N° 505

SÉNAT

SESSION ORDINAIRE DE 2022-2023

Enregistré à la Présidence du Sénat le 5 avril 2023

PROPOSITION DE LOI

relative à la **reconnaissance biométrique** *dans l'***espace public**,

PRÉSENTÉE

Par MM. Marc-Philippe DAUBRESSE, Arnaud de BELENET, Bruno RETAILLEAU, Jean-Michel ARNAUD, Jérôme BASCHER, Mmes Nadine BELLUROT, Catherine BELRHITI, Martine BERTHET, Annick BILLON, Christine BONFANTI-DOSSAT, MM. François BONHOMME, Gilbert BOUCHET, Mme Valérie BOYER, MM. Max BRISSON, Laurent BURGOA, Alain CADEC, Mme Agnès CANAYER, MM. Michel CANÉVET, Patrick CHAIZE, Pierre CHARON, Patrick CHAUVET, Olivier CIGOLOTTI, Édouard COURTIAL, Mmes Sonia de LA PROVÔTÉ, Catherine DEROCHE, M. Yves DÉTRAIGNE, Mmes Brigitte DEVÉSA, Catherine DI FOLCO, M. Alain DUFFOURG, Mmes Catherine DUMAS, Dominique ESTROSI SASSONE, Jacqueline EUSTACHE-BRINIO, Françoise FÉRAT, MM. Philippe FOLLIOT, Christophe-André FRASSA, Fabien GENET, Mmes Frédérique GERBAUD, Sylvie GOY-CHAVENT, Pascale GRUNY, MM. Charles GUENÉ, Olivier HENNO, Jean HINGRAY, Mme Micheline JACQUES, MM. Claude KERN, Christian KLINGER, Mme Florence LASSARADE, MM. Jacques LE NAY, Henri LEROY, Stéphane LE RUDULIER, Mmes Brigitte LHERBIER, Anne-Catherine LOISIER, MM. Jean-François LONGEOT, Gérard LONGUET, Pierre LOUAULT, Hervé MAUREY, Thierry MEIGNEN, Mmes Marie MERCIER, Brigitte MICOULEAU, MM. Jean-Marie MIZZON, Jean-Pierre MOGA, Mme Catherine MORIN-DESAILLY, MM. Jean-Jacques PANUNZI, Stéphane PIEDNOIR, Rémy POINTEREAU, André REICHARDT, René-Paul SAVARY, Bruno SIDO, Jean SOL, Mme Nadia SOLLOGOUB, MM. Philippe TABAROT, Jean-Marie VANLERENBERGHE, Mmes Anne VENTALON et Dominique VÉRIEN,

Sénateurs et Sénatrices

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

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

Popularisées dans l'imaginaire collectif par de nombreuses fictions et par de récentes utilisations dans certains pays, les technologies de reconnaissance biométriques font l'objet d'un débat particulièrement polarisé entre les tenants d'un moratoire et ceux qui mettent en exergue leurs bénéfices opérationnels pour favoriser la sécurité ou faciliter nombre d'actes de la vie quotidienne.

Afin d'assurer un débat apaisé sur la question, la commission des lois du Sénat a créé en mars 2022 une mission d'information transpartisane. Au terme des auditions et déplacements conduits par ses rapporteurs, Marc-Philippe DAUBRESSE, Arnaud de BELENET et Jérôme DURAIN, elle a adopté à l'unanimité leur rapport le 10 mai 2022, intitulé *La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance*.

Ce rapport a mis en lumière le fait que le déploiement des usages de la reconnaissance biométrique dans l'espace public s'effectue aujourd'hui en France sans encadrement juridique spécifique, ni réflexion éthique collective. De manière paradoxale, ces usages, pourtant marginaux, soulèvent de nombreuses oppositions tandis que la reconnaissance biométrique se banalise dans la vie de tous les jours avec une multiplication des usages individuels.

Convaincue que toute zone grise appelle une régulation pour éviter la démultiplication d'usages parfois contestables, la commission des lois estime qu'il est désormais impératif de construire une réponse collective à l'usage des technologies de reconnaissance biométrique dans l'espace public afin de ne pas être, dans les années à venir, dépassés par les développements industriels et commerciaux.

Fruit de cette réflexion, la présente proposition de loi tend à transcrire au niveau législatif les conclusions des travaux de la commission et poursuit à ce titre deux objectifs principaux : d'une part, répondre au besoin de régulation, qui s'accentue chaque jour, d'un système qui risque de nous échapper ; d'autre part, accorder aux pouvoirs publics

l'autorisation exceptionnelle d'utiliser des technologies certes intrusives, mais qui ne peuvent, dans le contexte de l'organisation prochaine des jeux Olympiques et Paralympiques par notre pays, être laissées au bon vouloir des acteurs commerciaux. Cela implique, en tout état de cause, un contrôle strict, exigeant et pluridisciplinaire.

