Commission DES LOIS

SÉNAT

…le rapport d'information

LA RECONNAISSANCE BIOMÉTRIQUE DANS L'ESPACE PUBLIC : 30 PROPOSITIONS POUR ÉCARTER LE RISQUE D'UNE SOCIÉTÉ DE SURVEILLANCE

Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain, rapporteurs

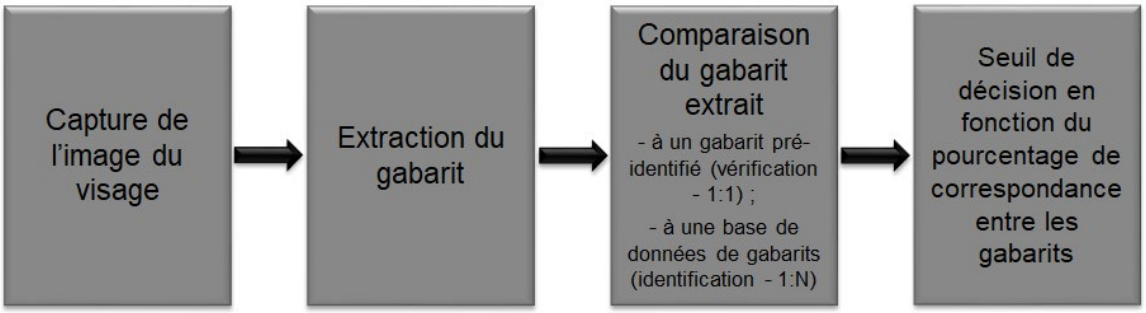
En octobre 2020, la commission des lois du Sénat a créé en son sein une mission d'information sur la reconnaissance faciale, une **technologie qui se développe rapidement grâce aux algorithmes d'apprentissage** et **polarise l'opinion publique** entre les tenants d'un moratoire portant sur toutes les technologies biométriques, qui seraient par nature attentatoires aux libertés, et ceux qui mettent en exergue leurs importants bénéfices potentiels.

À l'heure où une législation sur l'intelligence artificielle est en cours d'élaboration au niveau européen, il est indispensable de construire une **réponse collective** à l'utilisation des technologies de reconnaissance biométrique afin de ne pas être, dans les années à venir, dépassés par les développements industriels.

1. LA RECONNAISSANCE FACIALE : UNE TECHNOLOGIE AUX MULTIPLES FACETTES SOULEVANT DE NOMBREUX ENJEUX DE LIBERTÉ ET DE SOUVERAINETÉ

Parmi les techniques biométriques, qui regroupent l'ensemble des procédés automatisés permettant de reconnaître un individu à partir de la quantification de ses caractéristiques physiques, physiologiques ou comportementales, la reconnaissance faciale vise à **reconnaître une personne sur la base des données caractéristiques de son visage**.

Elle s'effectue en deux étapes : le visage de la personne est d'abord **capté et transformé 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**.



Source : Commission des lois du Sénat

Les cas d'usage de cette technologie sont **potentiellement illimités**. Ainsi, sans que cette liste soit exhaustive, la reconnaissance faciale 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.

En France, les usages pérennes dans les espaces accessibles au public sont extrêmement limités. Il s'agit pour l'essentiel du dispositif de rapprochement par photographie opéré dans le **Traitement des antécédents judiciaires** (TAJ) et du système Parafe 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.

Les questions que pose le déploiement de la reconnaissance faciale sont nombreuses. Elles ont trait tant aux libertés publiques qu'à la souveraineté technologique de la France, les deux thématiques étant interdépendantes.

Dans ce contexte, il est surprenant que la reconnaissance faciale, et plus largement les techniques de reconnaissance biométrique, ne fasse pas l'objet d'un encadrement *ad hoc*. Elles sont actuellement exclusivement **régies par le droit des données personnelles**.

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.

