N° 627

# SÉNAT

SESSION ORDINAIRE DE 2021-2022

Enregistré à la Présidence du Sénat le 10 mai 2022

# RAPPORT D'INFORMATION

FAIT

*au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur la* **reconnaissance faciale** *et ses* **risques** *au regard de la* **protection** *des* **libertés individuelles***,*

Par MM. Marc-Philippe DAUBRESSE, Arnaud de BELENET et Jérôme DURAIN,

Sénateurs

*(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. Alain Richard, 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. Ludovic Haye, 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. Thani Mohamed Soilihi, Jean-Yves Roux, Jean-Pierre Sueur, Mmes Lana Tetuanui, Claudine Thomas, Dominique Vérien, M. Dany Wattebled.

# S O M M A I R E

Pages

# AVANT-PROPOS

Les technologies de reconnaissance biométrique ont été popularisées dans l'imaginaire collectif par de nombreuses fictions. Ainsi, tant George Orwell dans son roman *1984* publié en 1949, que Steven Spielberg dans son film *Minority Report* sorti en 2002, ont souligné les risques des nouvelles technologies dans l'établissement d'une société de surveillance.

Le débat est désormais particulièrement polarisé entre les tenants d'un moratoire sur les technologies biométriques et ceux qui, à l'inverse, mettent en exergue leurs bénéfices opérationnels tant pour favoriser la sécurité des personnes et des biens que pour apporter un plus grand confort en facilitant un certain nombre d'actes de la vie quotidienne.

Parmi les technologies de reconnaissance biométriques, la reconnaissance faciale concentre l'attention. Le visage, qui conditionne selon Emmanuel Levinas « l'expérience d'autrui », nous appartient en effet en propre tout en étant offert à tous. Le déploiement de la reconnaissance faciale s'effectue cependant sans encadrement juridique spécifique, ni réflexion éthique collective.

Les possibilités d'usage de la reconnaissance faciale sont déterminées, aujourd'hui, par la règlementation relative à la protection des données personnelles. Les usages de cette technologie sont à ce jour limités, car lorsqu'ils ne se basent pas sur le consentement des personnes, ils nécessitent l'adoption d'une disposition législative ou règlementaire particulière. Deux usages développés par les forces de sécurité intérieure peuvent par exemple être cités : le dispositif PARAFE, qui permet des passages frontaliers sur la base d'une authentification biométrique, ou l'introduction d'un module de reconnaissance faciale d'aide à la décision sur le fichier du traitement des antécédents judiciaires (TAJ). Plusieurs expérimentations de la reconnaissance faciale dans les espaces accessibles au public ont par ailleurs été conduites par des acteurs privés sur la base du consentement des personnes, mais aucune d'entre elles n'a été pérennisée. Toutefois, malgré ces emplois marginaux dans l'espace public, la reconnaissance faciale se banalise avec une multiplication d'usages individuels dans la vie quotidienne, comme le déverrouillage de téléphones ou l'ouverture de comptes bancaires.

Il est donc impératif de construire une réponse collective sur l'utilisation de ces technologies, afin de ne pas être, dans les années à venir, dépassés par les développements industriels. C'est la raison pour laquelle la

commission des lois du Sénat a créée en son sein une mission d'information sur la reconnaissance faciale, ses risques en matière de surveillance et de libertés publiques, en en désignant rapporteurs Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain.

Après avoir près de 120 personnes et réalisé 4 déplacements, la mission en est arrivée à la conclusion que, compte tenu du changement d'échelle impliqué par ces technologies dans la capacité d'exploitation des images captées dans des espaces accessibles au public, il était impératif qu'un encadrement des technologies biométriques soit réalisé au niveau législatif. Elle a également conclu qu'il fallait, de manière très claire, rejeter le modèle d'une société de surveillance en établissant d'abord des lignes rouges, compte tenu de la multiplicité des cas d'usage de la reconnaissance faciale, potentiellement illimités. Ce n'est qu'une fois ces lignes posées qu'un raisonnement cas d'usage par cas d'usage doit s'imposer, car tous les usages permis par la technologie de reconnaissance faciale ne soulèvent pas les mêmes risques au regard des libertés.

La mission d'information s'est en conséquence prononcée en faveur d'une démarche d'expérimentations permettant :

- en premier lieu, de définir au cas par cas les utilisations des technologies de reconnaissance faciale, et plus généralement biométrique, dans les espaces publics pouvant être acceptables au regard notamment du bénéfice obtenu et des principes de nécessité et de proportionnalité ;

- en second lieu, d'établir un régime de redevabilité et de contrôle adapté, afin notamment d'assurer une information effective des personnes concernées. À défaut, le risque est celui d'une banalisation des technologies biométriques au détriment de l'élaboration d'une réponse collective à leur usage. Leur complexité ainsi que leur constante évolution rendent en effet délicate l'appréhension théorique de ces technologies par les citoyens. Il est donc impératif d'instruire le débat avec le résultat des expériences réalisées au cours des expérimentations.

Parallèlement, il importe d'assurer notre souveraineté technologique afin de renforcer la maîtrise des données de nos concitoyens. Il n'est pas acceptable que l'encadrement de la recherche et développement au niveau français et européen obère l'élaboration de solutions techniques souveraines et conduise les acteurs publics et privés à privilégier des solutions développées à l'étranger, avec des niveaux de contraintes bien moindre. La France et l'Union européenne ont un rôle à jouer dans l'encouragement de technologies de qualité développées de façon éthique.

# L'ESSENTIEL

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.

## I. 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**.

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.

## II. 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 :

- 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** :

- 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.

# LISTE DES PROPOSITIONS

## 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 statistiques 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 biométriques, 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, CNCTR), dans un périmètre spatiotemporel 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.

# PREMIÈRE PARTIE
# UNE TECHNOLOGIE AUX MULTIPLES FACETTES SOULEVANT DE NOMBREUX ENJEUX DE LIBERTÉ ET DE SOUVERAINETÉ

## *I.* LA RECONNAISSANCE FACIALE : UNE TECHNOLOGIE AUX MULTIPLES FACETTES

### *A. DÉFINITION : UNE TECHNOLOGIE BIOMÉTRIQUE PROBABILISTE DESTINÉE À L'AUTHENTIFICATION OU À L'IDENTIFICATION DES INDIVIDUS*

#### 1. La reconnaissance faciale : une technologie biométrique informatique et probabiliste de reconnaissance des visages

Au cours des dernières années, le déploiement de dispositifs biométriques s'est fortement accéléré en France et en Europe. Cette accélération est principalement due aux avancées des algorithmes d'apprentissage sur lesquels s'appuient ces technologies, dont la puissance de calcul permet désormais **une exploitation massive de grands ensembles de données**.

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 (empreintes digitales, iris, *etc.*)[1], **la reconnaissance faciale vise à reconnaître une personne sur la base des données caractéristiques de son visage**. Depuis son invention dans les années 1970, la reconnaissance faciale a énormément progressé et s'impose aujourd'hui comme une technologie mature permettant d'identifier ou de reconnaître une personne en s'appuyant sur les spécificités biométriques de son visage.

[1] *Ces caractéristiques sont qualifiées de données biométriques par le règlement général sur la protection des données (RGPD) – 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), car elles permettent ou confirment l'identification unique d'une personne.

**Données biométriques**

Le règlement général sur la protection des données qualifie, dans son article 4-14, 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* ».

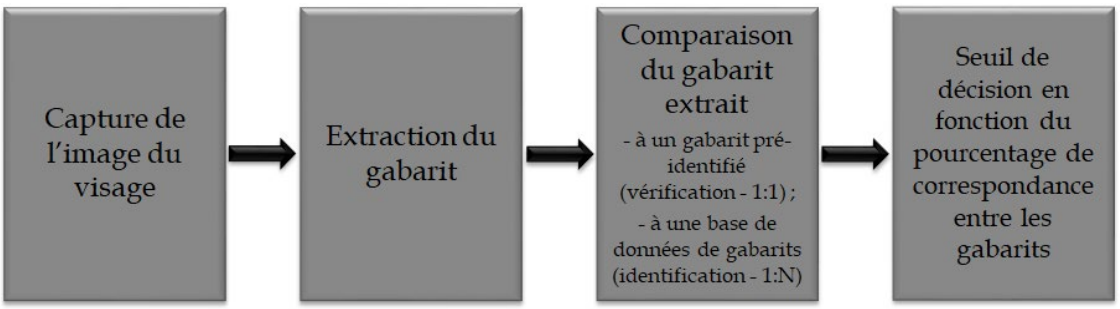
Ces données sont considérées comme des **données sensibles** au sens de l'article 9 du RGPD.

**La reconnaissance faciale – ou reconnaissance à partir de la biométrie du visage – s'opère en deux étapes :**

- d'abord, **la collecte du visage et sa transformation en un gabarit** : sur la base d'une image du visage de la personne, qui peut être recueillie à partir d'une photographie ou d'une vidéo, le logiciel de biométrie du visage extrait un modèle représentant d'un point de vue informatique certaines caractéristiques de ce visage. Ce modèle, dénommé « gabarit », est considéré comme unique et propre à chaque personne et est en principe permanent dans le temps ;

- ensuite, **la reconnaissance de ce visage par comparaison du gabarit correspondant avec un ou plusieurs autres gabarits**, préalablement réalisés ou calculés en direct à partir d'une image, photographie ou vidéo. Cette comparaison permet de déterminer si les gabarits concernés correspondent à une même personne.

**La reconnaissance d'une personne à partir de la biométrie du visage est une technique probabiliste**, car les résultats de comparaison entre les gabarits sont exprimés en pourcentage de correspondance. Si ce pourcentage dépasse un seuil déterminé par le système, celui-ci va considérer qu'il y a correspondance.




*Source : Commission des lois du Sénat*

### 2. Deux finalités : l'authentification et l'identification d'une personne

Comme toute technique biométrique, la reconnaissance faciale peut remplir deux fonctions distinctes.

**L'authentification (ou la vérification)** tout d'abord, qui consiste à **vérifier qu'une personne est bien celle qu'elle prétend être**. Le système compare alors un gabarit biométrique préenregistré avec celui extrait du visage 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 »**. Cet usage vise à répondre à la question : « *la personne qui se présente est-elle bien M. Untel* ? ». C'est par exemple la technique utilisée lorsqu'un usager déverrouille son smartphone à partir de son visage.

**L'identification** ensuite, qui vise 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. Le système restitue alors un ensemble de correspondances candidates. Cet usage vise à répondre à la question : « *qui est cette personne ?* ». L'objectif poursuivi est de retrouver une personne au sein d'un groupe d'individus filmés dans un lieu, figurant sur une image ou dont la photographie est présente dans une base de données. Il permet par exemple de lier un état civil à un visage ou de suivre la trajectoire d'une personne dans une foule.

**Le stockage des gabarits biométriques :**
**un élément distinctif des technologies de reconnaissance faciale**

Un autre élément à prendre en compte lors de l'étude des systèmes utilisant la biométrie du visage est constitué par les modalités de stockage des données biométriques. Trois modalités de stockage se distinguent :

- le gabarit biométrique de la personne est stocké sur un support dont elle a la **maîtrise exclusive** (passeport, badge, carte à puce, smartphone) – dit « gabarit de type 1 » ;

- le gabarit biométrique est sous **maîtrise partagée** : il est stocké au sein d'une base de données locale mais nécessite pour être exploité l'utilisation d'un « secret » détenu par la personne concernée (code personnel, par exemple) – dit « gabarit de type 2 » ;

- le gabarit biométrique **non maîtrisé par la personne** concernée est stocké sur une base de données et ne nécessite pas l'utilisation d'un « secret » par la personne concernée pour être exploité – dit « gabarit de type 3 ».

*Source : Commission des lois du Sénat*

### 3. Un sous-ensemble des systèmes de traitement d'images par intelligence artificielle

La reconnaissance faciale ne doit pas être confondue avec les **systèmes de traitements d'images grâce à l'intelligence artificielle**. Quatre niveaux de technologie permettent d'apporter une aide algorithmique au traitement d'une image ou d'une succession d'images, la reconnaissance biométrique n'en constituant que le quatrième niveau.

**Un premier niveau permet de détecter la présence d'un objet ou d'une personne dans une image sans en déterminer sa nature**, par comparaison avec une image de référence ou une image immédiatement antérieure. À titre d'exemple, la gendarmerie nationale utilise depuis 2017 un outil permettant d'exploiter *a posteriori* une vidéo de longue durée en filtrant les séquences au cours desquelles l'image est fixe.

**Un deuxième niveau permet de reconnaître des catégories**, par exemple la détection de types d'objets ou de piétons. Aucun élément supplémentaire sur les caractéristiques ou l'identité des personnes n'est alors rendu disponible. À titre d'exemple, le tournoi de tennis de Roland-Garros en 2020 a été l'occasion d'expérimenter le comptage de personnes présentes dans une file d'attente sur une voie privatisée ou dans une tribune et la détection de mouvements anormaux de foule. Un second exemple est constitué par l'expérimentation menée par la direction de l'ordre public et de la circulation (DOPC) de la préfecture de police de Paris permettant de détecter des types de véhicules circulant sans autorisation dans les couloirs de bus : ce système constitue une aide à la décision, dans lequel l'ensemble des opérations conduisant à une verbalisation reste décidé et réalisé par un agent de circulation. Peuvent également être cités la détection de comportements suspects, d'intrusions, de vols ou d'objets spécifiques.

**Un troisième niveau permet d'identifier une personne ou un objet à partir de ses caractéristiques non biométriques**, sans attacher à la personne une identité. Ces technologies permettent par exemple de suivre un individu dans une foule à partir de son habillement, comme a pu le faire par exemple la SNCF dans le cadre d'une expérimentation d'aide au suivi des personnes non-biométrique (projet PREVIENS).

**Un quatrième niveau**, qui inclut la reconnaissance faciale, **vise à reconnaître un individu à partir de ses caractéristiques biométriques**, qu'il s'agisse de son visage, son iris, sa démarche ou sa voix.

**La reconnaissance faciale se distingue également des technologies d'analyse faciale**, qui se rapportent au visage mais ne visent pas à en extraire le gabarit afin d'identifier ou d'authentifier la personne. Les technologies d'analyse faciale ou de **reconnaissance des émotions** ont ainsi pour objet de déterminer certaines caractéristiques des personnes présentes sur une image, comme leur âge, leur sexe, leur origine ou leurs émotions,

mais pas leur identité. Ces technologies peuvent par exemple être utilisées pour assurer le suivi des personnes atteintes de troubles neurocognitifs, notamment pour analyser leurs interactions sociales et leurs gestes fins[1].

### *B. DES CAS D'USAGE MULTIPLES ET POTENTIELLEMENT ILLIMITÉS*

Les algorithmes de reconnaissance biométrique du visage sont en constante évolution et ce mouvement connaît une accélération ces dernières années. De nombreux cas d'usage peuvent ainsi être distingués, poursuivant des finalités très diverses.

#### 1. Les usages facilitant la gestion de l'identité

La reconnaissance faciale, utilisée pour **l'établissement et le contrôle des titres d'identité**, permet de s'assurer que chaque personne dispose d'une identité unique. L'usage de cette technologie vise à limiter les risques d'obtention et d'utilisation illégitime de titres d'identité et d'usurpation d'identité, et rend impossible les identités multiples pour une seule et même personne. Dans ce cadre, la reconnaissance faciale peut être utilisée pour **lutter contre la fraude**.

La reconnaissance faciale permet également de **vérifier l'identité d'une personne à distance**. Il s'agit en premier lieu d'**offrir des solutions d'identification électronique sécurisées** qui, en s'appuyant sur la biométrie, permettent aux consommateurs de confirmer leur identité à distance pour souscrire ou accéder à un service en conformité avec la règlementation, notamment la lutte contre la corruption ou le blanchiment. C'est ainsi que des acteurs privés ont développé des modules permettant, par le biais de la reconnaissance faciale, de déverrouiller un smartphone, d'ouvrir un compte bancaire ou encore de louer une voiture. Il s'agit en second lieu de **sécuriser des transactions**. Peuvent par exemple être cités l'utilisation de cartes de paiement biométriques, l'autorisation de paiements ou la signature de contrats grâce à la biométrie (empreintes digitales ou reconnaissance faciale) depuis un smartphone.

#### 2. Les usages permettant d'assurer un contrôle des accès physiques sécurisé et fluidifié

La reconnaissance faciale permet également de **vérifier l'identité des personnes accédant à un lieu par le biais d'une authentification biométrique**. L'objectif poursuivi est alors d'**optimiser les contrôles d'accès, en en permettant la sécurisation et la fluidification.** Peuvent par exemple être concernés les accès à des zones dont l'accès doit être fortement sécurisé

[1] *Reconnaissance de gestes et des expressions faciales.*

(frontières, zones sécurisées de grands évènements, installations industrielles sensibles de production d'énergie ou de télécommunications notamment), à des services confidentiels (dossiers médicaux, systèmes financiers) ou encore à des zones dont l'accès est restreint (zones réservées dans les grands évènements, terminaux d'aéroports).

### 3. L'identification et le suivi des personnes à des fins de police administrative et judiciaire

**Les usages de la reconnaissance faciale les plus présents dans l'imaginaire collectif sont les usages d'identification à des fins policières ou de renseignement**. Parmi eux, peuvent être distingués les usages à finalité administrative ou judiciaire.

**L'identification par la biométrie du visage peut ainsi en premier lieu concourir à la sécurisation de certains espaces**. C'est par exemple le cas lorsqu'elle est utilisée **en temps réel en comparant des gabarits extraits à une base de personnes d'intérêt**, afin notamment de faire un criblage de la foule aux abords d'un lieu sensible. L'objectif poursuivi est alors, d'une part, d'éloigner les personnes s'étant vu interdire leur présence dans ce lieu et, d'autre part, d'anticiper les risques afin de faciliter la gestion de l'évènement en cours et de donner des éléments à des fins d'enquête dans le cas de la survenue ultérieure d'un incident. Cet usage peut être comparé au travail réalisé par des physionomistes chargés d'identifier des personnes aux abords d'un lieu particulier, par exemple un stade un soir de match à haut risque. Plus largement, la reconnaissance faciale peut également être utilisée à des fins de vidéoverbalisation des piétons, voire d'identification de toutes les personnes circulant sur la voie publique.

**En matière de renseignement**, la reconnaissance faciale peut également permettre **d'identifier des personnes d'intérêt ou de procéder au suivi de ces mêmes personnes afin de reconstituer leur parcours**.