Pour ce faire, le rapport recommandait de poursuivre une méthode précise afin que le Parlement s'empare du sujet et rejette clairement le modèle d'une société de surveillance. Il considérait qu'il était en premier lieu nécessaire d'établir clairement des lignes rouges, en fixant notamment le principe d'une interdiction de l'utilisation de la reconnaissance biométrique en temps réel dans l'espace public et de toute catégorisation et notation des personnes physiques sur la base de leurs données biométriques. Une fois celles-ci posées, le Parlement était en second lieu invité à conduire une réflexion sur les cas d'usage de la reconnaissance biométrique dans l'espace public, qui sont multiples et potentiellement illimités.

Dans ce contexte, un raisonnement cas d'usage par cas d'usage s'impose, prenant en considération les finalités poursuivies par chacun d'entre eux. Plusieurs distinctions doivent être opérées, les risques pour les libertés étant dans une large mesure conditionnées par celles-ci.

Une première distinction doit ainsi être réalisée entre 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 », un gabarit avec une base de données de gabarits.

Au sein des techniques d'identification, deux autres distinctions doivent être réalisées. La première d'entre elles a trait à la différence entre exploitation en temps réel, c'est-à-dire dans le cadre d'un processus permettant un usage immédiat des résultats pour procéder à un contrôle de la personne concernée, et utilisation *a posteriori*, par exemple dans le cadre d'une enquête. Dans ce dernier cas, les recherches se font généralement sur des enregistrements. Une seconde distinction, dans l'utilisation de l'identification par les acteurs publics, concerne le cadre dans lequel cette utilisation est réalisée : police administrative ou police judiciaire.

La proposition de loi, traduisant en cela le rapport, considère qu'une fois les lignes rouges définies et garanties, certains cas d'usage peuvent légitimement être expérimentés tandis que d'autres doivent être écartés. Ces expérimentations ne pourront toutefois avoir lieu que dans le cadre d'un régime de contrôle et de redevabilité adapté et renforcé.

L'**article 1er** vise à poser dans la loi des lignes rouges claires afin d'écarter le risque d'une société de surveillance. Il interdit ainsi toute catégorisation et notation des personnes physiques sur la base de leurs données biométriques, et 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.

Une fois ces lignes rouges définies, la proposition de loi détermine les cas d'usage qui pourraient, par exception, être expérimentés.

L'**article 2** concerne l'authentification biométrique. Il propose ainsi, 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 aux acteurs étatiques, dans l'organisation de grands évènements, d'organiser par exception un contrôle exclusivement biométrique de l'accès aux zones nécessitant une sécurisation exceptionnelle.

Les articles 3 à 6 autoriseraient l'expérimentation de quatre cas d'usage très limités de l'identification biométrique.

L'**article 3** vise à permettre, à titre expérimental, de manière subsidiaire et uniquement pour la recherche d'auteurs ou de victimes potentielles des infractions les plus graves, l'exploitation *a posteriori* d'images se rapportant à un périmètre spatio-temporel limité par le biais de logiciels de reconnaissance biométrique, sous le contrôle du magistrat en charge de l'enquête ou de l'instruction.

L'**article 4** instituerait, à titre expérimental, une nouvelle technique de renseignement permettant aux services du premier cercle de traiter *a posteriori* les images issues de la voie publique à l'aide de systèmes de reconnaissance biométrique, uniquement pour 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 5** vise à créer un cadre juridique expérimental permettant, par exception et de manière strictement subsidiaire, le recours ciblé et limité dans le temps à des systèmes de reconnaissance biométrique sur la voie publique en temps réel 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. De nombreuses garanties entourent ce dispositif, qu'il s'agisse de la formation spécifique des agents pouvant utiliser ces traitements, des modalités de leur développement, de celles de leur déploiement, ou encore du fait que ces dispositifs ne seraient déployés que sur un nombre limité de caméras dédiées et distinctes de celles des systèmes de vidéoprotection, ce qui permet de circonscrire fortement le périmètre géographique et temporel du déploiement.

L'**article 6** prévoit quant à lui la création d'un cadre permettant aux autorités judiciaires de recourir à des systèmes de reconnaissance biométrique sur la voie publique en temps réel dans le cadre d'enquêtes judiciaires relatives aux infractions les plus graves menaçant ou portant atteinte à l'intégrité physique des personnes.