2. ÉCARTER LE RISQUE D'UNE SOCIÉTÉ DE SURVEILLANCE EN EXPÉRIMENTANT AU CAS PAR CAS

A. DÉFINIR COLLECTIVEMENT UN CADRE COMPRENANT DES LIGNES ROUGES, UNE MÉTHODOLOGIE ET UN RÉGIME DE REDEVABILITÉ

a) Des lignes rouges écartant le risque d'une société de surveillance

Les rapporteurs considèrent qu'il est indispensable de fixer dans la loi **quatre interdictions** applicables aux acteurs publics comme privés :

Interdictions

- Interdiction de la **notation sociale**. Cette interdiction irait au-delà de celle proposée par la Commission européenne dans le règlement sur l'intelligence artificielle puisque cette dernière ne s'intéresse qu'aux acteurs publics. Il est en effet nécessaire de protéger les consommateurs de méthodes commerciales intrusives et d'empêcher le recours à la notation sociale par surveillance de leurs comportements dans les espaces de vente, de restauration ou les centres de loisirs ;

- Interdiction de la **catégorisation d'individus en fonction de l'origine ethnique, du sexe, ou de l'orientation sexuelle**, sauf dans le cadre de la recherche scientifique et sous réserve de garanties appropriées ;

- Interdiction de **l'analyse d'émotions**, sauf à des fins de santé ou de recherche scientifique et sous réserve de garanties appropriées ;

- Interdiction de la **surveillance biométrique à distance en temps réel dans l'espace public**, sauf exceptions très limitées au profit des forces de sécurité ; en particulier, cette interdiction porterait sur la surveillance biométrique à distance en temps réel lors de **manifestations sur la voie publique** et aux abords des **lieux de culte**.

Les rapporteurs préconisent également de **poser trois principes généraux** :

Principes généraux

- le principe de **subsidiarité,** pour que la reconnaissance biométrique ne soit utilisée que lorsqu'elle est vraiment nécessaire ;

- le principe d'un **contrôle humain systématique** afin qu'il ne s'agisse que d'une aide à la décision ;

- et le principe de **transparence** pour que l'usage des technologies de reconnaissance biométrique ne se fasse pas à l'insu des personnes.

b) Une méthodologie claire : la voie expérimentale dans le cadre d'une loi

La mission est favorable à l'adoption d'une **loi d'expérimentation** pour créer le débat et déterminer les usages de la reconnaissance biométrique qui pourraient être pertinents et efficaces. L'expérimentation pourrait être **autorisée pour une période de trois ans**, ce qui obligerait le Gouvernement et le Parlement à réévaluer le besoin et recadrer le cas échéant le dispositif en fonction des résultats obtenus.

Pour que cette phase d'expérimentation soit utile, serait mise en place une **évaluation publique et indépendante** pour connaître l'efficacité de la technologie dans le cas d'usage testé. Elle serait conduite par un comité composé de scientifiques et de spécialistes des questions éthiques dont les **rapports seraient rendus publics**.

Pour que les Français s'emparent du sujet en étant suffisamment à même d'en comprendre les différents enjeux, il est préconisé de rendre accessible **une information claire sur les techniques de reconnaissance biométrique**, les bénéfices qui en sont attendus et les risques encourus.

c) Un régime de contrôle *a priori* et *a posteriori*

La mission souhaite que les usages soient **autorisés *a priori***. En cas d'utilisation par les **forces de sécurité intérieure**, l'autorisation relèverait **soit d'un magistrat, soit du préfet**, selon qu'on s'insère dans un cadre de police judiciaire ou de police administrative. En cas de déploiement par un **acteur privé** dans un lieu accessible au public, la **CNIL** serait compétente.

La CNIL serait systématiquement consultée pour tout déploiement : pour les usages publics, parce que les analyses d'impact devraient impérativement lui être transmises pour avis, et pour les usages privés, parce qu'elle aurait à délivrer l'autorisation préalable.

Ces différentes autorisations feraient l'objet d'un **recensement national** pour garder une vision globale du recours aux techniques de reconnaissance biométrique, quelle que soit l'autorité ayant délivré l'autorisation.

