la CNIL a elle-même estimé qu'il était précis et encadré. L'expérimentation permettra d'apprécier ce que ce système apporte à la sécurisation des grands événements. Or l'équilibre qui a été trouvé n'inclut pas, comme le Conseil constitutionnel l'a souligné, la reconnaissance faciale. On ne sait pas encore si les caméras augmentées, sans reconnaissance faciale, sont utiles pour sécuriser les grands événements, pour repérer des agressions, des attentats, *etc*. Le collège de la CNIL s'est prononcé pour que l'on évalue si ces caméras augmentées sont utiles ; il s'est opposé à la mise en place de dispositifs de reconnaissance faciale.

Outre cette loi relative aux jeux Olympiques et Paralympiques (JOP), qui vient d'être votée, un débat a lieu au niveau européen sur un projet de règlement sur l'intelligence artificielle : l'enjeu est notamment de savoir si l'on doit autoriser ou non la reconnaissance faciale dans l'espace public.

Si une agression a eu lieu, il est déjà possible d'exploiter les vidéos et de les analyser *a posteriori* pour identifier des personnes à partir du traitement des antécédents judiciaires (TAJ). Une partie de ce que la proposition de loi vise à permettre en temps réel, de manière automatique, en disséminant l'accès aux bases centralisées de données biométriques dans les centres de supervision, peut donc déjà être réalisé, sans courir les risques que j'ai mentionnés, de manière manuelle. Certes, c'est un plus long, – il faut récupérer l'image, l'analyser, *etc*. –, mais c'est peut-être le prix à payer pour ne pas équiper nos espaces publics de ce type de dispositifs qui induisent un changement considérable dans la manière d'exercer nos libertés publiques.

En conclusion, au nom des services de la CNIL, je vous appelle à restreindre le champ de l'expérimentation. Continuons à expérimenter et à développer notre connaissance de l'utilité de ces nouvelles technologies, en expérimentant par exemple l'analyse *a posteriori* d'images dans le cadre des enquêtes judiciaires. Restons-en à l'équilibre trouvé dans la loi sur les jeux Olympiques et Paralympiques s'agissant du temps réel.

M. Philippe Bas, rapporteur. – Merci pour cet exposé très clair. J'aborderai directement le sujet qui fâche, le dernier parmi ceux que vous avez abordés. Nous devons rechercher le bon équilibre entre les impératifs de sécurité, d'une part, et le respect des libertés fondamentales et la protection de la vie privée, d'autre part. Alors que nous allons devoir organiser de grands événements, il serait regrettable, si une menace apparaissait, de ne pas avoir pu mettre en œuvre tous les moyens pour la prévenir. Craignez-vous finalement que l'installation de caméras dotées d'intelligence artificielle dans des lieux bien identifiés n'entraîne inéluctablement le maintien de celles-ci après la fin de l'expérimentation ? Il me semble que vous redoutez une pérennisation de fait.

L'article 5 de la proposition de loi mêle des procédures qui relèvent de la police administrative avec d'autres qui relèvent de la police judiciaire. Ne pourrait-on pas inscrire clairement ce dispositif dans de la police

administrative, en utilisant le mécanisme d'autorisation de recours aux techniques de renseignement prévu par la loi de 2015 sur le renseignement ? Nous pourrions ainsi prévoir une demande d'autorisation d'emploi de ces techniques émise par la direction générale de la sécurité intérieure, pour des lieux déterminés, à l'occasion de certains grands événements susceptibles d'être la cible d'un attentat terroriste, et alors que les personnes à surveiller auront été identifiées. L'autorisation serait donnée par le Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR), et sa décision serait susceptible d'être déférée au Conseil d'État. Ces modalités seraient-elles de nature à apaiser vos craintes ?

Que pensez-vous enfin de la proposition des députés Philippe Gosselin et Philippe Latombe visant à élargir la composition du collège de la CNIL aux présidents de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) et de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) pour renforcer son expertise en matière de système d'intelligence artificielle ?