S'agissant enfin de la gouvernance de ces expérimentations, l'**article 7** envisage la mise en place d'un régime de contrôle renforcé, en prévoyant la remise d'un rapport annuel au Parlement ainsi que l'information en temps réel de l'Assemblée nationale et du Sénat des mesures prises ou mises en œuvre par les autorités administratives en application de cette proposition de loi. Le Parlement pourrait également requérir toute information complémentaire du Gouvernement dans le cadre de l'évaluation de ces mesures.

L'**article 8** définit l'encadrement des expérimentations prévues aux articles 2 à 6. Ces mesures seraient applicables pour une durée limitée, de trois ans à compter de la promulgation de la loi. 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 l'évolution du droit de l'Union européenne en la matière.

L'**article 9**, enfin, assurerait l'application de la proposition de loi dans les territoires ultramarins.

Proposition de loi relative à la reconnaissance biométrique dans l'espace public

Article 1er

① L'article 95 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est complété par deux alinéas ainsi rédigés :

② « Toute catégorisation et notation des personnes physiques sur la base de leurs données biométriques sont interdites.

③ « 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 est interdite. »

Article 2

① Après 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, il est inséré un 4° *bis* ainsi rédigé :

② « 4° *bis* À la seule fin d'assurer la sécurité d'un grand évènement au sens de l'article L. 211-11-1 du code de la sécurité intérieure 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 lesquels l'organisateur desdits évènements a démontré un impératif particulier d'assurer un haut niveau de fiabilité de l'identification des personnes, les traitements conformes aux règlements types mentionnés au *c* du 2° du I de l'article 8 de la présente loi mis en œuvre par l'organisateur qui portent sur des données biométriques strictement nécessaires au contrôle de l'accès, à un autre titre que celui de spectateur ou de participant, à tout ou partie des établissements et des installations désignés par le décret mentionné au premier alinéa de l'article L. 211-11-1 du code de la sécurité intérieure dès lors qu'ils font l'objet d'une restriction de circulation et d'accès. »

Article 3

① Après le chapitre III du titre IV du livre I[er] du code de procédure pénale, il est inséré un chapitre III *bis* ainsi rédigé :

② « *CHAPITRE III* BIS

③ ***« Des logiciels de traitement de données biométriques***

④ « *Art. 230-27-1*. – Afin de faciliter le rassemblement des preuves des infractions et l'identification de leurs auteurs ou la recherche d'une personne disparue mentionnée à l'article 74-1, les services de la police nationale et de la gendarmerie nationale chargés d'une mission de police judiciaire ainsi que le service placé sous l'autorité du ministre chargé du budget chargé d'effectuer des enquêtes judiciaires peuvent mettre en œuvre, sous le contrôle de l'autorité judiciaire, des logiciels de traitement de données biométriques destinés à faciliter l'exploitation *a posteriori* des images recueillies dans le cadre des investigations au cours :

⑤ « 1° Des enquêtes préliminaires, des enquêtes de flagrance ou des investigations exécutées sur commission rogatoire sur des crimes et délits punis d'une peine d'emprisonnement de trois ans ou plus ;

⑥ « 2° D'une procédure d'enquête ou d'instruction de recherche des causes de la mort ou de la disparition prévue aux articles 74,74-1 et 80-4 ;

⑦ « 3° D'une procédure de recherche d'une personne en fuite prévue à l'article 74-2.

⑧ « *Art. 230-27-2*. – Les données exploitées par les logiciels faisant l'objet du présent chapitre ne peuvent provenir que des pièces et des documents de procédure judiciaire déjà détenus par les services mentionnés à l'article 230-27-1.

⑨ « Lorsque sont exploitées des données pouvant faire apparaître l'identité des personnes, celle-ci ne peut apparaître qu'une fois les opérations de rapprochement effectuées, et uniquement pour celles de ces données qui sont effectivement entrées en concordance entre elles ou avec d'autres informations exploitées par le logiciel.

⑩ « *Art. 230-27-3*. – Les données à caractère personnel révélées par l'exploitation des enquêtes et des investigations mentionnées au 1° de l'article 230-27-1 sont effacées à la clôture de l'enquête et, en tout état de cause, à l'expiration d'un délai de trois ans à compter de leur révélation.

⑪ « Les données à caractère personnel révélées par l'exploitation des enquêtes mentionnées au 2° du même article 230-27-1 sont effacées dès que l'enquête a permis de retrouver la personne disparue ou, en tout état de cause, à l'expiration d'un délai de vingt ans à compter de leur révélation.