**L'identification par reconnaissance faciale peut en second lieu constituer une aide à l'investigation judiciaire**. C'est par exemple le cas lorsqu'elle permet de **retrouver des personnes d'intérêt au sein d'une foule**, qu'il s'agisse de personnes recherchées parce qu'elles ont commis une infraction, parce qu'elles ont été témoin d'un fait et peuvent être utiles à l'enquête, ou parce qu'elles sont portées disparues – enlèvement par exemple. C'est également le cas lorsqu'elle est utilisée pour **identifier un suspect ou reconstituer *a posteriori* son parcours**.

Ainsi, en résumé, la reconnaissance faciale peut **permettre, sans que cette liste soit exhaustive, 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.

#### *4.* Les autres usages de l'identification des personnes par reconnaissance faciale

D'autres usages privés peuvent se développer dans un monde où la reconnaissance faciale n'est pas ou peu règlementée.

La société Facebook proposait ainsi la reconnaissance automatique des personnes présentes sur une image afin de suggérer l'identification nominative de ces personnes par comparaison entre les visages détectés sur l'image concernée et les gabarits de toutes les personnes présentes sur le réseau ayant consenti à cette fonctionnalité.

La société *Clearview AI*, une entreprise américaine qui a développé un logiciel de reconnaissance faciale dont la base de données repose sur la collecte de photographies et de vidéos publiquement accessibles sur internet, commercialise l'accès à sa base d'images sous la forme d'un moteur de recherche dans lequel une personne peut être recherchée à l'aide d'une photographie.

Au Royaume-Uni, la société Facewatch met à dispositions des gérants de commerce un logiciel de reconnaissance faciale les alertant lorsqu'une personne ayant été signalée par d'autres commerçants – dite « personne d'intérêt » – entre dans leur magasin. Le slogan de cette société est d'» *arrêter le crime avant qu'il n'arrive* ».

### *C. DANS LE MONDE, DES STRATÉGIES DIVERGENTES*

#### 1. La Chine : un développement à tout-va

La Chine est depuis quelques années à la pointe des technologies de reconnaissance faciale et plus largement biométrique. Selon les chercheurs de l'INRIA rencontrés par les rapporteurs, elle dispose d'une avance remarquable sur le plan de la recherche : **80 % des publications scientifiques relatives à la reconnaissance faciale proviennent actuellement de Chine**. Les algorithmes chinois, entraînés sur des bases de données de milliards de visages, sont en tête des classements du *National Institute of Standards and Technology* américain, qui est la référence en la matière[1]. Les entreprises chinoises fournissent des caméras à des prix imbattables qu'elles équipent sans surcoût de solutions logicielles pour les rendre « intelligentes ». Elles sont très désireuses de rentrer sur le marché européen[2].

---

[1] *Voir le III de la première partie.*

[2] *Ainsi la société Huawei avait-elle signé une convention prévoyant la mise à disposition gratuite d'un parc de caméras haute définition ainsi que des logiciels d'analyse automatisée des images captées par le système de vidéoprotection avec la ville de Valenciennes, qui a fait l'objet d'un avertissement de la CNIL le 12 mai 2021 après un contrôle sur place.*

Cette « force de frappe » scientifique et industrielle a avant toutes choses été développée **pour des besoins domestiques**. En 2019, sur les dix villes « championnes du monde de la vidéosurveillance », huit sont des villes chinoises, selon la revue Courrier international[1] qui cite un palmarès établi par la société Comparitech. Les réseaux de caméras de surveillance, tous interconnectés, sont **complétés par les applications numériques installées sur les téléphones mobiles des citoyens chinois**, qui sont utilisées notamment à des fins de paiement. Les géants du net tels Alipay et Wechat, ont mis au point des systèmes avec QR codes permettant notamment la reconnaissance faciale et des **systèmes de notation pour chaque geste de la vie quotidienne**, ainsi que le documente le reportage « *Ma femme a du crédit* », réalisé par Sébastien Le Belzic, journaliste français installé en Chine.

Depuis deux ans, a-t-il indiqué aux rapporteurs, l'État chinois a imposé à toute entreprise disposant de plus d'un million d'abonnés de lui transférer toutes ses données. Les autorités chinoises bénéficient ainsi de **milliards de données permettant de reconstituer la vie quotidienne de ses citoyens**. Selon lui, la pandémie de la Covid-19 a profondément aggravé le système de surveillance de masse avec, en particulier, la mise en place de QR codes de traçage et l'abandon progressif des paiements en argent liquide. Cet état de fait est pourtant **bien accepté de la population**, à l'exception des personnes âgées en raison de leur difficulté à s'adapter à cet environnement tout numérique.

**Une surveillance biométrique renforcée est par ailleurs exercée sur la population ouïghoure du Xinjiang** ainsi que l'a rapporté l'association Human Rights Watch : « *dans le cadre de la campagne " Frapper fort ", les autorités du Xinjiang ont également collecté des données biométriques, notamment des échantillons d'ADN, des empreintes digitales, des analyses de l'iris et des groupes sanguins de tous les résidents de la région âgés de 12 à 65 ans. Les autorités exigent d'eux des enregistrements de leurs voix lorsqu'ils font une demande de passeport. Toutes ces données figurent dans des bases de données gouvernementales centralisées et exploitables. Bien que les systèmes en place au Xinjiang soient particulièrement intrusifs, leur conception de base ne diffère pas de celles que la police élabore et utilise dans toute la Chine* »[2].

En 2014, le gouvernement chinois avait annoncé le lancement d'un **« système de crédit social »** dans le but d'assurer une meilleure application des lois et décisions de justice, sur le modèle des notes de fiabilité que certains services commerciaux délivrent à leurs usagers[3]. Selon Sébastien Le Belzic, les autorités chinoises sont depuis restées discrètes sur ce projet en raison de la mauvaise publicité occasionnée et, à ce jour, le

---

[1] https://www.courrierinternational.com/article/classement-videosurveillance-le-top-20-mondial-des-villes-qui-espionnent-leurs-habitants.

[2] « Les algorithmes de la répression en Chine : Rétro-ingénierie d'une application de surveillance de masse utilisée par la police du Xinjiang », *Human Rights Watch, mai 2019.*

[3] » En Chine, le "crédit social" des citoyens fait passer les devoirs avant les droits », *Brice Pedroletti,* Le Monde*, 16 janvier 2020.*

système de crédit social ne semble mis en place que pour restreindre l'accès aux transports (train et avion).

### 2. Le Royaume-Uni : la logique de l'empirisme

**Au Royaume-Uni, deux forces de police ont décidé de mettre en place des dispositifs de reconnaissance faciale dans l'espace public**. La police londonienne et la police du Pays de Galles déploient ainsi des dispositifs de reconnaissance faciale en temps réel visant à **identifier dans l'espace public des personnes référencées sur une liste de surveillance (*watchlist*)** établie pour chaque déploiement du dispositif, par comparaison avec les gabarits extraits des visages de toutes les personnes passant dans l'angle de la caméra. La police du Pays de Galles a également mis en place une application permettant aux policiers, en cas de doute sur l'identité déclinée par la personne au cours d'un contrôle d'identité, de recourir à la reconnaissance faciale pour **vérifier que la personne concernée ne fait pas l'objet de recherches**.

Les technologies de reconnaissance faciale automatisée sont utilisées comme un **outil technique d'assistance** à la reconnaissance de personnes impliquées dans des activités criminelles – la décision des suites à donner à une alerte est toujours humaine – dont les usages sont définis par les différentes polices en fonction de leurs besoins.

**En l'absence de cadre législatif spécifique et dans un contexte de *common law*, il revient aux juridictions de s'assurer du caractère adapté et proportionné de ces déploiements**. C'est ainsi que la Cour d'appel du Royaume-Uni, dans une décision du 11 août 2020, *Bridges*, a examiné le caractère proportionné de l'utilisation des outils de reconnaissance faciale par la police du Pays de Galles. Elle a jugé que le déploiement alors réalisé était illégal pour trois raisons : l'insuffisance de son régime juridique qui donnait trop de marge de manœuvre aux policiers dans l'établissement de la liste de surveillance, l'insuffisance de l'évaluation des risques en matière de protection des données personnelles, et le non-respect du principe d'égalité en raison d'une évaluation insuffisante des potentiels biais du logiciel.

À la suite de cette décision, la police du Pays de Galles avait dû suspendre l'utilisation de la reconnaissance faciale. Sur la base des éléments avancés par la Cour d'appel, la police du Pays de Galles a décidé de reprendre ses essais en mars 2022, afin de s'assurer que le système ne présentait désormais plus de risque en matière d'égalité et que son déploiement était « *responsable, proportionné et juste* »[1].

[1] *Selon les termes du responsable adjoint de la police du Pays de Galles, Mark Travis.*

Parallèlement, certains commerces ont acheté la solution fournie par la société Facewatch, qui permet la mise en place d'une liste de « *personnes d'intérêt* » partagée par tous les utilisateurs en vue de détecter les personnes signalées pour vol ou mauvais comportement dès leur entrée dans les commerces concernés. Ces usages, de même que ceux réalisés par les forces de police, ne sont pas règlementés et se développent au gré de leur adoption par les acteurs privés.

### 3. Les USA : des tendances contraires

#### *a) Une multiplication des interdictions de la reconnaissance faciale au niveau municipal dont la portée concrète est à relativiser*

Depuis l'adoption en mai 2019 par la ville de San Francisco d'une ordonnance[1] interdisant l'usage de la reconnaissance faciale par la municipalité, **le débat autour du développement, de l'usage et de l'encadrement de cette technologie est en plein essor aux États-Unis**. Le symbole est d'autant plus fort que cette interdiction prend place au cœur de la « *Silicon Valley* », dans une métropole qui abrite de nombreuses entreprises du numérique. Dans les motifs de cette décision, il est notamment avancé que « ***la propension de la technologie de reconnaissance faciale à mettre en danger les droits civiques et les libertés publiques l'emporte substantiellement sur ses prétendus bénéfices, et que cette technologie exacerbera les injustices raciales et menacera notre capacité à vivre en-dehors de toute surveillance continue du Gouvernement*** »[2].

Dans le sillage de la cité californienne, plusieurs grandes métropoles américaines ont entendu interdire ou règlementer le recours à la reconnaissance faciale. **Cet encadrement s'opère sur un périmètre et selon des modalités variables en fonction de la ville concernée** : il concerne l'usage d'algorithmes de reconnaissance faciale tantôt par les seuls services de police, tantôt par la totalité des services municipaux. Il peut même aller au-delà des seuls usages publics de cette technologie pour réguler des usages privés. **Les exceptions prévues à ce principe d'interdiction diffèrent également à la marge**, par exemple afin de laisser une latitude aux services de police dans l'usage de preuves obtenues par le biais de la reconnaissance faciale ou pour tolérer certains usages d'authentification privée.

---

[1] *Conseil de surveillance de la ville de San Francisco, Ordonnance sur l'acquisition de technologies de surveillance, mai 2019.*

[2] *En anglais dans le texte :* « The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring ».

**Des interdictions de la reconnaissance faciale à géométrie variable : les exemples de Boston, Portland et Baltimore**

**Boston** : le conseil municipal a interdit, à compter de juin 2020, « *l'obtention, la rétention, la possession, l'accès ou l'usage de tout système de reconnaissance faciale* »[1] par la ville de Boston ou ses agents, y compris par l'intermédiaire d'un accord avec un tiers. **En revanche, le service de police est autorisé à utiliser des preuves issues de système de reconnaissance faciale dès lors que leur obtention n'est pas le résultat d'une requête interne**. Certains usages limités à des fins d'authentification privée sont également exclus du champ de l'ordonnance.

**Portland** : la ville de l'Oregon a été la **première à aller au-delà de l'interdiction des seuls usages publics de la reconnaissance faciale pour également viser les usages privés**[2]. Concrètement, l'usage de cette technologie par des entités privées est prohibé dans certains « *lieux recevant du public* »[3]. Cette interdiction ne s'applique toutefois pas aux usages de technologies de reconnaissance du visage à des fins d'authentification sur des appareils personnels ou de détection automatique des visages sur les réseaux sociaux.

**Baltimore**[4] : le conseil municipal a adopté en août 2021 un **moratoire sur l'obtention, la détention, l'accès et l'usage d'algorithmes de reconnaissance faciale, ou de toute information obtenue par l'intermédiaire d'un tel système**, applicable à la ville de Baltimore et à toute personne privée, physique ou morale[5]. Ce moratoire arrivera à échéance le 31 décembre 2022, sauf si le conseil municipal décide de le proroger pour une durée maximale de cinq ans.

La violation de ce moratoire est passible d'une amende de 1 000 dollars et d'une peine de 12 mois de prison. **Deux exceptions, dont une de taille, sont néanmoins prévues** à ce principe général d'interdiction de la reconnaissance faciale :

- l'utilisation de systèmes de reconnaissance faciale par la police de Baltimore sur les données contenues par le « *Maryland Image Repository System* », dans le cadre d'investigations criminelles. Cette exception résulte du positionnement atypique de la police de Baltimore, laquelle est placée non pas sous l'autorité de la ville mais de l'État du Maryland ;

- les systèmes biométriques destinés à protéger l'accès à des lieux ou des systèmes d'informations particuliers.

*Source : Commission des lois du Sénat*

[1] *Conseil municipal de Boston, Ordonnance interdisant la technologie de surveillance faciale à Boston, juin 2020.*

[2] *Ville de Portland, Ordonnance* prohibant l'acquisition et l'usage de technologies de reconnaissance du visage par les services de la ville de Portland *et Ordonnance* prohibant l'usage de technologies de reconnaissance du visage par des entités privées dans les lieux publics*, septembre 2020.*

[3] *Entendus comme :* « any place or service offering to the public accommodations, advantages, facilities, or privileges whether in the nature of goods, services, lodgings, amusements, transportation or otherwise » *et à l'exclusion des lieux suivants :* « an institution, bona fide club, private residence, or place of accommodation that is in its nature distinctly private ».

[4] *Conseil municipal de Baltimore, Ordonnance* sur la surveillance technologique à Baltimore*, août 2021.*

[5] *À l'exclusion du gouvernement fédéral, du gouvernement d'État et, le cas échéant, de leurs cocontractants.*

À l'image de la décision californienne, les motivations avancées résident en premier lieu **dans la moindre efficacité des algorithmes de reconnaissance faciale lorsqu'ils sont utilisés sur des personnes de couleur ou des femmes**. Il s'agit, en second lieu, de protéger les libertés publiques, singulièrement le droit à la vie privée et la liberté d'expression, face à une technologie au caractère particulièrement intrusif et soulevant de ce fait d'importants enjeux de transparence.

**La portée concrète de ces interdictions doit néanmoins être relativisée**. Premièrement, les usages préexistants de la reconnaissance faciale par les villes concernées étaient le plus souvent modestes. Par exemple, le responsable de la police de Boston a indiqué dans une audition publique en juin 2020, soit avant l'entrée en vigueur de l'ordonnance précitée, que ses services n'avaient pas recours à la reconnaissance faciale et que « *cette technologie ne l'intéressait pas tant qu'elle n'était pas à 100 % efficace* »[1]. Deuxièmement, le contrôle de ces interdictions est délicat à mettre en œuvre, voire à la limite de l'impossible dans le cas des usages privés. À Baltimore, aucune poursuite n'a à ce jour été engagée sur le fondement d'une violation du moratoire. Troisièmement, des exceptions importantes peuvent être prévues, en particulier s'agissant de l'usage de la reconnaissance faciale par les services de police dans le cadre d'investigations criminelles.

**À certains égards, ce mouvement relève donc davantage d'une position de principe vis-à-vis de la reconnaissance faciale que d'un réel bouleversement des usages.** Les débats relatifs aux biais des algorithmes se tiennent par ailleurs dans un contexte de montée en puissance du mouvement « *Black Lives Matter* » et de regain des tensions raciales aux États-Unis à la suite du décès de Georges Floyd en mai 2020. Ce contexte amplifie sans nul doute la dynamique observée de renonciation à la reconnaissance faciale.

**Il serait toutefois réducteur de limiter l'analyse du développement de la reconnaissance faciale à cette seule succession d'interdictions locales.** La structure fédérale des États-Unis fait **qu'il existe potentiellement autant de doctrines d'usage que d'autorités susceptibles d'avoir recours à la reconnaissance faciale**, que ce soit au niveau fédéral, des États ou encore municipal. Au-delà des ordonnances d'interdiction précitées, cette technologie peut également être utilisée par certaines autorités locales à grande échelle et sans encadrement *ad hoc*, ainsi que l'a démontré la

[1] *Audition publique de la commission des affaires gouvernementales du conseil municipal de Boston, 9 juin 2020.*

controverse liée à l'utilisation par certains services de police de l'outil fourni par la société *Clearview AI*[1].

*b) Des règlementations locales des usages policiers de la reconnaissance faciale : les exemples de New-York et de Baltimore*

Les travaux des rapporteurs ont mis en lumière l'existence de règlementations locales de l'usage de la reconnaissance faciale par les services de police pouvant, par certains aspects, ressembler aux pratiques françaises[2]. C'est par exemple le cas des services de police de Baltimore et de New-York, où la reconnaissance faciale peut être utilisée dans le cadre d'enquêtes policières afin de comparer, dans certains cas limitativement énumérés, le visage d'une personne d'intérêt avec ceux figurant dans une base de données de plus ou moins grande envergure :

- à New-York : la base de données contient uniquement **des photos obtenues au cours d'arrestations et les visages des personnes en libération conditionnelle**[3] ;

- à Baltimore : tenue par le « *Maryland Department of Public Safety and Correctional Services* », **la base de données est beaucoup plus importante, voire massive.** Par exemple, l'intégralité des photos fournies à l'administration pour l'obtention d'un permis de conduire y figure.