Enfin, le pouvoir de contrôle de la CNIL serait réaffirmé afin qu'elle exerce **son rôle de gendarme de la reconnaissance biométrique**, qu'elle mène des **contrôles *a posteriori*** du bon usage des dispositifs et des éventuels détournements de finalité en

dehors de l'autorisation. Dans ce cadre, les rapporteurs rappellent l'importance de lui accorder les moyens humains, financiers et institutionnels adéquats.

B. RECENTRER LE DÉBAT DU CADRE JURIDIQUE SUR LES CAS D'USAGE

a) Autoriser, à titre expérimental, le traitement des images à l'aide de l'intelligence artificielle dans le cadre des finalités attribuées au dispositif de vidéoprotection déployé

Les cas d'usage de la reconnaissance faciale étant multiples et potentiellement illimités, **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 ainsi être opérées, les risques pour les libertés étant dans une large mesure conditionnées par celles-ci.

Les dispositifs de traitement des images sans utilisation de données biométriques se multiplient. Il peut s'agir de dispositifs de suivi ou de traçage, de détection d'évènements suspects ou d'objets abandonnés, ou de caractérisation de personnes filmées. À ce jour cependant, les traitements des images issues de la voie publique en s'appuyant sur l'intelligence artificielle **ne disposent pas d'un cadre juridique propre**. Il y a donc un débat sur la possibilité de les déployer. Certaines communes ont d'ores et déjà mis en place des systèmes de détection automatique des dépôts sauvages d'ordures, par exemple.

Les rapporteurs considèrent que l'application de l'intelligence artificielle aux images issues de la vidéoprotection constitue un **changement d'échelle dans l'exploitation de la vidéoprotection** ce qui, étant susceptible de porter atteintes aux libertés individuelles, nécessite une **base législative explicite**. Cette base est d'autant plus urgente que le déploiement de systèmes de détection de colis abandonnés ou de mouvements suspects dans une foule sera nécessaire pour assurer la sécurité au moment des Jeux Olympiques de 2024.

Il est donc proposé d'établir, **à titre expérimental**, une base législative qui permettrait aux opérateurs des systèmes de vidéoprotection dans les espaces accessibles au public de mettre en œuvre des **traitements d'images par intelligence artificielle**, sans traitement de données biométriques. **Ces traitements devraient s'inscrire dans les missions des personnes publiques et privées concernées et, surtout, dans les finalités attribuées au dispositif de vidéoprotection déployé**.

b) L'authentification biométrique en vue de permettre un contrôle d'accès sécurisé

S'agissant des logiciels de reconnaissance biométrique, notamment à partir de la biométrie du visage, **une distinction doit être effectuée entre authentification et identification**.

L'authentification biométrique, qui permet un contrôle sécurisé et fluidifié des accès, est **plus propice au recueil du consentement de la personne,** tout en constituant un **système moins intrusif**, car celui-ci peut dans certains cas être construit de façon à ce que le fournisseur de technologie n'ait pas accès aux données biométriques des personnes. Ainsi, dans le cadre français et européen actuel, des cas d'usage ont été mis en œuvre sur la base du consentement des personnes.

La mission propose de **donner une base légale à ces dispositifs** imposant aux personnes souhaitant les mettre en place de nombreuses **garanties** permettant, d'une part, d'**évaluer l'impact du dispositif** et, d'autre part, de s'assurer du **caractère libre, spécifique, éclairé et univoque du consentement donné**.

Dans certains cas très particuliers et à titre expérimental, ces dispositifs pourraient également être rendus possibles de manière obligatoire, pour accéder à des zones nécessitant une sécurisation exceptionnelle.

c) L'identification biométrique, *a posteriori* ou en temps réel

Les opérations d'identification biométriques doivent, quant à elles, faire l'objet d'un encadrement extrêmement strict au regard des risques encourus et être proportionnées

aux modalités d'usages, qu'il s'agisse d'une **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, **ou d'une utilisation *a posteriori***, par exemple dans le cadre d'une enquête. Dans ce second cas, les recherches se font généralement sur des enregistrements.