⑫ « *Art. 230-27-4*. – Sans préjudice des pouvoirs de contrôle attribués à la Commission nationale de l'informatique et des libertés par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République compétent qui peut demander qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. La rectification pour requalification judiciaire est de droit lorsque la personne concernée la demande.

⑬ « Le procureur de la République en charge de l'enquête dispose, pour l'exercice de ses fonctions, d'un accès direct à ces logiciels.

⑭ « *Art. 230-27-5*. – Un magistrat, chargé de contrôler la mise en œuvre des logiciels faisant l'objet du présent chapitre et de s'assurer de la mise à jour des données, désigné à cet effet par le ministre de la justice, concourt à l'application de l'article 230-27-4.

⑮ « Ce magistrat peut agir d'office ou sur requête des particuliers.

⑯ « Il dispose, pour l'exercice de ses fonctions, d'un accès direct à ces logiciels.

⑰ « *Art. 230-27-6*. – Peuvent seuls utiliser les logiciels faisant l'objet du présent chapitre :

⑱ « 1° Les agents des services mentionnés à l'article 230-27-1, individuellement désignés et spécialement formés et habilités, pour les seuls besoins des enquêtes dont ils sont saisis ;

⑲ « 2° Les magistrats du parquet et les magistrats instructeurs, pour les recherches relatives aux infractions dont ils sont saisis ;

⑳ « 3° Le procureur de la République compétent, aux fins du contrôle qu'il exerce en vertu de l'article 230-27-4 ;

㉑ « 4° Le magistrat mentionné à l'article 230-27-5.

㉒ « L'habilitation mentionnée au 1° du présent article précise la nature des données auxquelles elle donne accès.

㉓ « *Art. 230-27-7.* – Les logiciels faisant l'objet du présent chapitre ne peuvent en aucun cas être utilisés pour les besoins d'enquêtes administratives, ni à une autre fin que celle définie à l'article 230-27-1.

㉔ « *Art. 230-27-8.* – Les logiciels faisant l'objet du présent chapitre sont autorisés par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. Ce décret précise notamment les infractions concernées, les modalités d'alimentation du logiciel, les conditions de formation et d'habilitation des personnes mentionnées au 1° de l'article 230-27-6 et les modalités selon lesquelles les personnes intéressées peuvent exercer leur droit d'accès. »

Article 4

① Le titre V du livre VIII du code de la sécurité intérieure est complété par un chapitre VI ainsi rédigé :

② *« CHAPITRE VI*

③ ***« De l'utilisation de traitements de données biométriques* a posteriori**

④ « *Art. L. 855-1 D.* – I. – Dans les conditions prévues au chapitre I[er] du titre II du présent livre et pour les seules finalités prévues aux 1°, 2°, 4° et 5° de l'article L. 811-3, peut être autorisée l'utilisation, par les services spécialisés de renseignement mentionnés à l'article L. 811-2, de logiciels de traitement de données biométriques afin de retrouver une personne préalablement identifiée susceptible d'être en lien avec une menace. Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.

⑤ « Les données exploitées par les logiciels faisant l'objet du présent chapitre ne peuvent provenir que des images déjà détenues par les services mettant en œuvre lesdits logiciels à la suite de réquisitions portant sur des systèmes de vidéoprotection et de la mise en œuvre éventuelle des techniques mentionnées à l'article L. 853-1.

⑥ « Lorsque sont exploitées des données pouvant faire apparaître l'identité des personnes, celle-ci ne peut apparaître qu'une fois les opérations de rapprochement effectuées, et uniquement pour celles de ces données qui sont entrées en concordance entre elles ou avec d'autres informations exploitées par le logiciel.

⑦ « II. – Par dérogation à l'article L. 821-4, l'autorisation de mise en œuvre de la technique mentionnée au I du présent article est délivrée pour une durée maximale d'un mois. L'autorisation est renouvelable dans les mêmes conditions de durée.

⑧ « III. – Le service autorisé à recourir à la technique mentionnée au I rend compte de sa mise en œuvre à la Commission nationale de contrôle des techniques de renseignement. La commission dispose d'un accès permanent, complet, direct et immédiat aux informations ou aux documents collectés. Elle peut à tout moment adresser une recommandation tendant à ce que cette opération soit interrompue et que les renseignements collectés soient détruits.

⑨ « IV. – Le caractère d'urgence mentionné à la dernière phrase du deuxième alinéa de l'article L. 821-1 ne peut être invoqué que si l'autorisation prévue au présent article a été délivrée au titre des 1°, 4° ou *a* du 5° de l'article L. 811-3.