M. Jérôme Durain. – J'étais rapporteur avec mes collègues Marc-Philippe Daubresse et Arnaud de Belenet de la mission d'information sur la reconnaissance faciale. J'ai choisi, avec mon groupe, de ne pas m'associer à la démarche visant à déposer cette proposition de loi, en partie pour les raisons que vous avez évoquées. J'entends vos appels à la prudence. Vous avez souligné l'importance du saut technologique : pourriez-vous nous éclairer sur la manière dont le débat s'est déroulé sur ces sujets dans les autres pays ?

Le Conseil constitutionnel s'est prononcé sur le texte relatif aux jeux Olympiques et Paralympiques. Il a souligné l'absence de recours à des techniques de reconnaissance faciale ou de biométrie. Que retenez-vous de son analyse juridique ?

J'ai entendu parler d'un site qui permettrait aux citoyens d'exercer leur droit d'accès aux images qui auraient été prises d'eux par les caméras. Il faut remplir un formulaire et l'adresser à la préfecture de police : il semble que cette dernière a décidé de filtrer les demandes en n'acceptant que les demandes papier ? Cette limitation ne restreint-elle pas l'accès aux images par les citoyens ?

M. Louis Dutheillet de Lamothe. – Je ne crains pas du tout qu'une expérimentation soit nécessairement vouée à être pérennisée. L'État de droit prévaut. La loi fixe un cadre et toute prolongation ou pérennisation d'une expérimentation devrait être autorisée par le Parlement. Simplement, l'apparition des systèmes d'analyse en temps réel crée une rupture fondamentale. Dès qu'ils existent, ils peuvent faire l'objet de détournement, en dépit de toutes les garanties.

De ce point de vue, il est moins risqué d'utiliser des caméras *ad hoc*, installées pendant quelques heures avant d'être démontées, et dont les

données seraient sécurisées et *in fine* détruites. Cependant, de manière générale, on ne procède pas ainsi. Pour les caméras augmentées et la sécurisation des grands événements, les images seront dérivées du système du centre de vidéoprotection, en y associant une analyse logicielle automatique. Pour que l'expérimentation de la proposition de loi ait lieu et que, à la demande de l'autorité judiciaire, le dispositif soit déclenché pendant 48 heures renouvelables, il faudra qu'un tel système existe. Choisir d'expérimenter, c'est déjà créer un système, ce qui constitue un saut à ne pas franchir.

Ensuite, si le débat démocratique autorise une telle expérimentation, il faut prévoir un système de garanties à la hauteur des risques présumés. Le système de renseignement en place est robuste, au minimum il faut le transposer.

M. Bertrand Pailhès, directeur de l'innovation et des technologies de la CNIL. – Le déploiement des caméras augmentées concerne trois types d'images. Il s'agit d'abord de celles issues des systèmes de vidéoprotection installés. Il s'agit ensuite des images issues de caméras supplémentaires parfois installées, comme par exemple à l'occasion des marchés de Noël. Enfin, les images peuvent aussi provenir de drones, déployés uniquement lors des grands événements, qui fournissent des données soulevant d'autres défis – l'aspect mouvant des événements peut rendre l'analyse des images difficile.

M. Louis Dutheillet de Lamothe. – Concernant la composition du collège de la CNIL, je m'exprime à titre personnel. Il me semble que l'interrégulation est de plus en plus nécessaire. Les sujets sont de plus en plus imbriqués – voyez l'exemple du numérique, secteur de plus en plus régulé, concerné par un grand nombre de textes européens. La CNIL parle à l'Autorité de régulation de la communication audiovisuelle et numérique et à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse en permanence.

Une hybridation de ce type existe déjà : le président de la Commission d'accès aux documents administratifs (Cada), ou son représentant, siège au collège de la CNIL, et la présidente de la CNIL, ou son représentant, siège au collège de la Cada. Cela crée une remarquable fluidité entre les deux exigences que sont la protection des données personnelles et la bonne communication des documents administratifs. Le dialogue permanent fonctionne.