S'agissant d'abord de l'**identification *a posteriori***, la mission propose :

- en premier lieu, **de permettre une utilisation de la biométrie dans les fichiers de police, dans le cadre d'enquêtes judiciaires ou d'opérations de renseignement**. Il s'agit d'un moyen de fiabilisation et d'opérationnalisation des fichiers, dont le mouvement est déjà enclenché au niveau européen ;
- en deuxième lieu, **d'autoriser à titre expérimental** et de manière subsidiaire, uniquement pour **la recherche d'auteurs ou de victimes potentielles des infractions les plus graves**, l'exploitation *a posteriori* d'images **sous le contrôle du magistrat en charge de l'enquête ou de l'instruction ;**
- en troisième lieu, de **créer une technique de renseignement donnant aux services la possibilité d'utiliser des systèmes de reconnaissance faciale afin d'identifier une personne recherchée ou de reconstituer son parcours *a posteriori***. Un tel usage se révèlerait en particulier pertinent dans le cadre de la mission de prévention de toute forme d'ingérence étrangère, aux fins de détecter la présence sur le sol national d'agents de services étrangers qui entrent en France sous une fausse identité.

S'agissant ensuite de l'**identification biométrique à distance en temps réel**, les rapporteurs insistent sur leur volonté de lui **conserver un caractère particulièrement exceptionnel**. Sur leur proposition, la mission n'a donc prévu son déploiement que par exception, dans trois cas très spécifiques et circonscrits :

- dans le cadre **d'enquêtes judiciaires**, en vue de permettre, d'une part, **le suivi d'une personne venant de commettre une infraction grave** à partir des images issues de la vidéoprotection afin de faciliter son 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**. Les infractions concernées pourraient par exemple être limitées aux crimes menaçant ou portant atteinte à l'intégrité physique des personnes ;
- dans un **cadre administratif**, en vue de **sécuriser de grands évènements présentant une sensibilité particulière ou les sites particulièrement sensibles face à une éventuelle menace terroriste**. La détection ne pourrait se faire que sur un périmètre géographique limité et pour une période précisément déterminée ;
- dans un cadre de **renseignement**, en cas de **menaces imminentes pour la sécurité nationale.**

Ces déploiements devront en outre être entourés de **solides garanties**, notamment :

- la nécessité d'une **autorisation** et d'un **contrôle** d'une autorité, distincte en fonction des usages (magistrat, préfet ou Commission nationale de contrôle des techniques de renseignement) ;
- le caractère strictement **subsidiaire** de ces usages ;
- la **traçabilité** des usages ;
- la systématicité d'une supervision humaine, les technologies étant cantonnées à un **rôle d'aide à la décision** ;
- une **information du public** adaptée aux spécificités du déploiement.

d) Un usage de la reconnaissance biométrique par les acteurs privés fondé sur le consentement des usagers

S'agissant enfin des **usages des technologies de reconnaissance biométrique par les acteurs privés**, les rapporteurs considèrent qu'ils doivent être extrêmement limités et se baser, de manière générale, sur le consentement des personnes. En particulier, la mission souhaite interdire toute identification sur la base de données biométriques en temps réel ou en temps différé par des acteurs privés.

C. RENFORCER LA SOUVERAINETÉ TECHNOLOGIQUE DE LA FRANCE ET DE L'EUROPE

Les rapporteurs considèrent **qu'en matière de reconnaissance biométrique, la protection de notre autonomie technologique et la sauvegarde des libertés publiques sont les deux faces d'une même médaille**. L'usage d'algorithmes développés en Europe, à partir de données traçables et hébergées sur notre sol est par exemple largement préférable au recours à des algorithmes étrangers dont l'on ne sait parfois rien des conditions de création et d'entraînement.