⑩ « V. – Le nombre maximal des autorisations délivrées en application du présent article en vigueur simultanément est arrêté par le Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement. La décision fixant ce contingent et sa répartition entre les ministres mentionnés au premier alinéa de l'article L. 821-2 ainsi que le nombre d'autorisations d'identification délivrées sont portés à la connaissance de la commission.

⑪ « VI. – Les modalités d'application du présent article sont fixées par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des techniques de renseignement. »

Article 5

① I. – À titre expérimental, par dérogation au dernier alinéa de l'article 95 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction résultat de la présente loi, et à la seule fin d'assurer la sécurité de grands évènements sportifs, récréatifs ou culturels, qui, par leur ampleur ou leurs circonstances sont particulièrement exposées à des risques d'actes de terrorisme ou à des risques d'atteintes graves à la sécurité des personnes, les officiers de police judiciaire peuvent mettre en œuvre un traitement algorithmique destiné à identifier, sur la base de leurs caractéristiques biométriques, des personnes limitativement et préalablement énumérées faisant peser une menace grave et immédiate sur l'ordre public sur les images collectées au moyen de caméras dédiées et distinctes des celles des systèmes de vidéoprotection dans et aux abords des lieux accueillant ces évènements ainsi que dans les véhicules et les emprises de transport public et sur les voies les desservant.

② II. – Ces traitements sont régis par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

③ III. – Le public est informé par tout moyen approprié de l'emploi de traitements algorithmiques visant à identifier des personnes limitativement énumérées à partir de leurs caractéristiques biométriques sur les images collectées au moyen de caméras dédiées, sauf lorsque les circonstances l'interdisent ou que cette information entrerait en contradiction avec les objectifs poursuivis.

④ Une information générale du public sur l'emploi de traitements algorithmiques destinés à identifier des personnes limitativement énumérées à partir de leurs caractéristiques biométriques sur les images collectées au moyen de caméras dédiées est organisée par le ministre de l'intérieur.

⑤ IV. – Ces traitements ne peuvent procéder à aucun rapprochement, interconnexion ou mise en relation automatisée avec d'autres traitements de données à caractère personnel.

⑥ Leur recours obéit aux principes de nécessité et de proportionnalité, appréciés notamment au regard de la finalité qu'ils poursuivent et des circonstances dans lesquelles ils sont mis en œuvre, du caractère proportionné des images traitées et de leur durée de conservation.

⑦ L'identité des personnes ne peut apparaître qu'une fois les opérations de rapprochement effectuées par ces traitements, et uniquement pour celles de ces données qui sont entrées en concordance entre elles ou avec d'autres informations exploitées par le logiciel.

⑧ Ces traitements procèdent exclusivement à un signalement d'attention, strictement limité à l'indication de la probabilité de l'identification de la personne qu'ils ont été programmés à détecter. Ils ne peuvent fonder, par eux-mêmes, aucune décision individuelle ou aucun acte de poursuite. Ils demeurent en permanence sous le contrôle des personnes chargées de leur mise en œuvre.

⑨ Les signalements qu'ils génèrent donnent lieu à une analyse par des agents individuellement désignés et dûment formés et habilités des services de la police nationale et de la gendarmerie nationale. L'habilitation mentionnée au présent alinéa précise la nature des données auxquelles elle donne accès.

⑩ V. – Le recours à un traitement mentionné au I du présent article est, par dérogation à l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, autorisé par un décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés.

⑪ Ce décret fixe les caractéristiques essentielles du traitement. Il indique notamment les conditions d'habilitation et de formation des agents pouvant accéder aux signalements du traitement et, le cas échéant, les spécificités des situations justifiant l'emploi du traitement. Il désigne l'autorité chargée d'établir l'attestation de conformité mentionnée au dernier alinéa du VI du présent article.

⑫ Le décret est accompagné d'une analyse d'impact relative à la protection des données personnelles qui expose :

⑬ 1° Le bénéfice escompté de l'emploi du traitement au service de la finalité mentionnée au I ;

⑭ 2° L'ensemble des risques éventuellement créés par le système et les mesures envisagées afin de les minimiser et de les rendre acceptables au cours de son fonctionnement.