Je signale un point d'attention : le collège de la CNIL, avec 18 commissaires, est déjà très large et chacun de ses membres est indispensable. Les collèges des autres autorités administratives indépendantes comptent de 6 à 9 membres.

À l'échelle européenne, des discussions sont en cours avec les autres CNIL, avec le Comité européen de la protection des données (EDPB) et avec

le contrôleur européen de la protection des données (CEPB), dit *European Data Protection Supervisor* (EDPS). Ils ont pris des positions fermes sur le troisième type d'usage, à savoir la reconnaissance faciale en temps réel dans l'espace public. Mon discours très réservé sur le troisième type d'usage est en cohérence avec la position de toutes les CNIL européennes et avec l'avis du comité européen et du contrôleur européen sur le règlement européen sur l'intelligence artificielle (IA) de la Commission européenne.

Je ne peux vous dire en pratique où en sont les autres pays : il y a peu d'expérimentations ailleurs. Nous étions dans les premiers à avoir voté une loi sur les caméras augmentées sans reconnaissance faciale.

M. Bertrand Pailhès. – Aux États-Unis, les systèmes de reconnaissance faciale sont aussi utilisés à des fins commerciales. À New York, si tel est le cas, il existe une obligation d'information. Cependant, je ne sais pas quel fut le débat sur la question aux États-Unis.

M. Louis Dutheillet de Lamothe. – On avait cru reconnaître M. Dupont de Ligonnès en Angleterre, grâce à un système de reconnaissance faciale : voilà un autre exemple.

Le Conseil constitutionnel reste très prudent dans son avis sur l'article 10 de la loi sur les jeux Olympiques et Paralympiques : il le trouve équilibré. Cependant, il relève un certain nombre d'éléments permettant d'assurer la proportionnalité de l'article. Toutefois, ce débat a bien eu lieu sur la sécurisation des grands événements et des amendements ont été examinés. La CNIL et le Gouvernement se sont prononcés contre une expérimentation de la reconnaissance faciale en vue des jeux Olympiques et Paralympiques, en avançant aussi le fait qu'il reste peu de temps pour expérimenter. Dans un cadre restreint, acquérir des systèmes efficaces de caméras augmentées est un défi. Cela appelle à ne pas s'orienter vers ce dernier cas d'usage.

Quant aux demandes d'accès aux images de vidéoprotection de la préfecture de police de Paris, qui ne seraient acceptées que sous format papier, cela poserait une difficulté au regard du règlement général sur la protection des données (RGPD), de la directive Police-Justice et du code des relations entre le public et l'administration. En la matière, la jurisprudence de la CNIL consiste à dire qu'il faut proportionner la facilité demandée au responsable de traitement à la taille et aux moyens des services : on demande donc, à partir d'une certaine taille, que les saisines par voie électronique soient disponibles, *a fortiori* pour des autorités publiques. La CNIL demande que les saisines par format papier soient possibles, mais les procédures électroniques doivent aussi être mises en place.

M. Alain Marc. – Les agents de la société Thalès ont indiqué à Jérôme Durain et moi avoir équipé des aéroports à Singapour et aux États-Unis. Si vous voulez des éléments complémentaires, il suffit de vous rendre en banlieue parisienne et de discuter avec nos entreprises françaises.

M. Louis Dutheillet de Lamothe. – C'est un fait que l'Europe s'est dotée d'un système très différent, qui repose sur des valeurs très différentes par rapport à d'autres parties du monde.