Si la France dispose d'un **écosystème de recherche et de développement très performant** dans le champ de la reconnaissance biométrique, force est de constater que les acteurs du secteur évoluent dans **un cadre juridique et matériel peu propice à la recherche et au développement**. Ainsi, la mission d'information a identifié deux obstacles principaux :

- **un cadre juridique applicable à la recherche et au développement particulièrement complexe**, si bien que les acteurs du secteur n'arrivent pas toujours à distinguer ce qui est autorisé de ce qui ne l'est pas ;
- **la difficile constitution des jeux de données destinés à l'apprentissage des algorithmes** : l'obligation de recueillir le consentement de chaque personne figurant dans la base pour chaque projet de recherche rend très difficile la création de ce matériel. Cela est même quasiment impossible pour des laboratoires de recherche publique.

Pour renforcer la souveraineté technologique de l'Europe, les rapporteurs préconisent de **confier à une autorité européenne la mission d'évaluer la fiabilité des algorithmes de reconnaissance biométrique et de certifier leur absence de biais**, sur le modèle de ce qui existe déjà aux États-Unis. Il s'agit de réduire notre dépendance à l'extérieur sur cette mission d'apparence technique mais en réalité cruciale en termes de protection des libertés. Pour donner à cette autorité les moyens de son action, une **base d'images à l'échelle de l'Union européenne pourrait être créée** et alimentée, sous réserve de garanties appropriées, par la réutilisation de données détenues par les administrations des États membres ou par des contributions altruistes.

Pour lever les obstacles à la recherche et au développement, les rapporteurs plaident également pour l'établissement d'un **cadre juridique spécifique et adapté à cette activité**. Cela se traduirait, dans le respect des garanties prévues par le RGPD, par **des assouplissements des modalités pratiques de recueil du consentement** ou bien par des mécanismes sécurisés de mise à disposition de données biométriques détenues par l'État aux seuls laboratoires de recherche publique. Ce cadre juridique dérogatoire devrait être accompagné de fortes garanties. À titre d'exemple, cette réutilisation de données publiques serait subordonnée à un avis favorable de la CNIL.

LES CONSTATS

- **Un développement rapide des technologies de reconnaissance faciale, celles-ci étant considérées comme matures par les industriels.**
- **Une forte polarisation du débat sur les techniques de reconnaissance biométrique, entre les tenants d'un moratoire sur les technologies biométriques et ceux qui, à l'inverse, mettent en exergue leurs bénéfices opérationnels.**
- **L'absence d'encadrement juridique *ad hoc*, dans l'attente du règlement européen sur l'intelligence artificielle.**
- **Une utilisation croissante de la « vidéoprotection intelligente » en l'absence de cadre législatif propre.**
- **Des acteurs publics comme privés qui évoluent dans un cadre juridique et matériel peu favorable à la recherche et au développement.**

LES PRINCIPALES PROPOSITIONS

- **Écarter le risque d'une société de surveillance en fixant des lignes rouges au-delà desquelles aucun usage de la reconnaissance biométrique ne pourrait être admis, à l'instar des lignes rouges fixées en matière de bioéthique.**
- **Fixer dans une loi d'expérimentation, pour une période de trois ans, les conditions dans lesquelles et les finalités pour lesquelles la reconnaissance biométrique pourra faire l'objet de nouvelles expérimentations par les acteurs publics ou dans les espaces ouverts au public.**
- **Créer un cadre de redevabilité afin d'assurer le contrôle et l'évaluation des expérimentations mises en œuvre.**
- **Fixer dans la loi les cas d'usage possibles des techniques de reconnaissance biométrique, en distinguant selon les risques encourus. Entourer les éventuels déploiements de solides garanties.**
- **Créer un tiers de confiance européen ayant pour mission l'évaluation de la fiabilité des algorithmes de reconnaissance biométrique et la certification de leur absence de biais.**
- **Mettre en place un cadre juridique stable et spécifique à la recherche et au développement afin de favoriser la compétitivité des acteurs européen dans le respect des droits et libertés des personnes.**