⑮ VI. – L'État assure le développement du traitement ainsi autorisé, en confie le développement à un tiers ou l'acquiert. Dans tous les cas, le traitement doit satisfaire aux exigences suivantes :

⑯ 1° Des garanties sont apportées afin que les données d'apprentissage, de validation et de test choisies soient pertinentes, adéquates et représentatives, et leur traitement loyal, objectif et de nature à identifier et à prévenir l'occurrence de biais et d'erreurs. Ces données doivent demeurer accessibles et être protégées tout au long du fonctionnement du traitement ;

⑰ 2° Le traitement comporte un enregistrement automatique des signalements d'attention permettant d'assurer la traçabilité de son fonctionnement ;

⑱ 3° Le traitement dispose de mesures de contrôle humain et d'un système de gestion des risques permettant de prévenir et de corriger la survenue de biais éventuels ou de mauvaise utilisation ;

⑲ 4° Les modalités selon lesquelles, à tout instant, le traitement peut être interrompu sont précisées ;

⑳ 5° Le traitement fait l'objet d'une phase de test conduite dans des conditions analogues à celles de son emploi tel qu'autorisé par le décret mentionné au V, attestée par un rapport de validation.

㉑ Lorsque le traitement est développé ou fourni par un tiers, celui-ci doit en outre présenter des garanties de compétences et de continuité et fournir une documentation technique complète ainsi qu'une déclaration des intérêts détenus à date et au cours des cinq dernières années.

㉒ Dans le cadre du présent VI, la Commission nationale de l'informatique et des libertés exerce les missions prévues au 2° du I de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en particulier en accompagnant les personnes en charge du développement du traitement.

㉓ Le respect des exigences énoncées au présent VI fait l'objet d'une attestation de conformité établie par l'autorité administrative compétente. Cette attestation est publiée avant que le traitement soit mis à la disposition des services mentionnés au I qui demandent l'autorisation de l'utiliser dans les conditions prévues au VII.

㉔ VII. – A. – L'autorisation d'avoir recours aux traitements mentionnés au I est subordonnée à une demande adressée au représentant de l'État dans le département ou, à Paris, au préfet de police qui précise :

㉕ 1° Le service responsable des opérations ;

㉖ 2° Le ou les motifs de la mise en œuvre du traitement au regard de la finalité mentionnée au même I ;

㉗ 3° La liste des personnes recherchées, les modalités d'établissement de ladite liste ainsi que la justification de la menace pour l'ordre public que les personnes représentent ;

㉘ 4° La justification de la nécessité de recourir au dispositif, permettant notamment d'apprécier la proportionnalité de son usage au regard de la finalité poursuivie ;

㉙ 5° Le périmètre géographique concerné ;

㉚ 6° Le cas échéant, les modalités d'information du public ;

㉛ 7° La durée souhaitée de l'autorisation, proportionnée à l'évènement concerné.

㉜ B. – L'autorisation est délivrée par décision écrite et motivée. Elle ne peut être accordée que lorsque le recours au traitement est nécessaire et proportionné. Elle précise :

㉝ 1° Le responsable du traitement et les services associés à sa mise en œuvre ;

34 2° La manifestation sportive, récréative ou culturelle concernée et les motifs de la mise en œuvre du traitement au regard de la finalité mentionnée au I ;

35 3° Le périmètre géographique concerné par la mise en œuvre du traitement, qui ne peut inclure les abords des lieux de culte ou l'itinéraire d'une manifestation déclarée en application de l'article L. 211-1 du code de la sécurité intérieure ;

36 4° 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 ;

37 5° La durée d'autorisation. Cette durée ne peut excéder quarante-huit heures, renouvelable selon les mêmes modalités lorsque les conditions de sa délivrance continuent d'être réunies.

38 Le représentant de l'État dans le département ou le préfet de police peut mettre fin à tout moment à l'autorisation qu'il a délivrée, dès lors qu'il constate que les conditions ayant justifié sa délivrance ne sont plus réunies.

39 Le nombre maximal de caméras sur les images desquelles peut être simultanément mis en œuvre le traitement algorithmique mentionné au I du présent article dans chaque département est fixé par arrêté du ministre de l'intérieur.

40 VIII. – L'autorité responsable tient un registre des signalements générés par ces traitements, des suites qui y sont apportées ainsi que des personnes ayant accès aux signalements.

41 Ce registre est transmis chaque jour au représentant de l'État dans le département ou, à Paris, au préfet de police, qui s'assure de la conformité des interventions réalisées à l'autorisation délivrée. Le représentant de l'État dans le département ou, à Paris, le préfet de police informe la Commission nationale de l'informatique et des libertés des conditions dans lesquelles le traitement est mis en œuvre.

42 IX. – Les images mentionnées au I peuvent être, dans une limite de trente jours, utilisées comme données d'entraînement, à la seule fin de permettre la validation des paramètres de conception des traitements algorithmiques mentionnés au même I.