**Les six usages autorisés de la reconnaissance faciale par le New York City Police Department (NYPD) (Patrol Guide - Guide du policier en service)**

Dans le cadre d'enquêtes policières conduites par le service de police de New-York, **l'usage de la reconnaissance faciale est uniquement autorisé pour les six objectifs suivants** :

« *a) Identifier une personne lorsqu'il y a des raisons de croire qu'elle a commis, commet ou est sur le point de commettre une infraction ;*

« *b) Identifier une personne lorsqu'il y a des raisons de croire qu'elle est une personne disparue, la victime d'un crime ou le témoin d'une activité criminelle ;*

« *c) Identifier une personne décédée,*

[1] *Le site d'information* « Buzzfeed » *met par exemple à la disposition du public une base de données recensant 1 803 entités publiques, dont certains services de police, qui auraient utilisé l'outil de reconnaissance faciale fourni par la société* Clearview AI. *Il est néanmoins explicitement précisé que la présence sur cette liste ne signifie pas que le site a pu confirmer l'utilisation de cet outil par l'entité en cause, ni qu'elle a approuvé son usage par l'un de ses employés. Source : https://www.buzzfeednews.com/article/ryanmac/facial-recognition-local-police-clearview-ai-table.*

[2] *Voir* infra, *le II A de la première partie.*

[3] *» The photo repository only contains arrest and parole photographs » (New-York Police Department - Patrol Guide)*

*« d) Identifier une personne qui est incapable de s'identifier,*

*« e) Identifier une personne qui est en état d'arrestation et qui ne possède pas d'identification valide, qui ne dispose pas d'une pièce d'identité valide, ou qui semble utiliser l'identification de quelqu'un d'autre, ou une fausse identification,*

*« f) Atténuer une menace imminente pour la santé ou la sécurité publique (par exemple, pour contrecarrer un plan ou un complot terroriste actif,* etc.*) »*

*Source : Commission des lois du Sénat*

**Les deux services de police ont établi des lignes directrices visant à encadrer l'usage de la reconnaissance faciale, qui se rejoignent sur la plupart des points**. Au titre des garanties, la demande doit être déposée auprès d'une **unité dédiée**, seule autorisée à accéder au système. Il s'agit du « *Real Time Crime Center, Facial Identification Section* » à New-York et d'une « *Open Source Unit* » à Baltimore. Les enquêteurs de ces unités évaluent le bien-fondé de la demande et, le cas échéant, procèdent à la comparaison. **Les potentielles correspondances sont ensuite confirmées par une analyse visuelle d'une part, et par la consultation des fichiers de police pertinents, d'autre part**. La transmission des résultats au requérant est soumise à un double-degré de validation et, enfin, une trace est conservée de chacune des requêtes. **La technologie est uniquement utilisée comme un instrument d'aide à l'enquête.** Sur le plan juridique, l'établissement d'une correspondance ne constitue pas en elle-même une preuve justifiant par exemple une arrestation et elle doit systématiquement être accompagnée d'investigations complémentaires.

Au cours de son audition, Lisa Walden, conseillère en chef des Affaires policières du département juridique de la ville de Baltimore, a souligné **les résultats positifs produits par l'utilisation de la reconnaissance faciale**. Elle a également estimé **suffisamment robustes les garanties apportées par les protocoles en place en termes de protection des libertés publiques**. En particulier, les examens complémentaires pratiqués après la première recherche de correspondance préviendraient les erreurs générées par d'éventuels biais de l'algorithme.

En ce qui concerne New-York, le site internet du service de police affirme que le logiciel a régulièrement fourni **des pistes substantielles pour la résolution d'affaires criminelles**. Ainsi, sur les 9 850 demandes de comparaison enregistrées en 2019, « *2 510 correspondances possibles* [ont été identifiées], *dans 68 meurtres, 66 viols, 277 agressions criminelles, 386 vols qualifiés et 525 fraudes importantes* ». Il est par ailleurs précisé que « *le NYPD n'a pas connaissance à New-York d'une personne faussement arrêtée sur la base d'une correspondance de reconnaissance faciale* »[1].

[1] *Site internet du service de police de New-York (https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page).*

## *II.* UN USAGE EMBRYONNAIRE EN FRANCE SANS ENCADREMENT *AD HOC*

### *A. UN USAGE ENCORE EMBRYONNAIRE*

#### 1. Des usages pérennes limités

En France, **les usages pérennes sont limités et principalement le fait des pouvoirs publics**, hormis certains usages d'authentification avec consentement déjà déployés par exemple pour déverrouiller les téléphones portables ou ouvrir un compte bancaire à distance[1].

L'entrée en vigueur du règlement général de protection des données (RGPD)[2] le 25 mai 2018 a modifié le cadre d'intervention de la CNIL qui n'autorise plus *a priori* la mise en place de traitements de données biométriques. S'agissant des acteurs privés, elle n'intervient plus désormais qu'*a posteriori* à l'occasion de signalements par exemple[3]. Il est par conséquent **difficile d'avoir une vision exhaustive des utilisations commerciales en cours**, alors que tout traitement de données biométriques **mis en œuvre pour le compte de l'État**, doit faire l'objet *a minima* **d'une saisine pour avis de la CNIL** *via* une transmission systématique de l'analyse d'impact relative aux données personnelles (AIPD)[4].

*a) Les usages réalisés sans le consentement des personnes*

(1) Le « Traitement des antécédents judiciaires » (TAJ)

Un dispositif de rapprochement par photographies est opéré dans le **fichier du « Traitement des antécédents judiciaires » (TAJ)** constitué de données recueillies, dans le cadre des procédures établies par les **services de sécurité intérieure** (police nationale, gendarmerie nationale et douanes). Ce traitement, prévu par les articles R. 40-23 à R. 40-34 du code de procédure pénale, est mis en œuvre par le ministre de l'intérieur (direction générale de la police nationale et direction générale de la gendarmerie nationale) afin de

---

[1] *Voir par exemple la délibération n° 2018-051 du 15 février 2018* autorisant Boursorama à mettre en œuvre un système d'identification par reconnaissance faciale des prospects lors d'une entrée en relation à distance.

[2] *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.

[3] *En février 2021, à la suite de signalements, la Présidente de la CNIL a ainsi adressé un avertissement à un club sportif qui envisageait de recourir à un système de reconnaissance faciale afin d'identifier automatiquement les personnes faisant l'objet d'une interdiction commerciale de stade :* https://www.cnil.fr/fr/reconnaissance-faciale-et-interdiction-commerciale-de-stade-la-cnil-adresse-un-avertissement-un-club

[4] *Article 90 de la loi n° 78-17 du 6 janvier 1978* relative à l'informatique, aux fichiers et aux libertés.

faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs.

Depuis 2012, l'article R. 40-26 du code de procédure pénale autorise les forces de sécurité intérieure à **utiliser la reconnaissance faciale pour identifier les personnes fichées dans le TAJ**[1]. Il s'agit d'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. Il est également possible **d'établir des liens entre des affaires différentes**, voire de les attribuer à un même auteur sur la base de sa reconnaissance sur les photographies disponibles. Cet outil vient en soutien de l'enquêteur et est paramétré pour donner un maximum de 200 réponses avec un taux de correspondance minimum de 40 %. C'est l'enquêteur qui procède *in fine* à l'identification de la personne.

Cette fonctionnalité par « *rapprochement de photo de personne* » est mise en œuvre principalement **dans le cadre d'une enquête judiciaire, sous la direction et le contrôle d'un magistrat**[2]. Elle peut également être utilisée dans le cadre du renseignement en application de l'article L. 234-4 du code de la sécurité intérieure qui permet aux agents individuellement désignés et spécialement habilités des services spécialisés de renseignement des ministères de l'intérieur, de la défense, des finances et des comptes publics, de consulter le TAJ, selon un profil spécifique leur permettant d'accéder à toutes les données des procédures judiciaires, y compris celles en cours, à l'exclusion de celles relatives aux victimes.

L'utilisation de l'outil de reconnaissance faciale pour interroger le TAJ est **en accroissement notable depuis quelques années**. En 2021, il a été utilisé 498 871 fois[3] par la police nationale et environ 117 000 fois par la gendarmerie nationale[4]. Selon la direction centrale de la police judiciaire (DCPJ), qui est le gestionnaire du traitement, cette montée en puissance de l'utilisation de l'outil pourrait être consécutive à l'évolution technique de l'outil intervenue en 2019 qui en a nettement amélioré la performance.

L'utilisation d'une application de reconnaissance faciale sur le TAJ a été validée par le Conseil d'État[5] qui a notamment jugé que « *le traitement litigieux comporte des garanties appropriées pour les droits et libertés des personnes concernées et n'institue pas, contrairement à ce qui est soutenu, un "dispositif disproportionné"* ». Il a relevé que « *le dispositif de reconnaissance faciale ne peut*

---

[1] *Peut être enregistrée dans ce traitement la photographie comportant les caractéristiques techniques permettant le recours à un dispositif de reconnaissance faciale (photographie du visage de face des personnes mises en cause ou disparues et des corps non identifiés).*

[2] *Elle ne peut pas être utilisée dans le cadre d'un contrôle d'identité, en particulier lorsque les services utilisent l'outil en mobilité, comme le rappelle une circulaire du directeur général de la police nationale du 24 janvier 2022.*

[3] *Ce qui représente 3,2 % du total des consultations du TAJ qui s'élèvent à 15 341 000.*

[4] *Réponses de la direction générale de la police nationale et de la direction générale de la gendarmerie nationale au questionnaire des rapporteurs.*

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

*être utilisé par les services compétents qu'en cas de nécessité absolue, appréciée au regard des seules finalités du traitement, lorsque subsiste un doute sur l'identité d'une personne dont l'identification est requise* ».

(2) L'utilisation de la reconnaissance faciale comme technique de renseignement

La direction générale de la sécurité intérieure (DGSI) a indiqué aux rapporteurs utiliser, dans le cadre de la loi du 23 juillet 2015 *relative au renseignement*, qui définit un cadre propre, dérogatoire à la loi du 6 janvier 1978, pour la collecte, la conservation et l'exploitation des données issues de techniques de renseignement, des dispositifs de reconnaissance faciale afin **d'exploiter des données vidéo collectées par le biais de la mise en œuvre de techniques de renseignement**. Il s'agit alors soit d'identification (par exemple, la recherche du visage d'une cible particulière dans un flux vidéo ou dans une base souveraine de visages), soit d'authentification (regroupement de visages similaires présents dans un silo de données, afin de détecter d'éventuelles relations).

*b) Les usages basés sur le consentement des personnes*

Actuellement, un seul usage réalisé sur la base du consentement des personnes est mis en œuvre par les autorités publiques : il s'agit du traitement de données pour le contrôle aux frontières PARAFE, le projet d'identité numérique Alicem ayant été abandonné.

(1) PARAFE : un système en voie d'extension

Depuis 2010[1], un traitement de données à caractère personnel dénommé **« PARAFE » (passage rapide aux frontières extérieures)** est destiné à améliorer et faciliter les contrôles de police aux frontières extérieures pour les voyageurs aériens, maritimes et ferroviaires[2]. Il permet d'obtenir des gains à la fois en temps de contrôle et en effectifs de police engagés[3].

Le système PARAFE fonctionne sur la base de la **comparaison faciale entre l'image contenue dans le composant électronique du document de voyage présenté et la photo prise en direct de son titulaire à l'intérieur d'un sas de passage**. Le voyageur se présente face à l'entrée du sas et introduit son document d'identité biométrique dans le lecteur qui accède à la puce. Le franchissement *via* le sas s'effectue conformément aux

[1] *Décret n° 2010-1274 du 25 octobre 2010* portant création d'un traitement automatisé de données à caractère personnel dénommé PARAFE.
[2] *Voir les articles R. 232-6 et suivants du code de la sécurité intérieure.*
[3] *Il est prévu un effectif de police pour la supervision de 5 sas PARAFE (contre 1 effectif par aubette classique).*

règles édictées par le Code frontière Schengen (CFS)[1]. **Aucune image prise dans le sas et du portrait lu à partir du composant sans contact du titre d'identité n'est conservée**.

Depuis le début de leur déploiement en 2017, 47 batteries comptant 217 sas PARAFE ont été mises en service dans différents points de passage frontaliers tenus par la direction centrale de la police aux frontières (DCPAF), en particulier dans les aéroports de Paris-Charles-de-Gaulle, Orly, Marseille-Provence, Lyon, Nice, Bâle-Mulhouse et Bordeaux, dans les gares de Paris-Gare du Nord et Londres-Saint-Pancras, et également de part et d'autre de la liaison transmanche entre Coquelles et Cheriton.

La reconnaissance faciale à des fins d'authentification se fonde dans cette hypothèse sur le consentement de la personne qui **choisit de manière volontaire de passer dans un sas spécialement conçu à cet effet**, au lieu de se présenter à une aubette où est présent un garde-frontière. Cette option est offerte à toute personne majeure – ou, en entrée de territoire seulement, mineure âgée de plus de douze ans –, qui est citoyenne de l'Union européenne ou ressortissante de certains pays tiers[2] et détentrice d'un document de voyage en cours de validité comportant des données biométriques[3].

**Les réformes européennes : un recours global à la biométrie dans le cadre du système d'entrée et de sortie (EES) et l'interopérabilité des fichiers**

Dans le cadre de la stratégie Schengen de renforcement de la sécurité en Europe mise en œuvre en réaction aux attentats de 2013 en France, il a été décidé :

- la création d'une **base centralisée** opérée par l'agence européenne LISA[4] de **toutes les données relatives aux entrées et sorties des étrangers hors UE** dans l'espace Schengen, en particulier pour vérifier le respect de la durée autorisée de séjour dans l'État membre[5].

---

[1] *Après interrogation du fichier des personnes recherchées (FPR), du système d'information Schengen et de la base de données d'Interpol SLTD (documents de voyage volés ou perdus), sur la base des éléments d'identité biographiques de la personne (et non de sa biométrie)*

[2] *États partie à l'accord sur l'Espace économique européen (Norvège, Liechtenstein et Islande), Confédération suisse, États-Unis, Andorre, Australie, Royaume-Uni, Canada, Corée du Sud, Japon, Principauté de Monaco, Nouvelle-Zélande, Saint-Marin et Singapour.*

[3] *Doté d'une zone de lecture automatique au sens du document 9303 de l'Organisation de l'aviation civile internationale ou conforme au règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 modifié* établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.

[4] *Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA).*

[5] *Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017* portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) n° 767/2008 et (UE) n° 1077/2011.

À compter de l'automne 2022, chaque étranger devra disposer d'un dossier individuel avec **des données de biométrie faciale et digitale.** L'accès à ces données biométriques sera réservé aux agents affectés au contrôle transfrontière ;

**- l'interopérabilité des systèmes d'information de l'Union européenne** en matière de sécurité et de gestion des frontières et des migrations afin d'améliorer l'efficacité et l'efficience des vérifications aux frontières extérieures, de contribuer à prévenir l'immigration illégale et de favoriser un niveau élevé de sécurité.

Une réflexion est en cours pour **étendre le recours des sas PARAFE à tous les ressortissants de pays tiers en court séjour** dès lors qu'ils seraient connus du système EES et préenregistrés à un kiosque en amont.

(2) Alicem : un projet d'authentification sur mobile abandonné

Le projet Alicem, porté par le ministère de l'intérieur et l'Agence nationale des titres sécurisés (ANTS), a été lancé en 2019[1] comme étant « *la première solution d'identité numérique régalienne sécurisée* », conçue pour permettre de créer une identité numérique aux personnes possédant un titre d'identité ou un titre de séjour biométrique valide afin de parer à toute usurpation d'identité. Il reposait sur **un système de reconnaissance faciale statique et dynamique** mis en œuvre à l'aide du téléphone mobile[2].

Son développement a rapidement suscité des inquiétudes en raison justement du recours à la technologie de la reconnaissance faciale. La CNIL, dans son avis du 18 octobre 2018[3], s'était montrée réticente en raison du fait que « *la création d'une identité numérique Alicem est subordonnée à un processus de reconnaissance faciale* ***sans qu'aucune autre alternative équivalente***[4] *ne soit prévue pour permettre la délivrance d'une identité numérique par cette application* », ce qui pouvait remettre en cause le caractère libre du consentement.

---

[1] *Décret n° 2019-452 du 13 mai 2019* autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ».

[2] *Réalisation par l'utilisateur d'une vidéo en temps réel via le smartphone (en mode* selfie*) en effectuant 3 actions différentes (sourire, tourner la tête, cligner des yeux) dans un laps de temps resserré et dans un ordre aléatoire et comparaison d'une photographie extraite de la vidéo à celle conservée dans la puce du titre.*

[3] *Délibération n° 2018-342 du 18 octobre 2018* portant avis sur un projet de décret autorisant la création d'un traitement automatisé permettant d'authentifier une identité numérique par voie électronique dénommé « Application de lecture de l'identité d'un citoyen en mobilité » (Alicem) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile *(demande d'avis n° 18008244).*

[4] » Ces solutions alternatives pourraient notamment prendre la forme d'un face à face (tel qu'un déplacement en préfecture, en maire, ou auprès d'un autre service public accueillant directement le public), d'une vérification manuelle de la vidéo et de la photographie sur le titre (telle qu'un envoi de la vidéo au serveur de l'ANTS et vérification de l'identité opérée par un agent) ou d'un appel vidéo en direct avec un agent de l'ANTS » *a relevé la CNIL.*

Bien que le dispositif ait été validé par le Conseil d'État[1], le projet Alicem a finalement été **abandonné en avril 2022 et remplacé par le « Service de garantie de l'identité numérique » (SGIN)**[2]. Ce service a pour finalité de mettre à disposition des titulaires d'une carte nationale d'identité électronique (CNIe)[3] un moyen d'identification électronique leur permettant de s'identifier et de s'authentifier auprès d'organismes publics ou privés grâce à une application installée sur un téléphone permettant la lecture sans contact de ce composant[4].

Le site du programme interministériel « France identité numérique » annonce que **le SGIN n'utilisera pas la reconnaissance faciale :** « *l'État a choisi de développer des parcours utilisateurs les plus inclusifs possibles, qui puissent se passer de la vérification d'identité à distance, sans renoncer à un niveau de garantie élevé. Ainsi, l'application Alicem est finalement abandonnée* ***au profit d'un enrôlement initial capitalisant sur le face-à-face sécurisé en mairie au moment de la délivrance du titre*** » [5].

### 2. Des expérimentations à la marge

Depuis l'entrée en vigueur du RGPD en 2018, la CNIL a reçu la transmission de dix analyses d'impact relatives aux données personnelles (AIPD) mettant en jeu des dispositifs de reconnaissance faciale. **Huit d'entre elles concernaient des expérimentations**[6].

*a) Expérimentations menées par les collectivités territoriales*

Selon le Secrétariat général de la défense et de la sécurité nationale, (SGDSN), les collectivités locales sont moins avancées dans la connaissance de ce type de technologies, compte tenu du cadre légal mais aussi en raison d'un moindre recours par celles-ci aux techniques de supervision sophistiquées.