POUR EN SAVOIR +

- **Rapport d'information n° 788 (2015-2016), *Biométrie : mettre la technologie au service des citoyens*, de François Bonhomme et Jean-Yves Leconte, fait au nom de la commission des lois et publié le 13 juillet 2016. Le rapport est consultable à l'adresse suivante : https://www.senat.fr/notice-rapport/2015/r15-788-notice.html**
- **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). La note est consultable à l'adresse suivante : https://www.senat.fr/opecst/notes.html**
- ***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**
- ***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**
- ***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**
- ***Pour un usage responsable et acceptable par la société des technologies de sécurité*, Rapport au Premier ministre par Jean-Michel Mis, député, remis en septembre 2021. 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**
- ***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**

François-Noël Buffet

Président de la commission

Sénateur (Les Républicains) du Rhône

Marc-Philippe Daubresse

Rapporteur

Sénateur (Les Républicains) du Nord

Arnaud de Belenet

Rapporteur

Sénateur (Union Centriste) de la Seine-et-Marne

Jérôme Durain

Rapporteur

Sénateur (Socialiste, Écologiste et Républicain) de la Saône-et-Loire

Commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale

http://www.senat.fr/commission/loi/index.html

Téléphone : 01.42.34.23.37

Consulter le rapport :

http://www.senat.fr/rap/r21-627/r21-627.html

ANNEXE : LISTE DES PROPOSITIONS DE LA MISSION D'INFORMATION

I. DÉFINIR COLLECTIVEMENT UN CADRE COMPRENANT DES LIGNES ROUGES, UNE MÉTHODOLOGIE ET UN RÉGIME DE REDEVABILITÉ

1. Réaliser une enquête nationale visant à évaluer la perception de la reconnaissance biométrique par les Français, à cerner les cas d'usages auxquels ils se montrent plus ou moins favorables et à identifier les ressorts d'une meilleure acceptabilité de cette technologie.

Des lignes rouges écartant le risque d'une société de surveillance

2. Fixer dans la loi les cas où le développement, la mise sur le marché et l'utilisation de techniques de reconnaissance biométrique sont interdites, qu'elles soient mises en œuvre par des acteurs publics ou privés. En particulier :

- les systèmes de notation sociale des personnes ;

- les systèmes de catégorisation des personnes selon une origine, des convictions religieuses ou philosophiques ou une orientation sexuelle, sauf à des fins de recherche scientifique et sous réserve de garanties appropriées ;

- les systèmes de reconnaissance d'émotions, sauf à des fins de santé ou de recherche scientifique et sous réserve de garanties appropriées.

3. D'une manière générale, interdire l'utilisation de la reconnaissance biométrique à distance en temps réel dans l'espace public, sauf exceptions très limitées (voir la proposition n° 22) ; en particulier, interdire clairement la surveillance biométrique à distance en temps réel lors de manifestations sur la voie publique et aux abords des lieux de culte.

4. Appliquer systématiquement le principe de subsidiarité et en particulier, conditionner le recours sans consentement à la reconnaissance biométrique à la démonstration d'un impératif particulier d'assurer un haut niveau de fiabilité de l'authentification ou de l'identification des personnes concernées et la démonstration de l'inadéquation d'autres moyens de sécurisation moins intrusifs.

5. Cantonner le recours aux algorithmes et à la technologie d'identification par reconnaissance biométrique, lorsqu'elle est déployée par exception, à un rôle d'aide à la décision et prévoir un contrôle humain systématique.

6. Assurer la transparence de l'usage de technologies de reconnaissance biométrique à l'égard des personnes par la fourniture d'informations claires, compréhensibles et aisément accessibles.

Une méthodologie claire : la voie expérimentale dans le cadre d'une loi

7. Fixer dans une loi d'expérimentation, pour une période de trois ans, les conditions dans lesquelles et les finalités pour lesquelles la reconnaissance biométrique pourra faire l'objet de nouvelles expérimentations par les acteurs publics ou dans les espaces ouverts au public et prévoir la remise de rapports annuels détaillés au Parlement sur son application, dont le dernier au plus tard six mois avant la fin de la période d'expérimentation.

8. Soumettre ces expérimentations à l'évaluation régulière d'un comité scientifique et éthique unique et indépendant dont les rapports seront rendus publics.