Lors du colloque que j'ai évoqué, la présidente actuelle de la CNIL a cité dans son discours inaugural M. Jacques Fauvet, ancien président de la CNIL, qui disait, en 1988 : « Le législateur et la commission qu'il a créée n'ont jamais voulu empêcher ni même gêner les progrès des sciences et des techniques, comme parfois le reproche a pu leur être fait. L'auraient-ils prétendu que les enseignements de l'Histoire les auraient confondus. Loin d'entraver le développement de l'informatique, la CNIL les a rendues plus crédibles et plus efficaces, dans la mesure même où elle a toujours veillé à ce qu'elle soit au service de chaque citoyen. » Je martèle que la position de la CNIL n'est en rien anti-technologique. Au sujet des caméras augmentées, elle a discuté de manière très fructueuse avec le Gouvernement, ses propositions ont été reprises, votées par le Parlement et validées par le Conseil constitutionnel. Nous n'avons pas manqué d'être critiqués par la société civile, disant que c'était déjà inacceptable.

L'idée n'est pas d'empêcher la technologie, mais d'avoir conscience qu'installer dans l'espace public et les centres de supervision des systèmes de reconnaissance en temps réel, grâce à une comparaison avec des données biométriques, constitue un changement de nature dans la manière dont nous vivons l'espace public.

Nous ne savons pas encore si les images issues des caméras augmentées seront utiles à la police ; si tel n'était pas le cas, il faudrait renoncer à cet outil.

M. Bertrand Pailhès. – Nous avons été sollicités par Thales pour un autre cas d'usage, celui de l'embarquement dans des avions et des aéroports – comme à Singapour ou aux États-Unis –, avec une finalité de confort pour les voyageurs, ce qui soulève d'autres questions. En Italie, où une telle expérimentation est en cours, nous discutons avec nos homologues et avec les industriels – les industriels français sont bien placés pour ce type de technologies.

M. Louis Dutheillet de Lamothe. – La CNIL a d'ailleurs validé, en France, un certain nombre d'utilisations de la reconnaissance faciale pour les aéroports, notamment sous forme d'expérimentations, dès lors que le consentement de l'utilisateur est nécessaire au traitement de ses données. Cependant, Thales produit plutôt des équipements à finalité de police.

M. François-Noël Buffet, président. – Je vous remercie.

Cette audition a fait l'objet d'une captation vidéo disponible en ligne sur le site du Sénat.

LISTES DES PERSONNES ENTENDUES ET DES CONTRIBUTIONS ÉCRITES

PERSONNES ENTENDUES PAR LA COMMISSION

Commission nationale de l'informatique et des libertés (CNIL)

M. Louis Dutheillet de Lamothe, secrétaire général

PERSONNES ENTENDUES PAR LE RAPPORTEUR

MM. Philippe Gosselin, député de la Manche, et **Philippe Latombe**, député de Vendée, auteurs du rapport sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité

Ministère de l'intérieur et des outre-mer

Direction des libertés publiques et des affaires juridiques (DLPAJ)

M. Vincent Ploquin-Duchefdelaville, directeur adjoint

M. Dan Scemama, adjoint de la cheffe du bureau du droit des données et des nouvelles technologies, de la sous-direction des libertés publiques

Direction générale de la sécurité intérieure (DGSI)

Mme Caroline Boussion, conseillère juridique

Ministère de la justice

Direction des affaires criminelles et des grâces (DACG)

Mme Élise Barbé, sous-directrice de la négociation et de la législation pénales

Mme Claire Harismendy, rédactrice au bureau de la législation pénale spécialisée

Commission nationale de contrôle des techniques de renseignement (CNCTR)

M. Serge Lasvignes, président

M. Samuel Manivel, conseiller auprès du président

CONTRIBUTIONS ÉCRITES

Conférence nationale des procureurs de la République (CNPR)

Amnesty International France

Ligue des droits de l'Homme (LDH)

LA LOI EN CONSTRUCTION

Pour naviguer dans les rédactions successives du texte, le tableau synoptique de la loi en construction est disponible sur le site du Sénat à l'adresse suivante :

https://www.senat.fr/dossier-legislatif/ppl22-505.html