Au plan national, la seule expérimentation à grande échelle qui a été réalisée est celle menée durant le **carnaval de Nice**, en février-mars 2019, sur

---

[1] *Arrêt du Conseil d'État, 10ème et 9ème chambres réunies, 4 novembre 2020, n° 432656,* La Quadrature du Net.

[2] *Décret n° 2022-676 du 26 avril 2022* autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ».

[3] *Carte nationale d'identité comportant un composant électronique contenant les données de la carte d'identité, à l'exception de la signature, du code de lecture automatique et du numéro de support, ainsi qu'une image numérisée de la photographie et l'image numérisée des empreintes digitales de deux doigts (voir article 1-1 du décret n° 55-1397 du 22 octobre 1955* instituant la carte nationale d'identité*).*

[4] *La première carte d'identité électronique a été livrée le 15 mars 2021 par le groupe Imprimerie nationale.*

[5] *https://france-identite.gouv.fr/questions-frequentes/.*

[6] *Réponses de la CNIL au questionnaire des rapporteurs.*

la base du volontariat. La CNIL ne s'y était pas opposée car les principes du RGPD étaient respectés.

En revanche, en octobre 2019, elle avait refusé des expérimentations mettant en œuvre un « portique virtuel » de contrôle d'accès par reconnaissance faciale à l'entrée de deux lycées de la région Provence-Alpes-Côte d'Azur, considérant que le dispositif projeté était contraire aux grands principes de proportionnalité et de minimisation des données posés par le RGPD[1]. Les objectifs de sécurisation et la fluidification des entrées dans ces lycées pouvaient être atteints par des moyens bien moins intrusifs en termes de vie privée et de libertés individuelles, comme par exemple un contrôle par badge, prenant également en compte le fait que les mineurs devaient faire l'objet d'une protection renforcée.

*b) Expérimentations menées par le SGDSN*

Depuis 2019, le SGDSN a conduit une analyse du besoin en liaison avec la coordination nationale pour la sécurité des Jeux Olympiques et Paralympiques (JOP) et des grands événements sportifs internationaux du ministère de l'intérieur (CNSJ) et lancé une **opération d'identification des technologies pouvant être pertinentes dans l'organisation des grands évènements internationaux**.

Deux expérimentations reposant en partie sur des technologies de reconnaissance faciale ont été organisées.

Une expérimentation a été conduite dans le cadre du **tournoi de Roland-Garros 2020** pour tester un **dispositif de contrôle d'accès pour les arbitres**. Il s'agissait à la fois de vérifier l'authenticité des titres d'identité et de contrôler l'accès du personnel accrédité à certaines zones.

Une autre expérimentation similaire était envisagée en 2021 sur le **site du stade Orange vélodrome à Marseille**. Mais la CNIL, dans deux avis des 16 septembre 2021 et 2 décembre 2021, a considéré que les objectifs de l'expérimentation ne suffisaient pas à démontrer la **nécessité d'un stockage des données dans des serveurs distants** ou dans le cadre d'une maîtrise partagée, **ni même le recours à la biométrie**.

*c) Expérimentations menées par Aéroports de Paris*

La société **Aéroports de Paris** a mis en place une expérimentation en plusieurs phases de la reconnaissance faciale, qui a été suspendue en raison de la crise sanitaire. Cette expérimentation, initiée en 2019 en coordination avec la CNIL, est destinée à fluidifier les flux de passagers : le dispositif permet aux passagers volontaires de s'enregistrer et d'embarquer de manière autonome, par simple scan du visage *via* reconnaissance faciale, grâce à un enrôlement biométrique préalable. Retardée à cause de la crise sanitaire de la

[1] *https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position*.

Covid-19, la première phase a été menée entre mars et juillet 2021 puis la deuxième entre février et avril 2022.

### 3. Le projet avorté d'un usage d'identification à distance à grande échelle pour les JOP 2024

La France accueillera **deux grands évènements sportifs en 2023** (coupe du monde de rugby) **et 2024** (jeux olympiques et paralympiques). En raison des importants enjeux en matière de sécurité qu'ils posent[1], de nombreux acteurs avaient **préconisé le recours à une expérimentation nationale** suffisamment en amont pour pouvoir avoir recours à l'utilisation de l'identification en temps réel par reconnaissance faciale dans l'espace public.

Les pouvoirs publics semblaient prêts à lancer cette expérimentation. Le 24 décembre 2019, avait été annoncé le lancement d'une « *phase d'expérimentation, de six mois à un an, sous la supervision de la société civile et des chercheurs* » pour évaluer l'usage de la reconnaissance faciale à la vidéosurveillance[2]. Ce projet d'expérimentation a été abandonné et différentes raisons ont été invoquées : l'attente de la législation européenne en matière d'intelligence artificielle en cours d'élaboration[3], l'absence de certitude sur la nécessité d'un cadre légal *ad hoc* pour mener cette expérimentation, ou encore, les échéances électorales du printemps 2022 peu propices à un débat apaisé.

Cédric O, secrétaire d'État chargé de la transition numérique et des communications électroniques, l'a confirmé lors de son audition du 16 mars 2022 : « *la décision d'avoir recours à l'identification pour les jeux Olympiques de 2024 aurait dû être prise maintenant :* ***le Gouvernement a choisi de ne pas le faire, compte tenu du contexte politique et de la sensibilité du sujet****. Cela interdit donc de fait l'utilisation de dispositifs d'identification, mais ne devrait cependant pas nous empêcher* ***d'avancer sur l'authentification de certains personnels pour l'accès aux sites olympiques****, par exemple. Nous devrons donc trouver les moyens d'assurer la sécurité des jeux sans recourir à l'identification en temps réel* » [4].

La directrice des libertés publiques et des affaires juridiques du ministère de l'intérieur a de son côté indiqué aux rapporteurs que le ministère de l'intérieur réfléchissait à la mise en œuvre d'expérimentations destinées à sécuriser ces évènements et les grands rassemblements qu'ils

---

[1] *Selon le rapport de Jean-Michel Mis, député, au Premier ministre, environ 13 millions de billets seront vendus pour les compétitions en stade, auxquels s'ajouteront les visiteurs en* fanzones *et* live sites *(13 millions de personnes à Londres en 2012).*

[2] *Entretien avec Cédric O, secrétaire d'État chargé de la transition numérique et des communications électroniques, Caroline Piquet,* Le Parisien*, 24 décembre 2019.*

[3] https://www.senat.fr/questions/base/2020/qSEQ200113854.html.

[4] *Voir le compte rendu de l'audition de Cédric O, secrétaire d'État chargé de la transition numérique et des communications électroniques, du 16 mars 2022.*

impliquent. Mais il ne devrait s'agir désormais que de dispositifs de contrôle d'accès des personnels ou des athlètes en cohérence avec les propos tenus par le secrétaire d'État chargé de la transition numérique et des communications électroniques.

### *B. UN ENCADREMENT JURIDIQUE BALBUTIANT*

#### *1.* Une régulation actuelle par des normes centrées sur la protection des données personnelles

Tout comme les données relatives à la santé, aux opinions politiques ou les données génétiques, les « *données biométriques aux fins d'identifier une personne physique de manière unique* » sont des données « sensibles » au sens de l'article 9 du RGPD[1] et de l'article 10 de la directive « Police-Justice »[2], dont la définition a été reprise par l'article 6 de la loi du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*[3].

Ces données font l'objet d'un **encadrement juridique** strict car elles ont la particularité de permettre à tout moment l'identification de la personne sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir.

De ce fait, c'est principalement sous l'angle de la protection des données personnelles qu'est organisée la régulation de la reconnaissance faciale en France. Dans le RGPD, le principe est **l'interdiction de tels traitements**. Ils ne peuvent être mis en œuvre que **par exception** et dans certains cas particuliers : principalement, avec le consentement exprès des personnes, pour protéger leurs intérêts vitaux ou sur la base d'un intérêt public important. La directive « Police-Justice » ne permet, elle, le traitement de telles données qu'en cas de **nécessité absolue** et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée.

Ces données sont également **soumises aux principes généraux du RGPD**, dont le principe de minimisation des données : les traitements de données doivent être « *[adéquats, pertinents et limités] à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

---

[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 (règlement général sur la protection des données).

[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] *Loi n° 78-17 du 6 janvier 1978* relative à l'informatique, aux fichiers et aux libertés.

La loi du 20 juin 2018 *relative à la protection des données personnelles*[1] est venue modifier la loi du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*[2] pour transcrire ces principes dans le droit interne français. En particulier, le régime d'autorisation préalable qui existait en matière de données sensibles a été remplacé par un **régime de responsabilisation des acteurs** sur qui repose l'obligation de formaliser une **analyse d'impact** en cas de risque élevé pour les droits et libertés de la personne concernée et, dans certains cas seulement, de consulter la CNIL.

Compte tenu de la sensibilité de l'utilisation des données biométriques, le législateur a subordonné la mise en place des traitements de données sensibles, **lorsqu'ils sont mis en œuvre pour le compte de l'État agissant dans l'exercice de ses prérogatives de puissance publique**, à des **formalités préalables**[3]. À ce titre, ces traitements[4] doivent être autorisés par décret en Conseil d'État[5], pris après avis de la CNIL, et l'analyse d'impact relative aux données personnelles doit systématiquement être adressée à la CNIL avec demande d'avis[6].

En dehors du champ d'application de la directive « Police-Justice », la CNIL estime que le RGPD offre des marges de manœuvre suffisantes car en cas d'intérêt public important, il est possible de ne pas reposer sur le consentement des personnes. L'analyse des acteurs, qui regrettent **la rigidité de la CNIL,** est tout autre. Renaud Vedel, coordonnateur national pour l'intelligence artificielle, constate par exemple que la législation ne permet pas de distinguer la reconnaissance faciale *stricto sensu*, qui vise délibérément à identifier une personne physique, de l'analyse vidéo augmentée, qui peut procéder à l'analyse du visage à d'autres fins que l'identification.

### 2. Un encadrement européen encore en construction : le futur règlement sur l'intelligence artificielle

La proposition de règlement relative à l'intelligence artificielle (IA) publié en avril 2021[7] est conçue comme une **réponse politique de l'Europe au système de contrôle social chinois**[8].

---

[1] *Loi n° 2018-493 du 20 juin 2018* relative à la protection des données personnelles.
[2] *Loi n° 78-17 du 6 janvier 1978* relative à l'informatique, aux fichiers et aux libertés.
[3] *Article 27 de la loi du 6 janvier 1978* relative à l'informatique, aux fichiers et aux libertés.
[4] *Sauf si le traitement vise à protéger les intérêts vitaux d'une personne physique ou s'il porte sur des données manifestement rendues publiques par la personne concernée (article 88 de la loi du 6 janvier 1978* relative à l'informatique, aux fichiers et aux libertés*).*
[5] *Une loi est également possible.*
[6] *Article 90 de la loi du 6 janvier 1978* relative à l'informatique, aux fichiers et aux libertés.
[7] *Proposition de règlement du Parlement européen et du Conseil* établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union (COM/2021/206 final).
[8] *Audition du représentant permanent de la France auprès de l'Union européenne (RPFUE).*

Elle se fonde sur une « *approche réglementaire horizontale équilibrée et proportionnée de l'IA qui se limite aux exigences minimales nécessaires pour répondre aux risques et aux problèmes liés à l'IA, sans restreindre ou freiner indûment le développement technologique ni augmenter de manière disproportionnée les coûts de mise sur le marché de solutions d'IA* »[1].

La Commission européenne propose de consacrer une **définition technologiquement neutre des systèmes d'intelligence artificielle (**IA) dans le droit de l'Union européenne et d'établir une classification pour les systèmes d'IA imposant différentes exigences et obligations adaptées, **selon une approche fondée sur les risques.**

Les systèmes biométriques, comme la reconnaissance faciale, seraient considérés comme « IA à haut risque ».

Par principe, la Commission européenne propose **d'interdire l'utilisation des systèmes d'IA pour l'identification biométrique à distance en temps réel de personnes physiques dans des espaces accessibles au public à des fins répressives**[2]. Trois exceptions seraient toutefois prévues, lorsqu'un intérêt public important l'emporte sur les risques pour les droits fondamentaux : la **recherche ciblée de victimes potentielles d'actes criminels**[3], la **prévention d'une menace spécifique, substantielle et imminente** pour la vie ou la sécurité physique des personnes ou la prévention d'une attaque terroriste, et **la détection, la localisation, l'identification ou aux poursuites de l'auteur ou d'une personne soupçonnée d'avoir commis une infraction pénale d'une certaine gravité** dont il est fait état dans la décision-cadre relative au mandat d'arrêt européen[4].

Les systèmes d'IA destinés à être utilisés pour l'identification biométrique à distance en temps réel et ***a posteriori*** seraient classés **« à haut risque »** et soumis en conséquence à des obligations renforcées (évaluation de conformité avant la mise sur le marché, exigences en matière de sécurité concernant, par exemple, la gestion des risques, le contrôle humain et la gouvernance des données).

Enfin, les technologies de reconnaissance faciale pouvant être considérées comme des **systèmes de catégorisation biométrique** (destinés à affecter des personnes physiques à des catégories spécifiques selon le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, l'origine ethnique ou l'orientation sexuelle ou politique, *etc.*, sur la base de leurs données biométriques), **dès lors qu'ils ne relèvent pas de cas d'utilisation**

---

[1] *Voir l'exposé des motifs de la proposition de règlement.*

[2] *Voir l'article 5* (d) *de la proposition de règlement.*

[3] *L'exception pour la recherche d'enfants disparus semble avoir été abandonnée sous la présidence slovène, pour faire primer le droit à l'oubli et l'anonymat, ce qui n'empêche pas la recherche d'enfants victimes.*

[4] *Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002* relative au mandat d'arrêt européen et aux procédures de remise entre États membres.

**identifiés comme à haut risque**[1] - par exemple dans les domaines de l'emploi, de l'éducation, du maintien de l'ordre, de la migration et du contrôle aux frontières -, seraient soumises uniquement à des **mesures de transparence et d'information** des personnes concernées.

**Proposition de règlement en matière d'IA :**
**scénarios de réglementation des systèmes de reconnaissance faciale**[2]

| **Technique de reconnaissance faciale règlementée** | **Systèmes de reconnaissance faciale [à distance] en temps réel dans des espaces accessibles au public à des fins répressives** | | **Autres systèmes d'identification (en temps réel ou *a posteriori*) par reconnaissance faciale [à distance]** | **Systèmes de reconnaissance faciale à des fins de catégorisation** |
|---|---|---|---|---|
| **Règle** | Interdits par principe (risque inacceptable) | Autorisés pour des exceptions spécifiques (haut risque)<br>- Recherches de victimes d'actes criminels<br>- Menace pour la vie ou pour l'intégrité physique ou menace d'acte de terrorisme<br>- Infraction grave (mandat d'arrêt européen) | Autorisés (haut risque) | Autorisés (risque faible) |
| **Conditions** | | Autorisation *ex ante* (autorité judiciaire ou organisme administratif indépendant) | - Exigences préalables à la commercialisation<br>- Évaluation de conformité *ex ante* (autoévaluation ou évaluation par un tiers)<br>- Surveillance et supervision ex post du marché | - Transparence<br>- Information |

*Source : Analyse approfondie de la Règlementation de la reconnaissance faciale au sein de l'Union européenne, Service de recherche du Parlement européen*

[1] Les nouvelles règles encadrant l'intelligence artificielle, *Questions et réponses de la Commission européenne, 21 avril 2021.*

[2] *La législation préexistante, notamment les règles en matière de protection des données et de non-discrimination, continuerait par ailleurs de s'appliquer.*

Certains, comme la direction générale des douanes et droits indirects, regrettent que « *la démarche du projet [... ait] pour conséquence de* ***creuser un fossé inexplicable entre secteur public et secteur privé****. La Commission européenne postule en effet que l'usage de l'IA dans le secteur privé mérite moins d'attention que son usage dans le secteur public* »[1]. C'est ainsi, par exemple, que l'interdiction *a priori* de l'usage de l'identification biométrique en temps réel ne s'applique **qu'aux forces de l'ordre**[2], tandis que l'interdiction de système de notation sociale ne concerne que **les pouvoirs publics ou leurs sous-traitants**[3]. De même, des juristes[4] ont-ils noté que les IA à haut risque concernaient majoritairement des secteurs relevant de la puissance publique[5].

La proposition de règlement a été transmise au Parlement européen et au Conseil qui sont en cours d'élaboration leur position. **De nombreux points relevant de la justice et des affaires intérieures restent en discussion**. Ainsi le gouvernement français souhaite-t-il notamment que soient exclus de l'application du règlement non seulement les systèmes d'IA développés ou utilisés exclusivement à des fins militaires, mais également ceux qui le sont **à des fins de sécurité nationale** ou que l'interdiction de l'usage de l'identification biométrique en temps réel ne porte que sur les **contrôles à distance**, précision qui a été supprimée en cours de discussion lors de la présidence slovène.

### 3. Une autorégulation des acteurs insatisfaisante

En l'absence de cadre spécifique et compte tenu des enjeux sociétaux posés par la reconnaissance faciale, les développeurs américains et européens indiquent **défendre un usage et un développement responsables et éthiques des technologies biométriques**.

En juin 2020, Microsoft, par la voix de son président Brad Smith, a annoncé que son entreprise ne vendrait pas de solutions de technologie de reconnaissance faciale aux forces de l'ordre des États-Unis avant l'adoption d'une loi fédérale encadrant son utilisation. Elle a créé un « **bureau de l'IA responsable** » chargé de procéder à une revue des scénarios utilisant la reconnaissance faciale au regard de six principes éthiques identifiés.

La société IBM a de son côté organisé un « **comité d'éthique de l'IA »** pour soutenir un processus centralisé de gouvernance, d'examen et de

---

[1] *Réponses de la direction générale des douanes et droits indirects au questionnaire des rapporteurs.*

[2] « À des fins répressives » *précise la proposition.*

[3] *Article 5* (c) *de la proposition de règlement.*

[4] « Le projet européen de réglementation de l'intelligence artificielle oublie les citoyens », *tribune de Marc Clément, magistrat administratif, et Daniel Le Métayer, chercheur spécialiste des algorithmes, publiée dans* Le Monde *du 9 juin 2021.*

[5] *Police, justice, contrôle aux frontières, infrastructures stratégiques comme l'électricité, l'eau ou le gaz, éducation et accès à des services essentiels.*

décision sur les politiques, les pratiques, la communication, la recherche, les produits et services d'IBM en matière d'éthique.