43 Lorsque ces données sont nécessaires à la correction des paramètres du traitement et que cette correction exige la réutilisation de ces mêmes données, elles peuvent être conservées et traitées, à l'exclusion de tout autre usage, au-delà de la durée initialement prévue et dans la limite de trois mois.

(44) X. – La Commission nationale de l'informatique et des libertés exerce un contrôle sur l'application du présent article. À cette fin, elle peut mettre en œuvre les dispositions des sections 2 et 3 du chapitre II du titre I[er] de de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(45) Elle est informée tous les trois mois des conditions de mise en œuvre du présent article.

Article 6

(1) I. – À titre expérimental, par dérogation au dernier alinéa de l'article 95 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction résultant de la présente loi, les officiers de police judiciaire et, sur l'ordre et sous la responsabilité de ceux-ci, les agents de police judiciaire, peuvent mettre en œuvre un traitement algorithmique destiné à identifier, sur la base de leurs caractéristiques biométriques, des personnes limitativement et préalablement énumérées sur les images collectées au moyen de caméras dédiées et distinctes des celles des systèmes de vidéoprotection si cette opération est exigée par les nécessités :

(2) 1° D'une enquête ou d'une instruction portant sur :

(3) *a)* Un acte de terrorisme mentionné aux articles 421-1 à 421-6 du code pénal ;

(4) *b)* Une infraction en matière de prolifération des armes de destruction massive et de leurs vecteurs mentionnée aux 1° et 2° du I de l'article L. 1333-9, à l'article L. 1333-11, au II des articles L. 1333-13-3 et L. 1333-13-4 et aux articles L. 1333-13-5, L. 2339-14, L. 2339-15, L. 2341-1, L. 2341-2, L. 2341-4, L. 2342-59 et L. 2342-60 du code de la défense ;

(5) *c)* Une infraction en matière d'armes mentionnée à l'article 222-54 du code pénal et à l'article L. 317-8 du code de la sécurité intérieure ;

(6) *d)* Une infraction en matière d'explosifs mentionnée à l'article 322-11-1 du code pénal et à l'article L. 2353-4 du code de la défense.

(7) *e)* Une infraction relative à une atteinte à l'intégrité des personnes punies de trois ans d'emprisonnement ou plus ;

(8) 2° D'une procédure d'enquête ou d'instruction de recherche des causes de la mort ou de la disparition prévue aux articles 74,74-1 et 80-4 du code de procédure pénale ;

⑨ 3° D’une procédure de recherche d’une personne en fuite prévue à l’article 74-2 du même code.

⑩ II. – Ces traitements sont régis par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et par la loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés.

⑪ III. – Le recours à ces traitements est autorisé :

⑫ 1° Dans le cadre d’une enquête de flagrance, d’une enquête préliminaire ou d’une procédure prévue aux articles 74 à 74-2 du code de procédure pénale, par le procureur de la République, pour une durée maximale de vingt-quatre heures, renouvelables sur décision expresse et motivée ;

⑬ 2° Dans le cadre d’une instruction ou d’une information pour recherche des causes de la mort ou des causes de la disparition mentionnées aux articles 74,74-1 et 80-4 du même code, par le juge d’instruction, pour une durée maximale de quarante-huit heures renouvelables sur décision expresse et motivée.

⑭ IV. – La décision autorisant le recours à ces traitements comporte tous les éléments permettant d’identifier les lieux et les personnes concernées et précise sa durée.

⑮ L’autorisation écrite du procureur de la République ou du juge d’instruction est mentionnée ou versée au dossier de la procédure. Elle n’a pas de caractère juridictionnel et n’est susceptible d’aucun recours.

⑯ V. – Les opérations prévues au présent chapitre se déroulent sous l’autorité et le contrôle du magistrat qui les a autorisées. Ce magistrat peut ordonner à tout moment leur interruption.

⑰ Les opérations ne peuvent, à peine de nullité, avoir un autre objet que celui pour lequel elles ont été autorisées. Le fait que ces opérations révèlent d’autres infractions ne constitue pas une cause de nullité des procédures incidentes.

⑱ VI. – L’identité des personnes ne peut apparaître qu’une fois les opérations de rapprochement effectuées par ces traitements, et uniquement pour celles de ces données qui sont effectivement entrées en concordance entre elles ou avec d’autres informations exploitées par le logiciel.

⑲ 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, dresse procès-verbal des traitements mis en œuvre, des signalements générés et des suites qui y sont apportées. Ce procès-verbal mentionne la date et l'heure du début et de la fin des opérations.

⑳ Les enregistrements sont placés sous scellés fermés.