9. En accompagnement de ces expérimentations, apporter une information accessible à tous sur les techniques de reconnaissance biométrique, les bénéfices qui en sont attendus et les risques encourus afin de sensibiliser le public sur leurs enjeux.

Un régime de contrôle a priori *et* a posteriori

10. Soumettre le déploiement des technologies de reconnaissance biométrique par les pouvoirs publics à l'autorisation du préfet en matière de police administrative ou d'un magistrat en matière de police judiciaire.

11. Soumettre le déploiement des technologies de reconnaissance biométrique par les acteurs privés dans les espaces accessibles au public à l'autorisation de la Commission nationale de l'informatique et des libertés (CNIL).

12. Prévoir le recensement au niveau national des actes autorisant le déploiement des technologies de reconnaissance biométrique.

13. Renforcer les moyens de la CNIL afin qu'elle puisse, le cas échéant avec l'assistance du Pôle d'expertise de la régulation numérique (PEReN), assurer le suivi du déploiement des techniques de reconnaissance biométrique, détecter d'éventuels détournements de finalité ou des usages illégaux de ces technologies et sanctionner les contrevenants.

II. RECENTRER LE DÉBAT DU CADRE JURIDIQUE SUR LES CAS D'USAGE

Distinguer technologies de reconnaissance biométrique et technologies connexes

14. Autoriser, à titre expérimental, l'usage de traitements d'images issues des espaces accessibles au public à l'aide de l'intelligence artificielle sans utilisation de données biométriques dans le cadre des finalités attribuées au dispositif de vidéoprotection déployé, après autorisation du préfet territorialement compétent et consultation, le cas échéant, de la CNIL. Assurer l'information du public.

15. Prévoir les conditions dans lesquelles le droit d'opposition des personnes concernées peut être écarté lors du déploiement de dispositifs de traitements d'images provenant d'espaces accessibles au public n'impliquant pas des données sensibles à des fins de traitement statistique d'un groupe de personnes.

L'authentification biométrique en vue de permettre un contrôle d'accès sécurisé

16. Créer, à titre expérimental, un cadre juridique permettant l'usage de technologies d'authentification biométrique pour sécuriser l'accès à certains évènements et fluidifier les flux, sur la base du consentement des personnes. Accompagner l'ouverture de cette possibilité de fortes garanties, comprenant notamment :

- la réalisation d'une étude d'impact justifiant l'intérêt de cette technologie ainsi que les mesures de protection des données personnelles mises en œuvre, notamment en matière de sécurisation des systèmes informatiques ;

- les modalités de recueil du consentement des personnes concernées ;

- l'obligation de maintenir une alternative valable à l'usage de l'authentification biométrique ;

- l'absence de conservation des images collectées et analysées des personnes se présentant au contrôle d'accès ;

- le maintien d'un contrôle humain.

17. Tout en conservant le principe d'une interdiction de l'usage de la biométrie pour l'accès à certains lieux sans alternative non biométrique, 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.

Distinguer, au sein des dispositifs d'identification biométrique, l'identification en temps réel de celle réalisée a posteriori

18. Mettre en place, par la prise de décrets en Conseil d'État, la possibilité pour les forces de sécurité nationales d'interroger à l'occasion d'une enquête judiciaire ou dans un cadre de renseignement certains fichiers de police par le biais d'éléments biométriques. Opérer, par ce biais, une fiabilisation des fichiers concernés pour éviter les identités multiples.

19. Évaluer l'efficacité des modules de reconnaissance faciale dans le Traitement des antécédents judiciaires (TAJ) ainsi que, le cas échéant, dans les autres fichiers de police où un tel module serait mis en place.

20. 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.

21. Autoriser, à titre expérimental, les services spécialisés de renseignement à traiter *a posteriori* les images issues de la voie publique à l'aide de systèmes de reconnaissance biométrique, dans le cadre des seules finalités mentionnées aux 1°, 2°, 4° et 5° de l'article L. 811-3 du code de la sécurité intérieure.