La société Facebook, pour sa part, indique utiliser un « **cadre d'innovation responsable »** et s'engager avec des experts extérieurs pour garantir que les futurs systèmes sont fiables et équitables.

En France, la société Thales s'appuie sur l'approche « TrUE » qui prône la traçabilité, l'intelligibilité et l'éthique. L'Alliance pour la confiance numérique (ACN) revendique une vision française et européenne de la confiance numérique et contribue activement, dans le cadre du comité stratégique de filière « Industries de sécurité », à l'élaboration d'une **charte éthique de la profession visant à rendre plus visibles les valeurs fondamentales européennes**. La société ID3 Technologies se fixe ses propres lignes rouges : son président a indiqué aux rapporteurs refuser de développer des algorithmes pour équiper des armes létales ou vendre des solutions de reconnaissance faciale à des systèmes dictatoriaux...

Chaque entreprise développe donc son propre cadre éthique et responsable, ce qui ne semble pas offrir les garanties suffisantes. Caroline Lequesne-Roth, maître de conférences en droit public à l'Université Côte d'Azur, relève ainsi que « *la juridicisation des enjeux éthiques apparaît [...] indispensable pour **éviter leur instrumentalisation**. Ainsi, les prises de position de certains géants du numérique, pour louables qu'elles soient, annonçant la suspension de leurs activités en matière de reconnaissance faciale - ou plus récemment, d'une reconnaissance faciale dite "éthique" - **n'offrent pas de garanties suffisantes.** Elles induisent de surcroît **un biais d'acceptabilité**, qui pourrait conduire à desserrer la contrainte réglementaire et institutionnaliser,* in fine*, des pratiques démocratiquement contestables* »[1].

## *III.* DES ENJEUX FORTS EN TERMES DE LIBERTÉS PUBLIQUES ET DE SOUVERAINETÉ

### *A. UNE TECHNOLOGIE SUSCEPTIBLE DE PORTER ATTEINTE À DE NOMBREUSES LIBERTÉS PUBLIQUES*

**L'installation progressive de la reconnaissance faciale dans notre quotidien et son utilisation, certes limitée, par les pouvoirs publics, y compris pour des usages policiers, ne vont pas sans poser de questions sur le plan de la sauvegarde des libertés publiques**. Particulièrement intrusive, cette technologie est en effet susceptible de porter atteinte à de nombreuses libertés, au premier rang desquelles le droit à la vie privée. Même les usages *a priori* les moins problématiques comme les systèmes d'authentification requérant le consentement peuvent susciter des interrogations, par exemple lorsqu'il n'existe pas d'alternative pour accéder au service concerné ou au

[1] *Réponses de Caroline Lequesne-Roth au questionnaire des rapporteurs.*

sujet du niveau de sécurisation des données à caractère personnel. L'ensemble des personnes auditionnées par les rapporteurs convergent ainsi pour dire que les technologies de reconnaissance biométrique du visage soulèvent des questions majeures en termes de protection des libertés, pour des raisons extrêmement variées et avec des nuances qui s'expriment quant à la manière d'y répondre.

Dans ce contexte, les implications du développement de la reconnaissance faciale sur la sauvegarde des libertés publiques doivent guider à chaque étape la réflexion parlementaire. **Alors que ce sujet d'une importante technicité suscite une préoccupation légitime au sein de la société civile, il est de la responsabilité du Parlement d'objectiver le débat en procédant à une évaluation sincère, exhaustive et transparente des risques engendrés par la montée en puissance de la reconnaissance faciale**. Ces risques peuvent être classés en **trois catégories**, selon qu'ils tiennent :

**- à la nature et au recueil des données utilisées par les algorithmes ;**

**- à l'emploi en tant que tel des solutions de reconnaissance faciale ;**

**- aux modalités techniques de fonctionnement des algorithmes.**

### 1. Les risques liés à la nature et au recueil des données utilisées par les algorithmes

*a) La biométrie du visage, une donnée particulièrement sensible*

**Les données nécessaires aux algorithmes de reconnaissance faciale pour fonctionner revêtent un caractère sensible à double titre.**

Comme pour toute donnée biométrique, le traitement des données biométriques du visage doit faire l'objet d'une vigilance particulière dès lors que ces données permettent, selon les termes de la CNIL, « *à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir* »[1]. **Loin d'être une donnée anodine, la biométrie du visage touche au plus profond de notre identité personnelle**. **Les conséquences potentielles d'un traitement détourné, disproportionné ou dysfonctionnel de cette donnée peuvent se révéler particulièrement dommageables**, s'étirant du refus d'accès à un service déterminé jusqu'à une implication injustifiée dans une enquête criminelle. Juridiquement, cette caractéristique justifie la classification de la biométrie du visage au rang des « ***données*** [à caractère personnel] ***sensibles*** » au sens tant de l'article 9 du RGPD que de l'article 10 de la directive dite « *Police-Justice* » et dont le traitement est, en principe, prohibé.

[1] « Reconnaissance faciale : pour un débat à la hauteurs des enjeux », *CNIL, 15 novembre 2019 (p. 6).*

**Surtout, à la différence d'autres données biométriques telles que les empreintes digitales ou l'iris, le visage d'un individu peut être recueilli à distance et potentiellement à son insu, voire contre son gré**. Le Défenseur des droits oppose ainsi les technologies « *actives* » nécessitant une action volontaire de l'individu pour fournir la donnée, des technologies « *passives* » où son recueil est possible sans intervention du sujet[1]. C'est le cas de la biométrie du visage et, par conséquent, de la reconnaissance faciale.

**Cette possibilité de captation furtive renforce substantiellement le risque d'atteinte aux libertés publiques et justifie l'introduction de garanties renforcées.**

*b) La constitution des bases de données d'apprentissage et de comparaison*

**Au-delà de la nature même de la donnée utilisée, ce sont les conditions de son recueil qui sont synonymes de risques pour les libertés publiques**. Deux constats s'imposent. D'une part, **le recueil des données biométriques du visage est aujourd'hui relativement aisé**, compte tenu de la progression constante des dispositifs de captation et de la disponibilité directe d'un volume massif d'images sur l'espace numérique. D'autre part, **cet accès facilité à une donnée indispensable au développement et à l'utilisation des algorithmes génère des risques d'appropriation indue et soulève la question du consentement et de l'information des personnes concernées**.

Il convient de garder à l'esprit que la performance d'un algorithme est conditionnée par le nombre, la qualité et la diversité des données qui lui sont soumises, que ce soit à des fins :

**- d'entraînement** : tout algorithme doit être préalablement entraîné sur des jeux de données « *d'apprentissage* » avant d'atteindre un niveau de fiabilité satisfaisant ;

**- d'utilisation en conditions réelles** : la base de données soumise à l'algorithme pour la recherche d'une correspondance dépendra de la finalité d'usage.

(1) Des moyens de captation de la donnée de plus en plus répandus et performants

On observe, sur la période récente, **une très forte progression des dispositifs de captation d'images**, et par conséquent des moyens de recueil de données biométriques du visage, autour de trois mouvements concomitants :

**- leur multiplication :** au fil du progrès technologique, les appareils de captation tendent à se diversifier (smartphones, télé-connectées, caméras portatives…) ;

[1] *Défenseur des droits,* Technologies biométriques : l'impératif respect des droits fondamentaux*, 2021 (p. 8).*

**- leur démocratisation :** chaque individu est potentiellement en capacité de recueillir le visage d'une personne, par exemple en réalisant des photos ou des vidéos avec son *smartphone*. Cela se fait parfois de manière inconsciente, par la captation incidente de personnes en arrière-plan. Or une donnée biométrique, en l'espèce le gabarit du visage, peut être en théorie extraite de n'importe quelle photo, au prix d'une manipulation plus ou moins lourde ;

**- leur perfectionnement :** certains dispositifs de captation atteignent désormais des niveaux de résolution particulièrement élevés, facilitant d'autant l'extraction du gabarit et le recours à la reconnaissance faciale.

**Ce constat est particulièrement vérifié s'agissant du recueil d'images sur la voie publique par les forces de sécurité intérieure.** En effet, le nombre et la qualité des dispositifs de captation d'images, fixes ou mobiles, déployés sur l'espace public ont considérablement augmenté au cours des dernières années. Force est de constater **que, en théorie, les forces de sécurité intérieure pourraient utiliser la reconnaissance faciale sur un vaste périmètre et à partir d'un réservoir de données conséquent**.

**Des dispositifs publics de captation de données sur la voie publique de plus en en plus répandus**

La Cour des comptes estimait en 2011 à près de 10 000 le nombre de caméras de vidéoprotection installées sur l'espace public. Sept années plus tard ce chiffre se portait, selon les données à sa disposition, entre 60 000 selon la direction des libertés publiques et des affaires juridiques (DLPAJ) et 76 000 selon les directions métiers (819 communes dotées de 37 757 caméras en zone police, sans compter Paris et la petite couronne, et 3 200 communes équipées de 38 700 caméras en zone gendarmerie)[1]. On observe toutefois de fortes disparités entre les communes en termes de ratio de caméra par habitants, pouvant aller de 0 jusqu'à une pour 99 personnes, comme dans le cas de Berre-l'Étang dans les Bouches-du-Rhône.

Plus récemment, l'institution de la rue Cambon s'est penchée sur le plan de vidéoprotection de la préfecture de police de Paris[2], pour l'application duquel elle communique le chiffre de 4 000 caméras déployées en propre par la préfecture de police et de plus de 37 000 caméras interconnectées sur le territoire régional.

Par ailleurs, ces chiffres ne tiennent pas compte du recours à des caméras mobile par les forces de l'ordre ou les sapeurs-pompiers.

*Source : Commission des lois du Sénat*

[1] *Cour des comptes, rapport public thématique,* Les polices municipales, *octobre 2020 (p. 64).*
[2] *Cour des comptes, référé,* Le plan de vidéoprotection de la préfecture de police de Paris, *10 février 2022.*

(2) Des données parfois directement accessibles au public

Si les dispositifs de captation du visage ont connu une progression exponentielle, ils ne sont pas nécessairement indispensables au recueil de la donnée, tant celle-ci peut être **directement et massivement accessible dans l'espace numérique**. Selon les estimations publiques disponibles et avec les précautions d'usage, près de deux milliards d'individus utiliseraient par exemple quotidiennement le réseau social Facebook dans le monde, et 350 millions d'images y seraient enregistrées chaque jour pour un volume total d'environ 250 milliards de photos stockées[1].

**Estimations disponibles du nombre d'utilisateurs quotidiens des principaux réseaux sociaux (en 2021)**

| | **Facebook** | **Instagram** | **Youtube** |
|---|---|---|---|
| **Utilisateurs mensuels** *(en millions)* | 2 895 | 1 386 | 2 291 |
| **Stock de photos/vidéos** *(en milliards)* | 350 | 50 | - |
| **Dont ajout quotidiens** *(en millions)* | 250 | 100 | 720 000 heures |

*Source : Tableau constitué à partir des données accessibles publiquement sur le site internet le « Blog du modérateur »*[2]

À bien des égards, **Internet constitue donc un vivier quasi-infini d'images, dont une proportion importante, bien qu'impossible à évaluer avec certitude, d'images du visage permettant d'en extraire les données biométriques**.

(3) Une disponibilité accrue de la donnée qui emporte des risques

**L'accès de plus en plus aisé à des données biométriques n'est pas sans conséquences pour les libertés publiques**. Ainsi que la démontré l'exemple précité de la société *Clearview AI*, **le risque d'appropriation indue des données biométriques de tout un chacun est réel**. Pour rappel, cette société a été mise en demeure fin 2021 par la CNIL[3] pour avoir « *aspiré* » sans base légale et sans recueil du consentement des intéressés, près de 10 milliards d'images disponibles sur internet afin de constituer une base de données biométriques mise à disposition de ses clients, dont des services de maintien de l'ordre. **La possibilité de perdre la maîtrise d'une donnée aussi sensible que la biométrie du visage, parfois sans même être alertée, a ainsi déjà été éprouvée**.

---

[1] *Selon les données accessibles publiquement sur le site internet le « Blog du modérateur » : https://www.blogdumoderateur.com/chiffres-facebook/.*

[2] Ibid.

[3] *Décision n° MED-2021-134 du 26 novembre 2021 mettant en demeure la société* Clearview AI.

### 2. Les risques liés à l'emploi de la reconnaissance faciale

*a) Une technologie dont l'emploi est susceptible de porter atteinte à de nombreuses libertés publiques*

(1) La reconnaissance faciale : une technologie qui n'est jamais banale

**Les rapporteurs estiment qu'aucun usage de la reconnaissance faciale n'est complètement neutre au regard des libertés publiques**. Certains d'entre eux, tels que le déverrouillage de son smartphone, peuvent certes paraître présenter des risques limités, dans la mesure où il existe une alternative et où le recours à la reconnaissance faciale n'a d'autres conséquences que d'autoriser ou non l'accès au menu de son smartphone. Le cas cité par la CNIL de distributeurs de billets de banques reconnaissant leurs clients par reconnaissance faciale peut également être perçu comme une modalité supplémentaire et bienvenue de sécurisation des transactions[1]. **Sans remettre en cause les bénéfices réels que peut apporter la reconnaissance faciale dans certains de ces cas, leur diffusion croissante, apparemment anodine, appelle deux remarques des rapporteurs** :

- **elle engendre un risque d'accoutumance** : l'installation progressive et « *à bas bruit* » de la reconnaissance faciale dans notre quotidien pourrait faussement instaurer l'idée d'une acceptabilité par défaut de cette technologie, alors même que certains cas d'usages sont beaucoup plus problématiques ;

- **la question de la porosité entre les usages ne peut être éludée** : la technologie et ses cas d'usages ne se recoupent que partiellement. D'un point de vue purement technique, et ainsi que l'ont confirmé les auditions conduites par les rapporteurs avec différents acteurs du secteur, un même algorithme peut être utilisé pour plusieurs finalités, au prix d'ajustements plus ou moins lourds. Par exemple, un même algorithme d'identification pourrait, à partir d'une base de données appropriée, tout aussi bien être utilisé pour retrouver des personnes disparues que pour repérer des personnes d'intérêt au cours d'une manifestation ou aux abords d'un lieu de culte, avec à la clé des conséquences sensiblement différentes sur le plan des libertés publiques.

(2) Des cas d'usages qui emportent des risques importants d'atteintes aux libertés publiques

Les travaux menés par les rapporteurs comme l'examen de la littérature disponible permettent de dégager un constat clair : **les conséquences de la reconnaissance faciale en matière de sauvegarde des libertés publiques constituent une source de préoccupation unanimement partagée** par les acteurs impliqués. Côté institutionnel, le Défenseur des droits évoque « *des risques considérables d'atteinte aux droits*

[1] *Rapport précité.*

*fondamentaux* »[1], tandis que le député Jean-Michel Mis souligne les « *enjeux fondamentaux pour les libertés* »[2] suscités par les évolutions techniques en cours, dont le développement de la reconnaissance faciale. Comme évoqué précédemment, certains acteurs de la recherche et du développement ont mené une réflexion approfondie sur cet aspect, avec des conséquences diverses, allant de l'adoption de normes éthiques internes jusqu'à l'arrêt de toute activité liée à la reconnaissance faciale.

Parce qu'elle repose sur des données sensibles et qu'elle est susceptible d'être mobilisée pour des finalités extrêmement diverses, y compris de la part des forces de sécurité intérieure, la reconnaissance faciale peut potentiellement porter atteinte à de nombreuses libertés publiques. Si en dresser la liste exhaustive est sans doute illusoire, compte tenu de la multiplicité des cas d'usages, **ces potentielles atteintes peuvent schématiquement être classées en deux catégories**.

**La première catégorie est celle des atteintes directes à un droit ou une liberté protégés**. Elles concernent au premier chef le **droit à la protection des données à caractère personnel**, garantie tant par la loi Informatique et Libertés que par le RGPD, et le **droit au respect de la vie privée**. Au niveau européen, cette notion est comprise dans le droit à la « *vie privée et familiale* » consacré par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. En droit interne, elle a été inscrite en 1970 à l'article 9 du code civil[3] puis consacré par le juge constitutionnel[4]. Ainsi que le rappelaient Yves Détraigne et Anne-Marie Escoffier en 2009, cette notion de respect recouvre à la fois les concepts d'intimité et d'autonomie, tandis que le droit au respect de la vie privée doit être généralement entendu comme « *un droit à la tranquillité* »[5]. Particulièrement intrusive, la reconnaissance faciale peut de toute évidence représenter une entrave à l'exercice de ces deux droits.

**La seconde catégorie est celles des atteintes indirectes à des droits ou libertés protégés par l'intermédiaire d'un « *chilling effect* »**. Ce terme décrit la théorie selon laquelle la seule connaissance de l'utilisation, ou de la potentielle utilisation, d'une technologie de surveillance va amener le citoyen à modifier son comportement. Selon les termes du député Jean-Michel Mis, cette « *pression indirecte* » générerait ainsi des « *comportements d'autocensure* »[6]. Sans que l'usage en tant que tel de la

---

[1] *Rapport précité.*
[2] *Jean-Michel Mis,* Pour un usage responsable et acceptable par la société des technologies de sécurité*, septembre 2021.*
[3] *Loi n° 70-643 du 17 juillet 1970* tendant à renforcer la garantie des droits individuels des citoyens.
[4] *Décision 99-416 DC du 23 juillet 1999.*
[5] *Sénat, Rapport d'information de Yves Détraigne et Anne-Marie Escoffier au nom de la commission des lois,* La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, 2009.*
[6] *Rapport précité.*

reconnaissance faciale soit attentatoire aux libertés, il empêcherait *de facto* les citoyens de jouir pleinement de leurs droits et libertés. **Sans être exhaustif, la liberté d'aller et venir, de réunion, d'association, de culte ou d'expression sont autant de libertés dont la portée pourrait être restreinte du fait d'un usage illégitime ou disproportionné de la reconnaissance faciale**.

*b)* A maxima*, le risque d'une* « société de surveillance »

Certains cas d'usages envisageables de la reconnaissance faciale emportent des risques particulièrement élevés pour les libertés publiques. Comme le relève la CNIL, cette technologie porte en effet en elle un « ***potentiel de surveillance inédit*** »[1], au vu notamment de la démultiplication des capteurs d'images au sein de la société et de la possibilité de les coupler à des systèmes de reconnaissance faciale.