㉑ L'officier de police judiciaire ou l'agent de police judiciaire agissant sous sa responsabilité décrit, dans un procès-verbal versé au dossier, les données enregistrées qui sont utiles à la manifestation de la vérité. Aucune séquence relative à la vie privée étrangère à l'objet pour lequel les opérations ont été autorisées ne peut être conservée dans le dossier de la procédure.

㉒ VII. – Les données à caractère personnel révélées par l'exploitation des enquêtes et des investigations mentionnées aux 1° et 3° du I sont effacées à la clôture de l'enquête et, en tout état de cause, à l'expiration d'un délai de trois ans à compter de leur révélation.

㉓ Les données à caractère personnel révélées par l'exploitation des enquêtes mentionnées au 2° du même I sont effacées dès que l'enquête a permis de retrouver la personne disparue ou, en tout état de cause, à l'expiration d'un délai de vingt ans à compter de leur révélation.

㉔ Il est dressé procès-verbal de l'opération de destruction.

㉕ VIII. – La mise en œuvre des traitements mentionnés au I est conditionnée à l'existence et à la robustesse de mesures de contrôle humain et d'un système de gestion des risques permettant de prévenir et de corriger la survenue de biais éventuels ou de mauvaise utilisation.

㉖ Ces traitements ne peuvent fonder, par eux-mêmes, aucune décision individuelle ni poursuites automatisées. Les signalements qu'ils génèrent donnent lieu à une analyse par des agents individuellement désignés et dûment formés et habilités des services de la police nationale et de la gendarmerie nationale.

㉗ L'habilitation mentionnée au deuxième alinéa du présent VIII précise la nature des données auxquelles elle donne accès.

㉘ IX. – Les traitements faisant l'objet du présent article ne peuvent être autorisés que par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. Ce décret précise notamment les infractions concernées, les modalités d'alimentation du traitement, les conditions de formation et d'habilitation des personnes mentionnées au I et les modalités selon lesquelles les personnes intéressées peuvent exercer leur droit d'accès.

Article 7

① I. – L'Assemblée nationale et le Sénat sont informés sans délai des mesures prises ou mises en œuvre par les autorités administratives en application de l'article 5 de la présente loi, du 4° *bis* de l'article 44 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et du chapitre VI du titre V du livre VIII du code de la sécurité intérieure. Ces autorités administratives leur transmettent sans délai copie de tous les actes qu'elles prennent en application de ces dispositions. L'Assemblée nationale et le Sénat peuvent requérir toute information complémentaire dans le cadre du contrôle et de l'évaluation de ces mesures.

② Le Gouvernement adresse chaque année au Parlement un rapport détaillé sur l'application de ces mesures et de celles prises ou mises en œuvre en application de l'article 6 de la présente loi et du chapitre III *bis* du titre IV du livre I^{er} du code de procédure pénale.

Article 8

① Les articles 5 et 6 de la présente loi, ainsi que le 4° *bis* de l'article 44 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le chapitre III *bis* du titre IV du livre I^{er} du code de procédure pénale et le chapitre VI du titre V du livre VIII du code de la sécurité intérieure, dans leur rédaction résultant de la présente loi, sont applicables pour une durée de trois ans à compter de la promulgation de la présente loi.

② Un comité scientifique et éthique dont la composition, l'organisation et les modalités de fonctionnement sont fixées par décret est chargé d'évaluer régulièrement l'application de ces mesures. Ses rapports, transmis aux présidents de la commission des lois de l'Assemblée nationale et du Sénat, sont rendus publics.

③ Au plus tard six mois avant la date mentionnée au premier alinéa du présent article, le Gouvernement adresse au Parlement un rapport évaluant l'application de ces mesures 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.

Article 9

① I. – L'article 125 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi rédigé :

② « *Art. 125*. – La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna et dans les Terres australes et antarctiques françaises, dans sa rédaction résultant de la loi n° du relative à la reconnaissance biométrique dans l'espace public. »

③ II. – Au premier alinéa des articles L. 895-1, 896-1, 897-1 et 898-1 du code de la sécurité intérieure, la référence : « n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement » est remplacée par la référence : « n° du relative à la reconnaissance biométrique dans l'espace public ».

④ III. – Le premier alinéa de l'article 804 du code de procédure pénale est ainsi rédigé :

⑤ « Le présent code est applicable, dans sa rédaction résultant de la loi n° du relative à la reconnaissance biométrique dans l'espace public, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna, sous réserve des adaptations prévues au présent titre et aux seules exceptions : ».

⑥ IV. – La présente loi est applicable sur l'ensemble du territoire national.