22. 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 et de sites sensibles face à une menace terroriste, pour faire face à une menace imminente pour la sécurité nationale, et à des fins d'enquête judiciaire relatives à des infractions graves menaçant ou portant atteinte à l'intégrité physique des personnes. Ce système devrait être strictement encadré, les garanties prévues incluant notamment :

- le caractère strictement subsidiaire du déploiement de cette technologie ;

- un déploiement du dispositif autorisé *a priori* et contrôlé *a posteriori* par une autorité adaptée à la finalité du traitement (magistrat, préfet, Commission nationale de contrôle des techniques de renseignement – CNCTR), dans un périmètre spatio-temporel rigoureusement délimité ;

- en matière de police administrative, un nombre de caméras proportionné pouvant être utilisées dans ce cadre ;

- une minimisation des données utilisées et leur sécurisation ;

- une supervision humaine systématique ;

- une traçabilité des usages ;

- une information du public adaptée aux spécificités du déploiement et, en tout état de cause, une information générale réalisée par le Gouvernement.

Un usage de la reconnaissance biométrique par les acteurs privés fondé sur le consentement des usagers

23. Interdire tout usage privé des technologies de reconnaissance biométrique ne requérant pas le consentement des utilisateurs, à l'exception, dans quelques rares cas particuliers et dûment justifiés, de traitements pour contrôler l'accès aux lieux et aux outils de travail (accès à des zones ou à des produits nécessitant un niveau de protection particulièrement élevé).

III. RENFORCER LA SOUVERAINETÉ TECHNOLOGIQUE DE LA FRANCE ET DE L'EUROPE

La nécessaire création d'un tiers de confiance européen

24. Dans le cadre des négociations sur la législation européenne sur l'intelligence artificielle, promouvoir la création d'une autorité européenne ayant pour mission l'évaluation de la fiabilité des algorithmes de reconnaissance biométrique et la certification de leur absence de biais.

Assurer l'indépendance et la qualité de l'évaluation en garantissant la diversité des données qui y sont contenues et en ayant recours à la méthodologie des « données séquestrées », où les développeurs n'ont accès à la base de données ni pour l'entrainement des algorithmes ni pour la phase de test.

Mettre à disposition de l'autorité en charge de l'intelligence artificielle une base d'images à l'échelle de l'Union européenne afin de lui donner les moyens de son action. Alimenter cette base à travers plusieurs mécanismes s'inspirant de la proposition de règlement de l'Union européenne sur la gouvernance européenne des données.

Mettre en place des mécanismes adaptés d'information des citoyens et prévoir la possibilité de demander à tout moment le retrait de ses données de la base.

Lever les obstacles à la recherche et au développement par la mise en place d'un cadre juridique stable et spécifique, et faciliter l'accès aux jeux de données pour la recherche publique

25. Créer un cadre juridique spécifique et adapté à la recherche et au développement visant notamment à autoriser, sous réserve d'une déclaration préalable à la CNIL, la réutilisation de données par l'intermédiaire de recueils de consentement groupés.

26. Formaliser la doctrine de la CNIL sur la recherche et le développement en matière de reconnaissance biométrique au sein d'un document unique à destination des développeurs.

27. Anticiper l'adoption du règlement sur la gouvernance européenne des données en autorisant, sous réserve d'un avis favorable de la CNIL, la mise à disposition de données publiques biométriques à des fins de recherche publique sur la reconnaissance biométrique.

Imposer que la mise à disposition se fasse dans un environnement de traitement sécurisé fourni par l'État et sans possibilité d'en exporter les données.

28. Mettre en place au sein de l'État, un service dédié à l'accompagnement des demandes de réutilisation de données publiques de la part des acteurs de la recherche en reconnaissance biométrique.

Conserver la maîtrise technologique des algorithmes en assurant la traçabilité des données utilisées et la sécurité des infrastructures d'hébergement

29. Créer un dispositif de labellisation des logiciels de reconnaissance biométrique, en prenant notamment en compte l'origine et la traçabilité des données d'apprentissage.

30. Prévoir un contrôle régulier par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de la sécurité des infrastructures d'hébergement des données biométriques utilisées par la puissance publique à des fins expérimentales.