L'une des inquiétudes majeures, à laquelle les rapporteurs s'associent sans réserve, concerne le développement de la reconnaissance faciale sur l'espace public à distance et en temps réel. Dans une vision maximaliste, **l'usage d'un outil capable d'identifier une personne sur la voie publique, d'en suivre les mouvements en temps réel et, le cas échéant, de reconstituer son parcours signerait la fin de l'anonymat dans l'espace public et l'avènement d'une forme de « *société de la surveillance* » que personne ne peut raisonnablement souhaiter.**

**Si les instruments à notre disposition ne semblent en l'état pas pouvoir être utilisés à cette fin, ne serait-ce que par l'absence d'une base de données universelle permettant les comparaisons, leur progression constante incite à adopter dès à présent une position ferme sur le sujet**.

**Dans le monde,**
**des cas d'usage contestables de la reconnaissance faciale**
**ont déjà pu être observés**

Dans son rapport précité intitulé « *Technologies biométriques : l'impératif respect des droits fondamentaux* », le Défenseur des droits met en avant plusieurs cas d'usage de la reconnaissance faciale qui ont été observés à travers le monde et qui interrogent fortement au regard de leur impact sur les libertés :

- **en Russie** : des systèmes de reconnaissance faciale sont désormais largement implantés dans les stations de métro de Moscou afin de pouvoir procéder à des paiements sans contact, mais aussi d'identifier des personnes recherchées. Néanmoins, les autorités locales auraient également utilisé le système municipal de vidéoprotection pour contrôler le respect des mesures de restriction sanitaire pendant la pandémie ;

[1] *Rapport précité.*

- **en Italie** : le rapport du Défenseur des droits revient sur l'interdiction par l'autorité italienne de protection des données du système mobile « *Sari real time* »[1] qui aurait notamment été utilisé par la police, en raison de l'absence de base légale pertinente et du risque de surveillance indiscriminée.

*Source : Commission des lois du Sénat*

*c) Une position incertaine de la société civile vis-à-vis du déploiement de la reconnaissance faciale*

La question de la reconnaissance faciale génère des réactions équivoques au sein de la société civile. **Il existe encore peu de sondages sur le sujet, et ceux qui sont disponibles ne permettent pas d'obtenir des certitudes quant à l'état de l'opinion sur cette technologie**. À titre d'exemple, un sondage Odoxa réalisé l'année dernière indiquait que 50 % des Français étaient favorables à l'usage de la reconnaissance faciale à des fins de sécurité, pour 49 % d'avis contraire[2]. Selon une autre étude, une large majorité de Français estimaient que le fait que cette technologie puisse manquer de transparence concernant le traitement des données collectées (85 %) ou risque de réduire les libertés individuelles (82 %) jouait de manière déterminante ou importante en défaveur de son utilisation[3]. Par ailleurs, les Français semblent majoritairement éprouver un sentiment de mauvaise information quant à l'utilisation de leurs données personnelles[4].

La plupart des acteurs associatifs intervenant sur le sujet et auditionnés par les rapporteurs affichent **une position nettement plus tranchée à l'égard de la reconnaissance faciale**. C'est par exemple le cas des associations La Quadrature du Net et la Ligue des droits de l'homme qui ont manifesté leur opposition sans réserve tant aux systèmes de reconnaissance faciale qu'aux technologies connexes se focalisant, par exemple, sur l'habillement des personnes. Le risque d'un « *effet cliquet* » matérialisé par la pénétration actuelle d'usages « *ludiques* » tels que le déverrouillage de téléphone comme préalable à des utilisations plus problématiques a notamment été évoqué. L'association Amnesty International, qui a certes établi une distinction entre les usages d'authentification et d'identification au cours de l'audition, a de son côté lancé une pétition appelant à « *établir de*

---

[1] *Rapport précité.*

[2] *Sondage Odoxa pour le rendez-vous de l'innovation,* « La sécurité et la surveillance en ligne », *13 mai 2021. Ce sondage est consultable à l'adresse suivante : http://www.odoxa.fr/wp-content/uploads/2021/05/Rendez-vous-de-linnovation-Mai-2021.pdf.*

[3] *Enquête* « Reconnaissance faciale : quel regard des Français ? » *pour Renaissance numérique et selon la méthodologie de l'IFOP, décembre 2019. Cette enquête est consultable à l'adresse suivante : https://www.renaissancenumerique.org/publications/reconnaissance-faciale-ce-que-nous-en-disent-les-francais.*

[4] *Selon un sondage Odoxa dont les résultats ont été publiés en mai 2021 dans une dépêche d'AEF info, 75 % des Français se disent mal informés sur l'utilisation de leurs données personnelles. Ce sondage est consultable à l'adresse suivante : https://www.aefinfo.fr/depeche/652827-reconnaissance-faciale-74-des-francais-la-jugent-incontournable-pour-la-securite-et-la-surveillance-sondage-odoxa.*

*manière définitive une interdiction mondiale des technologies de reconnaissance faciale permettant une surveillance de masse et discriminatoire* », qui réunissait 49 761 signataires au 30 avril 2022[1].

Les rapporteurs considèrent **qu'il doit être remédié à l'absence de données précises sur l'état de l'opinion vis-à-vis de la reconnaissance faciale, et plus largement biométrique, par la réalisation d'une étude** qui poursuivrait trois objectifs :

- dresser un état des lieux général de la perception de cette technologie par les Français ;

- cerner précisément les cas d'usages auxquels la population apparaît plutôt favorable et, *a contrario*, identifier les principales sources d'inquiétudes ;

- identifier les ressorts d'une meilleure acceptabilité de cette technologie, en particulier les garanties perçues comme indispensables pour susciter la confiance entre la population et les utilisateurs de la reconnaissance faciale.

De l'avis des rapporteurs, **la production plus ciblée et régulière de données décrivant l'opinion de la population sur la reconnaissance biométrique est la condition *sine qua non* d'un débat parlementaire éclairé**.

> **Proposition n° 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.**

### 3. Les risques liés au fonctionnement des algorithmes de reconnaissance faciale : des questions sur leur fiabilité qui semblent pouvoir être au moins partiellement résolues

#### *a) Des atteintes potentielles aux libertés publiques étroitement liées au niveau de fiabilité des algorithmes*

**La question de l'impact de la reconnaissance faciale sur les libertés publiques ne peut être déconnectée de celle de la fiabilité de cette technologie. De fait, l'usage d'algorithmes peu performants rend, dans le meilleur des cas, cette technologie inopérante et risque, dans le pire des cas, de décupler les atteintes aux libertés publiques précédemment évoquées**. Les usages policiers de la reconnaissance faciale requièrent notamment un haut niveau de fiabilité, dans la mesure où l'établissement

[1] *Pétition* « La reconnaissance faciale dans nos villes : c'est non ! », *consultable à l'adresse suivante : https://www.amnesty.fr/liberte-d-expression/petitions/non-a-la-reconnaissance-faciale*.

d'une correspondance erronée (faux positif), ou de l'incapacité de l'algorithme à déceler une correspondance pourtant réelle (faux négatif), peuvent se traduire par des conséquences individuelles et collectives particulièrement regrettables.

Toute réflexion sur la fiabilité des algorithmes de reconnaissance faciale suppose de garder à l'esprit trois éléments :

**- la reconnaissance faciale est une technologie par essence probabiliste** : les algorithmes n'ont pas vocation à confirmer ou infirmer définitivement une correspondance entre deux gabarits mais à estimer la probabilité de ladite correspondance. Il appartient à l'être humain de définir un seuil de probabilité adapté au cas d'usage et de configurer l'algorithme en ce sens ;

**- les algorithmes sont sujets à deux types d'erreurs, qui sont interdépendantes** : les taux de faux négatifs et de faux positifs entretiennent une relation de balancier. Lorsque l'algorithme est configuré de manière à produire un faible taux de faux positifs, celui de faux négatifs s'en trouve mécaniquement augmenté, et réciproquement. Là encore, il revient au concepteur de configurer l'algorithme à partir d'un seuil de tolérance à l'un de ces taux et pertinent au regard du cas d'usage. Pour le contrôle de l'accès à un site sensible par exemple, la priorité sera d'empêcher les entrées indues et le système sera donc conçu avec une tolérance faible aux faux positifs, ce qui renchérira le taux de rejets erronés ;

**- les erreurs produites par les algorithmes peuvent s'expliquer par trois principaux facteurs** :

* *la qualité de la conception de l'algorithme et les modalités de son entraînement* : on observe d'importants différentiels de performance selon les développeurs et les algorithmes sont d'autant plus efficaces qu'ils sont entraînés sur des bases de données de grande taille et diversifiées ;

* *des conditions d'emplois plus ou moins favorables* : les résultats produits par les algorithmes dépendent largement de la qualité des données sources. Ils seront sensiblement meilleurs en présence d'une photo d'identité, réalisée de face dans un environnement maîtrisé avec un cadrage et une luminosité optimales, que d'une image de qualité inférieure, du fait de sa résolution, de la posture du sujet, de l'environnement extérieur, ou de son ancienneté par exemple ;

* *d'éventuels « biais »* : des différentiels de performance plus ou moins importants peuvent être observés selon le sexe, l'âge ou l'origine ethnique du sujet de référence.

**Aussi, la question de la fiabilité des algorithmes ne relève pas uniquement de leurs performances intrinsèques, mais également du seuil de correspondance souhaité et du taux d'erreur toléré pour chaque cas d'usage**.

**La fiabilité des algorithmes de reconnaissance faciale est aujourd'hui principalement évaluée par le *National Institute of Standards and Technology* (NIST)**, qui est une agence rattachée au département du commerce des États-Unis. Les algorithmes lui sont transmis par les développeurs, sur une base volontaire, puis testés sur des bases de données internes et construites de manière à évaluer les performances générales de l'algorithme, mais également plus finement selon la qualité des images ou par catégories de population.

**Le NIST, organisme de référence en matière d'évaluation de la fiabilité des algorithmes de reconnaissance faciale**

Le NIST a conduit de premiers travaux dans le champ de la reconnaissance faciale par l'intermédiaire du programme ***Face Recognition Technology (FERET)***. Parrainé par le département de la défense[1], ce programme s'est étalé de 1993 à 1997 pour un montant total d'environ 6,5 millions de dollars. Il visait premièrement à soutenir la recherche par la **constitution d'une base de données centralisée de plus de 14 000 images mise à disposition des développeur**s, en lieu et place des jeux de données que chacun d'entre eux avait rassemblés isolément. Deuxièmement, l'objectif était de professionnaliser l'évaluation des algorithmes, qui étaient jusqu'alors réalisée ponctuellement, sur des bases de données différentes et de faible envergure. **Premiers du genre, les « *tests FERET* » ont permis d'élaborer un référentiel de comparaison unique, construit de manière indépendante et à partir de tests réalisés sur une base de données commune**.

Avec la mise sur le marché des premiers systèmes de reconnaissance faciale au début des années 2000, le besoin est né d'une évaluation robuste de ces algorithmes à usage commercial. Le programme *Face Recognition Vendor Test (FRVT)* a été lancé en 2000 pour prendre en compte ce nouveau contexte et se poursuit depuis lors. Le NIST évalue les performances des algorithmes qui lui sont soumis par des développeurs et publie un classement, régulièrement actualisé. **Depuis 2018, 693 algorithmes d'authentification et 354 d'identification ont ainsi été testés**.

Pour tester les algorithmes, **le NIST a recours à des bases de données massives**. Par exemple, les bases utilisées pour **la dernière batterie d'évaluation des algorithmes d'identification pouvaient contenir jusqu'à 12 millions d'images**. Elles étaient constituées d'images issues des services de l'immigration (photos d'identité, photos prises lors du passage de la frontière, de l'usage d'un kiosque d'enregistrement) et recueillies lors d'opérations de maintien de l'ordre (photos d'identité standard, y compris de profil, photos réalisées à partir d'une webcam).

La méthodologie utilisée par le NIST respecte le **principe de la « *boîte noire* »**. Il ne s'agit pas d'apprécier la manière dont les algorithmes fonctionnent mais d'évaluer leur performance. Il est fait usage de « ***données séquestrées*** » auxquelles les développeurs n'ont accès ni pour tester ni pour entraîner leurs algorithmes, garantissant ainsi un haut niveau de fiabilité de l'évaluation.

*Source : Commission des lois du Sénat*

[1] *Plus précisément le* « Counterdrug Technology Development Program Office ».

b) *Des performances des algorithmes qui progressent rapidement et atteignent, dans des conditions d'emploi optimales, de très hauts niveaux de fiabilité*

À partir des évaluations conduites dernièrement par le NIST, il est possible de formuler le constat suivant : **les algorithmes de reconnaissance faciale sont de plus en plus fiables, y compris lorsqu'ils sont utilisés à partir de données dégradées**, ce que l'agence qualifie en introduction de son dernier rapport sur les algorithmes d'identification[1], de « ***révolution industrielle*** ». De manière générale, l'institut constate que « *le développement de la reconnaissance faciale se poursuit rapidement et que les évaluations FRVT n'offre qu'un aperçu instantané des capacités actuelles* »[2].

**D'un point de vue technique, les taux d'erreurs sont résiduels lorsque les conditions d'emploi sont optimales. Des marges d'amélioration importantes subsistent néanmoins lorsque l'image source est d'une qualité moindre.**

(1) Des taux d'erreurs résiduels dans des conditions d'emploi maîtrisées

Les résultats des dernières séries de tests publiés par le NIST en mars 2022 sur des algorithmes d'identification[3] et d'authentification[4] démontrent **la maturité de cette technologie lorsqu'elle est utilisée à partir d'images de bonne qualité**. La comparaison de photos d'identité réalisées dans un environnement maîtrisé, de face avec un éclairage et un fond adaptés, permet ainsi de réduire à la portion congrue les taux d'erreurs des algorithmes les plus performants.

**En matière d'authentification, les 100 algorithmes les mieux classés présentent un taux de faux négatifs systématiquement inférieur à 0,4 %**. Pour ce qui est de l'identification, des algorithmes atteignent des scores encore plus élevés, avec un taux de faux négatif à 0,12 % pour le premier d'entre eux. Ce niveau de performance est toutefois observé chez un nombre réduit d'algorithmes et le niveau de fiabilité se dégrade rapidement au fil du classement. La taille de la base de données de référence doit également être prise en compte, puisque son augmentation affecte négativement l'efficacité des algorithmes.

---

[1] *Patrick Grother, Mei Ngan, Kayee Hanaoka, NIST - Face Recognition Vendor Test, Part 2: Identification (NISTIR 8271 Draft Supplement), 30 mars 2022.*

[2] *En anglais dans le texte :* « This is evidence that face recognition development continues apace, and that FRVT reports are but a snapshot of contemporary capability ».

[3] Ibid.

[4] *Patrick Grother, Mei Ngan, Kayee Hanaoka, Joyce C. Yang, Austin Homn NIST – Face Recognition Vendor Test, Part 1: Verification, 30 mars 2022.*

**Taux de faux négatifs des algorithmes évalués par le NIST sur des photos d'identité**

| | | Authentification (*) | Identification (**) | |
|---|---|---|---|---|
| | | | *Base de données : 12M* | *Base de données : 1,6M* |
| **Classement de l'algorithme** | ***1*** | 0,21 % | 0,18 % | 0,12 % |
| | ***2*** | 0,22 % | 0,19 % | 0,13 % |
| | ***3*** | | 0,21 % | |
| | ***10*** | 0,24 % | 0,28 % | 0,18 % |
| | ***25*** | 0,26 % | 0,74 % | 0,31 % |
| | ***50*** | 0,30 % | 1,83 % | 0,76 % |
| | ***100*** | 0,39 % | 3,73 % | 1,69 % |

*Source : Commission des lois du Sénat, à partir des données publiées par le NIST en mars 2022.*
*(*) Avec un seuil de tolérance aux faux positifs fixé à 1 pour 100 000.*
*(**) Avec un seuil de tolérance aux faux positifs fixé à 3 pour 1 000.*

(2) Des résultats en progrès mais encore perfectibles en présence d'une donnée source de qualité réduite

Dans un contexte d'amélioration croissante de la fiabilité des algorithmes, le NIST conclut que les erreurs restantes sont principalement dues au « *vieillissement, à la faible résolution de certaines images et aux blessures faciales* »[1]. De fait, **les tests réalisés à partir de données d'une moindre qualité font apparaître des taux d'erreur plus importants.**

Premièrement, **l'effet du vieillissement** est relativement modeste dans le cas des algorithmes d'identification, avec des taux de faux négatifs qui demeurent inférieurs ou proches de 0,5 % pour les 100 premiers d'entre eux lorsqu'il existe une différence d'au moins douze années entre les deux images comparées. En revanche, seule une poignée d'algorithmes d'identification arrive à maintenir des taux de faux négatifs inférieurs à 1 % dans cette configuration.

Deuxièmement, l'usage de ces algorithmes sur des **photos réalisées « *sans coopération* »** du sujet, en l'espèce à partir de caméras situées en surplomb de kiosques d'enregistrement administratifs (angle de prise de vue inadapté et basse résolution) aboutit à des taux d'erreurs relativement importants, de l'ordre de 4,61 % en authentification et de 6,68 % en identification pour les mieux classés.

Troisièmement, la comparaison à des fins d'identification de **photos de faible résolution**, réalisées par l'intermédiaire d'une webcam, multiplie, à taille de base de données égale, par près de 6,8 le taux de faux négatifs. Quant aux **images de profil**, le NIST relève certes de très forts progrès dans

[1] *Patrick Grother, Mei Ngan, Kayee Hanaoka, NIST - Face Recognition Vendor Test, Part 2: Identification (NISTIR 8271 Draft Supplement), 30 mars 2022.*

ce domaine, mais les trois meilleurs algorithmes génèrent des taux de faux positifs proches ou supérieurs à 1 pour 10.

**Taux de faux négatifs des algorithmes évalués par le NIST à partir d'images dégradées**

| | | Authentification (a) | | Identification (b) | | | |
|---|---|---|---|---|---|---|---|
| | | *Kiosque (c)* | *Temps (d)* | *Webcam (e)* | *Profil (f)* | *Kiosque (c)* | *Temps (d)* |
| **Classement de l'algorithme** | ***1*** | 4,61 % | 0,20 % | 0,82 % | 8,95 % | 6,68 % | 0,49 % |
| | ***2*** | 4,75 % | 0,21 % | 0,89 % | 11,02 % | 6,72 % | 0,59 % |
| | ***3*** | 4,77 % | | 1,01 % | 11,64 % | 6,73 % | 0,70 % |
| | ***10*** | 5,37 % | 0,25 % | 1,16 % | 18,90 % | 8,60 % | 1,30 % |
| | ***25*** | 6,50 % | 0,28 % | 1,99 % | 39,35 % | 11,20 % | 3,72 % |
| | ***50*** | 7,51 % | 0,38 % | 3,32 % | 69,89 % | 15,84 % | 11,07 % |
| | ***100*** | 11,42 % | 0,53 % | 6,15 % | 97,52 % | 28,24 % | 28,86 % |

*Source : Commission des lois du Sénat, à partir des données publiées par le NIST en mars 2022.*
*(a) Avec un seuil de tolérance aux faux positifs fixé à 1 pour 100 000.*
*(b) Avec un seuil de tolérance aux faux positifs fixé à 3 pour 1 000.*
*(c) Base de données de 1 600 000 photos prises au-dessus d'un kiosque d'enregistrement aux services de l'immigration et sans coopération de l'usager (regard non dirigé vers la caméra, prise de vue en hauteur, personnes grandes ou petites pouvant être coupées et présence potentielle d'autres personnes en arrière-plan).*
*(d) Comparaison avec une ou des photos prises au moins douze années après l'enrôlement.*
*(e) Base de données de 1 600 000 photos prises à partir d'une webcam et de qualité réduite.*
*(f) Base de données de 1 600 000 photos de profil (angle : 90°).*

**Les usagers de la reconnaissance faciale entendus au cours des travaux ont mis en avant les difficultés engendrées par cette moindre efficacité des algorithmes lorsqu'ils sont utilisés dans des conditions sous-optimales**. Dans le cadre de l'expérimentation d'un processus d'embarquement par reconnaissance biométrique à l'aéroport d'Orly, le groupe Aéroports de Paris doit par exemple mener une réflexion sur les conditions de prise d'image afin de maintenir un niveau de fiabilité satisfaisant du dispositif. Une telle expérimentation serait, par exemple plus difficile à mettre en œuvre sur la plateforme de Roissy, qui se caractérise par d'importantes surfaces vitrées, et engendrant une forte luminosité qui pourrait affecter la qualité de la prise d'image. **La question de la fiabilité des algorithmes ne peut donc être déliée de celle de leurs conditions opérationnelles d'emploi**.

**La reconnaissance faciale à l'épreuve du port du masque**[1]

Dans le contexte de la pandémie de Covid-19 et de généralisation du port du masque, le NIST a publié une étude visant à évaluer l'efficacité des algorithmes d'authentification lorsqu'ils sont utilisés sur des sujets masqués, dont 70 % du visage est couvert (à partir d'images prises lors du passage de la frontière et de qualité intermédiaire) :

- **effet sur les faux négatifs** : le port du masque se traduit par un surcroît de faux négatifs, qui se porte à 1 ou 2 % dans le meilleur des cas, mais peut atteindre 10 à 40 % pour des algorithmes au niveau de performance très élevé en conditions normales[2]. Cet effet est toutefois moins marqué lorsque le sujet porte un masque sur les deux photos comparées ;

- **effet sur les faux positifs** : ici, le taux d'erreur est en général réduit lorsque l'on compare une photo d'enrôlement sans masque à une photo réalisée avec masque. En revanche, lorsque les deux sujets sont masqués, le taux de faux positif peut être 10 à 100 fois supérieur au précédent cas de figure ou aux situations où les deux sujets sont démasqués. Un nombre très réduit d'algorithmes démontrent toutefois une meilleure tolérance à ces variables.

*Source : Commission des lois du Sénat*

*c) La question des « biais » des algorithmes : des différentiels de performance avérés sur certaines catégories de population, qui tendent toutefois à se réduire*

(1) Des différentiels de performance établis de longue date selon le sexe, l'âge et la couleur de peau

**La question des « *biais* » des algorithmes**, c'est-à-dire l'existence d'un différentiel de performance lorsqu'ils sont utilisés sur des catégories de population présentant des caractéristiques particulières, **représente une source de préoccupation majeure pour l'ensemble de l'écosystème de la reconnaissance faciale, ainsi que pour l'opinion publique**. En effet, l'usage d'algorithmes biaisés aggraverait significativement le risque d'atteinte au principe de non-discrimination.

La publication en 2018 d'une étude relative aux biais de plusieurs algorithmes de « *classification du genre* »[3] disponibles sur le marché a notamment contribué au mouvement évoqué précédemment de renonciation à la reconnaissance faciale par certaines villes américaines[4]. En dépit de

[1] *Mei Ngan, Patrick Grother, Kayee Hanaoka, NIST - Ongoing Face Recognition Vendor Test, Part 6B: Face recognition accuracy with face masks using post-Covid-10 algorithms (NISTIR 8331 Draft Supplement), 20 janvier 2022.*

[2] *Taux de faux négatif inférieur à 1 %.*

[3] *Buolamwini, J., & Gebru, T. (2018, January). Gender shades: Intersectional accuracy disparities in commercial gender classification. In* Conference on fairness, accountability and transparency *(pp. 77-91).*

[4] *Voir le I- B- 3. de la première partie du rapport.*

performances générales satisfaisante de ces algorithmes, des taux d'erreur substantiellement plus importants étaient relevés pour :

**- les femmes** : avec un surplus d'erreurs de l'ordre de 8,1 % à 20,6 % ;

**- les personnes à la couleur de peau foncée** : avec un différentiel compris entre 11,8 % et 19,2 %.

Ce déficit de fiabilité était décuplé lorsque l'on croisait ces populations, avec des écarts de performance pouvant aller jusqu'à 34,7 % dans le cas des femmes à la couleur de peau foncée. Ces différences s'expliquaient notamment par **une surreprésentation des personnes à la peau claire dans la base de données de référence**.

Dans ce contexte, le NIST a engagé des tests visant à évaluer l'effet des variables démographiques sur la performance des algorithmes. Dans un rapport publié en 2019, l'agence rapportait « *avoir trouvé des preuves empiriques démontrant l'existence de différentiels de performance selon une variable démographique dans la majorité des algorithmes de reconnaissance faciale* [qu'elle] *a évalué* »[1]. Plus précisément, les écarts de faux positifs étaient, pour les algorithmes d'authentification, substantiellement supérieurs (parfois 10 à 100 fois) à ceux de faux négatifs (en général très inférieurs à 3). Ces différences variaient toutefois significativement d'un algorithme à l'autre, les plus performants d'entre eux présentant un nombre limité d'erreurs. S'agissant des populations concernées :

**- pour les faux négatifs** : sur des images d'identité domestiques, l'efficacité de l'algorithme était diminuée pour les personnes d'origine asiatique ou amérindienne. Une performance généralement moindre sur les femmes et les personnes jeunes était également relevée, avec toutefois de nombreuses exceptions empêchant de conclure à la présence systématique de biais ;

**- pour les faux positifs** : ils étaient entre 2 et 5 fois plus fréquents chez les femmes et selon l'origine ethnique, chez les personnes originaire d'Asie ou d'Afrique de l'Est et de l'Ouest. S'agissant de l'âge, un surcroît de faux positifs était constaté aux deux extrémités de la pyramide des âges.

Il est en outre précisé que les « *différentiels de performance en fonction de l'origine démographique décelés dans les algorithmes d'authentification sont en général mais pas toujours présents dans les algorithmes d'identification* **»**.[2]

---

[1] *Mei Ngan, Patrick Grother, Kayee Hanaoka, NIST - Face Recognition Vendor Test, Part 3 : Demographic Effects (NISTIR 8280), 19 décembre 2019. En anglais dans le texte :* « We found empirical evidence for the existence of demographic differentials in the majority of contemporary face recognition algorithms that we evaluated ».

[2] *En anglais dans le texte : "We note that demographic differentials present in one-to-one verification algorithms are usually, but not always, present in one-to-many search algorithms".*

**L'existence de biais est ainsi largement documentée**, ainsi qu'ont pu le confirmer les travaux des rapporteurs. Dans les contributions écrites qu'elles ont transmises aux rapporteurs, les entreprises Microsoft et IBM partagent ce constat, en estimant respectivement que « ***les risques de biais et de discrimination sont réels*** » et « [qu'il] ***ne fait aucun doute que les préjugés humains peuvent influencer les algorithmes et entraîner des résultats discriminatoires*** ».

(2) Des biais en diminution et qui peuvent dans une certaine mesure être contenus

Pour autant, la question des différentiels de performance des algorithmes doit être abordée avec du recul. Depuis la publication des études précitées, les performances générales des algorithmes ont, d'une part, continué à augmenter rapidement, réduisant mécaniquement les écarts observés en fonction de groupes de population. D'autre part, **il existe des moyens de prévenir ou de corriger d'éventuels biais.**

**La constitution de bases de données plus diversifiées paraît en tout état de cause être la clef pour rendre les algorithmes plus équitables.** À titre d'exemple, le NIST mentionnait en 2019 le cas d'algorithmes développés en Chine qui produisaient des taux de faux positifs faibles sur les personnes originaires d'Asie de l'Est, parfois inférieurs à ceux observés pour les personnes caucasiennes. Cela semble accréditer l'idée qu'**une base de données cohérente avec la composition de la population locale est de nature à réduire les différentiels de performance**. Le NIST relève également que, dans certains cas, la réalisation d'un second essai peut permettre de corriger les faux négatifs.

Enfin, le NIST souligne que, pour **certains des algorithmes d'identification les mieux classés, aucun différentiel de performance ne peut être décelé**. Parmi ceux-ci figurent des algorithmes produits par la société Idemia, dont les représentants ont confirmé au cours de leur audition être désormais confrontés à la problématique des biais dans le seul champ de l'authentification.

### *B. POUR PALLIER CES RISQUES POUR LES LIBERTÉS PUBLIQUES, L'INDISPENSABLE PROTECTION DE NOTRE SOUVERAINETÉ TECHNOLOGIQUE*

#### 1. Deux prérequis pour assurer la sauvegarde des libertés publiques : la traçabilité et la sécurisation des données utilisées

S'agissant de la reconnaissance faciale, **les questions de la protection de la souveraineté technologique de la France et de la sauvegarde des libertés publiques ne sont en aucun cas déconnectées**. En présence d'une technologie potentiellement très intrusive et dont le fonctionnement repose sur l'utilisation de données biométriques sensibles,

**l'autonomie technologique est un instrument essentiel pour garantir un usage de la reconnaissance faciale respectueux des libertés**. S'il ne fait pas disparaître les risques pour les libertés publiques, l'usage d'un algorithme dont les données qui ont servi à son apprentissage sont traçables et les modalités ainsi que le lieu de stockage des données des utilisateurs connues permet, *a minima*, de les limiter substantiellement.

Dans ce contexte, les rapporteurs considèrent **que la protection de notre souveraineté technologique dans le domaine de la reconnaissance faciale, et plus largement des techniques de reconnaissance biométriques, représente une garantie indispensable pour la sauvegarde des libertés publiques**. Ils entendent insister tout particulièrement sur trois points :

**- la traçabilité des données d'apprentissage :** l'entraînement des algorithmes suppose, pour atteindre un niveau de performance satisfaisant selon les standards internationaux, d'avoir accès à des bases de données de masse dont la constitution est, pour des raisons légitimes, strictement encadrée par le RGPD en Europe. Dans ce contexte, le procédé le plus simple pour les développeurs de rang mondial est d'entraîner les algorithmes au sein de filiales à l'étranger sur des bases de données agrégées localement, où les garanties prévues par le RGPD ne s'appliquent pas. Ces procédés sont manifestement insatisfaisants en termes de libertés publiques ;

**- la maîtrise des modalités de stockage des données des usagers :** lesdites données peuvent être stockées sur une base de données centralisée, physiquement à l'intérieur ou à l'extérieur du site où le traitement est effectué, ou être stocké sur un support conservé par l'usager (technologie du *match on card*). Ces procédés sont plus ou moins attentatoires aux libertés :

* *la conservation de la donnée par l'usager :* la recommandation constante de la CNIL est de privilégier autant que possible cette modalité de stockage, grâce à laquelle l'usager ne perd jamais le contrôle de sa donnée et décide seul d'en faire ou non usage ;

* *la base de données centralisée :* cette solution est moins satisfaisante mais la CNIL l'a néanmoins accepté dans le cadre de l'expérimentation d'embarquement par biométrie menée par Aéroports de Paris (ADP), et ce en raison du « *caractère local de la base de données (en aéroport) et* [du] *caractère provisoire du stockage des gabarits (jusqu'au décollage de l'avion)* »[1]. En revanche, le stockage des données sur une base centralisée située à l'extérieur du site de traitement suscite plus de réserves ;

* *la base de données décentralisée :* il s'agit de la solution la moins satisfaisante, dans la mesure où il est plus complexe pour les usagers de retracer leurs données et d'en recouvrer la maîtrise. À titre d'exemple, le groupe ADP a indiqué que des expérimentations d'embarquement par biométrie étaient également menées par « *StarAlliance* » à Francfort et

[1] *Support de présentation de la société Aéroports de Paris (déplacement de la mission d'information du 21 février 2022).*

Munich, avec un stockage des données des passagers sur le *cloud* de Microsoft, ce qui est, de l'opinion des rapporteurs, tout à fait insatisfaisant ;

**- la sécurisation des structures d'hébergement des données des usagers :** lorsque les données sont stockées sur des bases, il est impératif de pouvoir en garantir la sécurisation contre les attaques informatiques. Les conséquences pour les libertés d'une fuite de données pourraient en effet s'avérer désastreuse si celle-ci concernait des gabarits biométriques.

### 2. Des entraves significatives à la recherche et au développement qui font peser le risque, à terme, d'une perte de souveraineté technologique

Si la France dispose **d'un écosystème de recherche et de développement de pointe** dans le domaine de la reconnaissance faciale, force est de constater que les acteurs du secteur évoluent dans **un cadre juridique, administratif et matériel peu propice au lancement de projets d'innovation ambitieux**. Ce constat est particulièrement prégnant dans le secteur de la recherche publique, dont les difficultés accrue d'accès à la donnée en entravent significativement le développement. Loin de se cantonner au champ économique, les conséquences de ces multiples obstacles à la recherche et au développement concernent également au premier chef les libertés publiques.

De fait, **dans un contexte de forte concurrence internationale, l'hypothèse d'une perte progressive de souveraineté technologique ne saurait être minorée**, au risque de voir la reconnaissance faciale poursuivre son développement en France à partir d'algorithmes développés à l'étranger, dans des conditions plus ou moins opaques. **La protection d'un écosystème de recherche et de développement national, à la fois performant et respectueux des garanties fixées par le RGPD, revêt donc un caractère prioritaire aux yeux des rapporteurs.**

*a) Un écosystème de recherche et de développement performant*

**Le tissu de recherche et de développement français dans le secteur des technologies biométriques** en général et de la reconnaissance faciale en particulier est particulièrement riche en France. Comme le souligne l'Alliance pour la confiance numérique, « *l'écosystème français de l'identité numérique et plus spécialement de la reconnaissance faciale est extrêmement riche et diversifié. Il se compose aussi bien de grands groupes leaders mondiaux, que d'ETI, de PME ou de start-up extrêmement dynamiques et innovantes* »[1].

[1] *Réponses de l'Alliance pour la confiance numérique au questionnaire des rapporteurs.*

**Deux des trois entreprises de rang mondial de la reconnaissance faciale sont implantés en France : Idemia et Thalès**[1]. À titre d'illustration, la première indique vendre les technologies de sécurité et d'identité biométrique et numérique qu'elle développe à des acteurs publics et privés de plus de 180 pays du monde, posséder plus de 1 500 familles de brevets actives et déposer annuellement 50 brevets en France[2]. Dans le champ de la reconnaissance faciale, les algorithmes qu'elle produit se placent régulièrement dans le haut des classements publiés par le NIST. L'algorithme d'identification « *Idemia_009* » est, par exemple, le troisième le plus performant sur une base de données de 12 millions de photos d'identités, avec un taux de faux négatif de 0,21 %[3]. S'agissant de l'entreprise Thalès, celle-ci a indiqué lors d'un déplacement d'une délégation de la mission d'information sur l'un de ses sites de recherches, contribuer à plus de **300 programmes gouvernementaux dans le champ des techniques biométriques**. Par exemple, des technologies développées par l'entreprise sont utilisées dans le cadre de l'émission des nouveaux passeports britanniques mis en circulation après le Brexit.

**L'écosystème français de la reconnaissance faciale ne se limite néanmoins pas à ces deux entreprises**. Des entreprises de taille intermédiaire sont également bien implantées sur le marché. C'est le cas d'ID3 Technologies, entreprise grenobloise qui revendique une approche « *citoyenne* » de la reconnaissance faciale, par le développement de systèmes peu onéreux, nécessitant une faible puissance de calcul algorithmique et où les données sont hébergées sous un format « *match on card* ». Très présente à l'international, cette entreprise dispose d'une branche à Bogota et a, par exemple, développé les systèmes biométriques utilisés dans les passeports du Mali.

Illustration de cette bonne santé du secteur industriel de l'identité biométrique en France, l'Alliance pour la confiance numérique estimait en 2020 que le segment « "***identification et authentification des personnes" générait un chiffre d'affaires annuel de 1,76 milliard d'euros et représentait un volume de 8 500 emplois répartis dans 490 entreprise***s »[4].

**Si ces projets sont rares, certains organismes de la recherche publique mènent également des travaux relatifs à la reconnaissance faciale**. C'est notamment le cas de l'Institut national de recherche en informatique et en automatique (INRIA) avec le projet « STARS » (« *Spatio-Temporal Activity Recognition System* ») basé au centre de recherche INRIA Sophia Antipolis - Méditerranée, où les rapporteurs se sont rendus.

---

[1] *Le troisième étant l'entreprise NEC, selon les analyses présentées par l'entreprise Thalès lors du déplacement d'une délégation de la commission des lois sur son site de Meudon le 23 avril 2022.*
[2] *Contribution écrite d'Idemia.*
[3] *Données accessibles sur le site du NIST et accessibles à cette adresse : https://pages.nist.gov/frvt/html/frvt1N.html.*
[4] *Réponses de l'Alliance pour la confiance numérique au questionnaire des rapporteurs.*

*b) Des obstacles juridiques, administratifs et matériels néanmoins importants à la recherche et au développement qui alimentent un risque de perte de souveraineté technologique*

Les acteurs de la recherche et du développement dans le domaine de la reconnaissance faciale sont confrontés, dans des proportions variables, à **trois catégories principales de difficultés**.

Premièrement, les incertitudes tenant aux évolutions à venir du cadre juridique sont peu propices au lancement de projets de recherche et de développement. Les acteurs du secteur **accueillent plutôt favorablement le projet de législation européenne sur l'intelligence artificielle, en ce qu'il permettra de stabiliser le cadre juridique applicable à la recherche et au développement.** Dans l'attente, les auditions conduites par les rapporteurs ont fait ressortir un risque de ralentissement de la recherche et du développement, les acteurs étant réticents à s'engager dans des projets d'ampleur sans savoir dans quelle mesure ceux-ci seront impactés par l'entrée en vigueur du futur règlement européen sur l'intelligence artificielle.

La deuxième difficulté réside dans le **caractère particulièrement restrictif et touffu du cadre juridique actuel** s'agissant de la conduite d'activités de recherche scientifique à partir de données sensibles. Si le traitement de ces données est en principe interdit, la CNIL liste quatre exceptions pouvant être mobilisées à des fins de recherche lorsque[1] :

**- la personne concernée a donné son consentement** libre, spécifique, éclairé et univoque à l'utilisation de ses données à caractère personnel ;

**- les données utilisées ont manifestement et délibérément été rendues publiques par leur propriétaire** : ce critère est toutefois délicat à évaluer, notamment en ce qui concerne les données publiées sur les réseaux sociaux, où il est par exemple recommandé de prendre en compte l'accessibilité de la page où les données ont été publiées ;

**- la recherche est nécessaire pour des motifs d'intérêt public important**, sous réserve d'un texte l'autorisant, en général un décret en Conseil d'État pris après avis de la CNIL ;

**- l'utilisation des données est nécessaire à la recherche publique** : ce qui suppose un avis de la CNIL établissant la présence de « *motifs d'intérêt publics importants* » justifiant cette nécessité.

Ce cadre limite fortement les possibilités juridiques de recherche et de développement en matière de reconnaissance faciale, en particulier s'agissant du secteur privé. Sa complexité nuit par ailleurs à la lisibilité d'ensemble et certains acteurs ont, au cours des auditions, expliqué être parfois confrontés à une **certaine confusion pour déterminer ce qui est ou non autorisé**.

---

[1] *Notice consultable sur le site internet de la CNIL : https://www.cnil.fr/fr/recherche-scientifique-hors-sante/focus-certaines-categories-donnees-personnelles.*

**Le troisième écueil est celui de l'accès aux données**. L'obligation de recueillir le consentement de chaque personne pour chaque projet de recherche représente en effet un obstacle de taille à la constitution des bases de données nécessaires à l'entraînement des algorithmes. Si les entreprises privées de rang mondial peuvent le surmonter dans une certaine mesure en raison des importants moyens humains dont elles disposent et de la possibilité de s'appuyer sur des filiales à l'étranger, **cet obstacle est quasiment insurmontable en matière de recherche publique**, ainsi que l'ont souligné les membres de l'équipe « *STARS* » précitée rencontrés par les rapporteurs sur le site de Sophia-Antipolis.

Dans ce contexte, le risque que cet écosystème de recherche et de développement performant se voit dépassé par la concurrence venue de l'étranger ne doit pas être sous-estimé. **Compte tenu de l'imbrication forte des enjeux de souveraineté technologique et de sauvegarde des libertés publiques, les rapporteurs considèrent ainsi comme essentiel de définir un cadre juridique adapté et spécifique à la recherche.**

# DEUXIÈME PARTIE
# ÉCARTER LE RISQUE D'UNE SOCIÉTÉ DE SURVEILLANCE EN EXPÉRIMENTANT AU CAS PAR CAS

Au cours de leurs travaux sur la reconnaissance faciale, il est rapidement apparu opportun aux rapporteurs de ne pas cantonner leurs recommandations aux techniques biométriques qui utilisent le visage pour identifier de manière unique une personne, mais de **faire rentrer dans leur champ l'ensemble des techniques biométriques**. En effet, les avancées de la recherche rendront sans doute possible à l'avenir la collecte d'autres traits physiologiques (iris, voix, démarche, *etc.*) dans l'espace public. Par ailleurs, la demande toujours plus accrue de sécurité conduit les développeurs à proposer des solutions combinant plusieurs types de données biométriques (visage et empreinte digitale par exemple).

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

Ainsi que l'a appelé de ses vœux la CNIL dans son rapport de 2019[1], il convient de **fixer les 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[2]. Dans le même temps, il semble également nécessaire de déterminer une méthodologie et un cadre de contrôle et de redevabilité de la mise en œuvre de la technologie.

Il est en effet important que la manière de réguler une technique susceptible d'apporter des changements profonds à la société française soit **fixée de manière collective**, à l'issue d'un débat parlementaire. La pratique actuelle qui laisse la main à la CNIL – qui n'est pourtant ni décideur ni prescripteur comme elle le rappelle elle-même – voire, aux acteurs privés, dont les chartes d'éthique relèvent de considérations liées à leur image et à leur réputation, n'est pas à la hauteur des enjeux.

---

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

[2] *Voir en particulier, l'interdiction du clonage en matière de recherche sur les embryons humains.*

### *A. DES LIGNES ROUGES QUI ÉCARTENT LE RISQUE D'UNE SOCIÉTÉ DE SURVEILLANCE*

L'article 1er de la loi du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés* dispose que « *l'informatique doit être au service de chaque citoyen. [...] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ». De même le RGPD pose-t-il les principes généraux en matière de traitement des données personnelles (licéité, loyauté, transparence ; limitation des finalités ; minimisation des données ; intégrité et confidentialité...).

Toutefois, compte tenu du caractère intrusif des techniques de reconnaissance biométrique, en particulier celles qui utilisent le visage qui est aisément captable dans l'espace public, il est nécessaire de compléter ces règles générales avec des **dispositions spécifiques en la matière** pour poser de manière claire et accessible des lignes rouges et fixer un cadre tant aux industriels qu'aux pouvoirs publics et ainsi répondre aux légitimes inquiétudes des citoyens.

De nombreux organismes y ont déjà réfléchi en matière d'intelligence artificielle : dans le cadre européen, le Comité européen de la protection des données (European data protection board – EDPB – regroupant l'ensemble des CNIL européennes) et le Contrôleur européen de la protection des données (CEPD)[1] ou le Comité de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108)[2] ; au niveau français, le Comité national pilote d'éthique du numérique (CNPEN) ou la Commission nationale consultative des droits de l'homme (CNCDH).

Certaines de leurs préconisations ont été reprises par la Commission européenne dans sa proposition de règlement sur l'intelligence artificielle. Elles peuvent être transposables en matière de reconnaissance biométrique.

Mériteraient ainsi de figurer parmi les lignes rouges :

- l'interdiction de l'utilisation des technologies de reconnaissance biométrique **à des finalités de notation sociale**, définie par la Commission européenne comme « *évaluant 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* ». Cette interdiction devrait selon les rapporteurs concerner **tant les autorités publiques que les entreprises privées**. Cette extension aux entreprises privées n'est pas pour l'heure prévue par le projet européen de règlement IA, mais est souhaitée

[1] *Avis conjoint 05/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle).*

[2] *Lignes directrices sur l'intelligence artificielle et la protection des données adoptées par le Comité de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (Convention 108) le 25 janvier 2019.*

par l'EDPB et le CEPD. Il semble en effet nécessaire de **protéger les consommateurs de méthodes intrusives** et d'empêcher le recours à la notation sociale par surveillance des comportements dans les espaces de vente, de restauration ou les centres de loisirs ;

- l'interdiction de l'utilisation de la technologie de reconnaissance biométrique **aux fins de catégoriser les individus en fonction de l'origine ethnique, du sexe, ainsi que de l'orientation politique ou sexuelle**, ou tout autre motif de discrimination au sens de l'article 225-1 du code pénal. Une exception dans le cadre de la recherche scientifique et sous réserve de garanties appropriées pourrait être envisagée pour ne pas bloquer les travaux universitaires qui reposent sur de telles catégorisations (par exemple en sociologie) ;

- l'interdiction de l'utilisation de la technologie de reconnaissance biométrique pour **déduire les émotions d'une personne physique**. Le Comité de la Convention 108 cible en particulier les systèmes qui seraient utilisés à des fins de recrutement professionnel, d'accès aux assurances ou en matière d'éducation. Pourraient en revanche être acceptées des **utilisations à des fins de santé ou de recherche scientifique** et une fois encore, sous réserve de garanties appropriées. Il convient en effet de favoriser les recherches faites par exemple par les équipes de l'INRIA de Sophia-Antipolis pour évaluer et stimuler des patients atteints de troubles neurocognitifs, dans le cadre du projet STARS, conduit en coopération avec le CHU de Nice. Cette recherche va dans le sens de l'exception souhaitée par la CNCDH qui préconise d'admettre « *par exception leur utilisation dès lors qu'elles visent à renforcer l'autonomie des personnes, ou plus largement l'effectivité de leurs droits fondamentaux* »[1].

**<u>Proposition n° 2 :</u> 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.**

[1] « Intelligence artificielle et droits humains : Pour l'élaboration d'un cadre juridique ambitieux », *Commission nationale consultative des droits de l'homme, 7 avril 2022.*

Une autre ligne rouge doit concerner plus spécifiquement la reconnaissance faciale mise en œuvre dans le cadre d'un **système d'identification à distance en temps réel dans les espaces accessibles au public**, que tout le monde s'accorde à reconnaitre comme présentant les risques plus élevés au regard des libertés publiques.

Dans leur avis commun, l'EDPB et le CEPD se sont prononcés pour **l'interdiction totale de toute forme d'identification biométrique à distance en temps réel dans l'espace public**[1]. En parallèle, le Parlement européen a, dans l'attente de la future législation européenne, demandé un **moratoire sur le déploiement de systèmes de reconnaissance faciale à des fins répressives destinés à l'identification**[2], à moins qu'ils ne soient utilisés qu'aux fins de l'identification des victimes de la criminalité.

Le Défenseur des droits préconise d'étendre l'interdiction explicite de recours à l'utilisation de logiciels de reconnaissance faciale appliquée aux images captées par drones aux autres dispositifs de surveillance existants[3]. Cette position est partagée par les associations de défense des droits sur internet et le Conseil national des barreaux qui ont été entendus par les rapporteurs.

La Commission nationale consultative des droits de l'homme (CNCDH) recommande également l'interdiction de l'identification biométrique à distance des personnes dans l'espace public et les lieux accessibles au public, en raison des risques d'atteinte grave aux droits et libertés fondamentaux liés à une remise en cause, réelle ou supposée, de l'anonymat dans l'espace public[4]. À titre d'exception, elle admet toutefois la possibilité d'envisager son utilisation, dès lors que celle-ci serait strictement nécessaire, adaptée et proportionnée pour la prévention d'une menace grave et imminente pour la vie ou la sécurité des personnes et celle des ouvrages, installations et établissements d'importance vitale.

À l'instar de la Commission européenne qui l'a classé parmi les pratiques interdites en matière d'intelligence artificielle[5], les rapporteurs considèrent qu'il convient de **poser une interdiction de principe** et de ne permettre qu'à titre très exceptionnel leurs recours par les forces de sécurité intérieure en cas de menace grave ou pour les besoins d'une enquête judiciaire sur une infraction grave. Dans ce cadre, il semble impératif

---

[1] *Avis conjoint 05/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle).*

[2] *Résolution du Parlement européen du 6 octobre 2021 sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales (2020/2016(INI)).*

[3] *Rapport* « Technologies biométriques : l'impératif respect des droits fondamentaux », *Défenseur des droits, juillet 2021.*

[4] *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, 7 avril 2022.*

[5] *Article 5 de la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union (COM/2021/206 final).*

**d'exclure clairement tout recours à cette technique lors de manifestations sur la voie publique et aux abords des lieux de culte** afin que les citoyens de se sentent pas empêchés d'exercer leur droit de manifester ou de pratiquer leur religion par une crainte de la levée de leur anonymat.

> **Proposition n° 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.**

Au-delà des interdictions et toujours dans la perspective de fixer un cadre clair et compréhensible pour tous, il est également nécessaire de fixer quelques obligations positives et en particulier, **poser le principe de subsidiarité du recours à la reconnaissance faciale**. Cet impératif a été relevé par la CNIL dans son avis de 2019 : « *la reconnaissance faciale ne peut légalement être utilisée, même à titre expérimental, si elle ne repose pas sur un impératif particulier d'assurer un* ***haut niveau de fiabilité de l'authentification ou de l'identification*** *des personnes concernées et sans démonstration de l'inadéquation d'autres moyens de sécurisation* ***moins intrusifs*** ».

> **Proposition n° 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.**

De la même manière, les rapporteurs souhaitent que le **contrôle humain** soit inscrit parmi les lignes rouges de la reconnaissance biométrique. Comme l'a relevé le CNPEN, « *cette idée d'une* ***Garantie Humaine de l'IA*** *est issue d'un mouvement de propositions académiques, citoyennes mais aussi de professionnels de santé. Ce principe a été reconnu dans les avis 129 et 130 du CCNE et dans l'article 11 du projet de loi bioéthique en cours d'examen devant le Parlement français*[1]*. Cette notion a également été portée dans le cadre des travaux en cours de la* task-force *sur la régulation de l'IA dans le cadre de l'Organisation Mondiale de la Santé. Le concept de "Garantie Humaine" peut paraître abstrait mais il est, en réalité, très opérationnel. Dans le cas de l'IA, l'idée est d'appliquer les principes de régulation de l'intelligence artificielle* ***en amont et en aval de l'algorithme lui-même en établissant des points de supervision humaine****.*

[1] *Devenu article 17 de la loi n° 2021-1017 du 2 août 2021* relative à la bioéthique.

***Non pas à chaque étape, sinon l'innovation serait bloquée****. Mais sur des points critiques identifiés dans un dialogue partagé entre les professionnels, les patients et les concepteurs d'innovation »*[1].

Le RGPD a consacré, en son article 22, le droit « *de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire »*[2].

> **Proposition n° 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.**

Le RGPD pose également le **principe de transparence** qui doit être assuré en toutes circonstances, par la fourniture **d'informations claires, compréhensibles et aisément accessibles aux personnes dont les données font l'objet d'un traitement**. S'agissant des algorithmes, le code des relations entre le public et l'administration transpose ce principe en prévoyant qu'en cas de décision administrative prise par un algorithme à propos d'un individu, ce dernier doit en être informé et pouvoir accéder, à sa demande, aux « *règles définissant ce traitement ainsi que les principes caractéristiques de sa mise en œuvre* », sauf lorsque l'algorithme est utilisé dans le cadre d'une finalité relevant de la sûreté de l'État, de la sécurité publique, de la sécurité des personnes ou de recherche et de prévention d'infractions de toute nature.

Une telle transparence doit également être assurée en matière de reconnaissance biométrique **qui ne doit pas être déployée à l'insu des citoyens**.

> **Proposition n° 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.**

---

[1] *Consultation sur le Livre blanc sur l'intelligence artificielle* - Une approche européenne Contribution du Comité National Pilote d'Éthique du Numérique *(CNPEN, France).*

[2] *Droit soumis à exceptions : lorsque la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ; lorsqu'elle est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée; ou lorsqu'elle est fondée sur le consentement explicite de la personne concernée.*

### *B. UNE MÉTHODOLOGIE CLAIRE : LA VOIE EXPÉRIMENTALE DANS LE CADRE D'UNE LOI*

Selon l'universitaire Caroline Lequesne-Roth que les rapporteurs ont entendue, « *la protection des libertés publiques, en jeu dans le cadre de la mobilisation des outils de reconnaissance faciale, impose une* ***intervention du législateur****. L'exhaustivité (concernant notamment la finalité des usages et l'ouverture de recours) et la spécificité des garanties apportées conditionneront d'ailleurs la constitutionnalité du régime établi. Tel est également le sens de la jurisprudence européenne* »[1].

Les rapporteurs sont favorables à l'élaboration d'une loi d'expérimentation permettant de créer le débat et de déterminer quels usages de la reconnaissance faciale sont pertinents avant de **pérenniser, par une seconde loi, ceux d'entre eux qui le seraient.** Cette méthode en trois étapes – expérimentation, évaluation puis éventuelle pérennisation – permettrait de rentrer dans le vif du sujet sans s'en tenir aux positions de principe.

Il s'agirait ni plus ni moins que de **repenser le besoin au regard de la balance coûts/avantages**, sans céder à la course en avant que semble faire naître la masse des données à analyser, compte tenu d'un recours de plus en plus fréquent à la vidéoprotection.

**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 dans 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] *Réponses de Caroline Lequesne-Roth au questionnaire des rapporteurs.*

**Exemples de dispositions législatives adoptées à titre expérimental pour une durée limitée**

La technique permettant la mise en œuvre sur les réseaux des opérateurs de communications électroniques d'un algorithme identifiant les indices d'une menace terroriste a été adoptée à titre expérimental, jusqu'au 31 décembre 2018, par la loi n° 2015-912 du 24 juillet 2015 *relative au renseignement*[1], puis jusqu'au 30 juin 2021 par la loi du 24 décembre 2020[2].

La loi SILT du 30 octobre 2017[3] a permis à titre expérimental jusqu'au 31 décembre 2020[4], la mise en place d'un régime de contrôle administratif et de surveillance des personnes constituant une menace grave pour la sécurité et l'ordre publics (dont les mesures individuelles de contrôle administratif ou MICAS) et de visites domiciliaires et de saisies à des fins de prévention des actes de terrorisme (perquisitions administratives).

La technique permettant à l'administration fiscale et l'administration des douanes de collecter et exploiter au moyen de traitements informatisés et automatisés les contenus librement accessibles publiés sur Internet par les utilisateurs de plateformes en ligne afin de détecter les comportements frauduleux de contribuables a été autorisée à titre expérimental jusqu'au 30 décembre 2022 dans le cadre de la loi *de finances pour 2020*[5].

Enfin, plus récemment, l'interception des correspondances émises ou reçues par la voie satellitaire par les services spécialisés de renseignement a été adoptée à titre expérimental jusqu'au 31 juillet 2025 dans le cadre de la loi du 30 juillet 2021 *relative à la prévention d'actes de terrorisme et au renseignement*[6].

*Source : Commission des lois du Sénat*

L'expérimentation autorisée pendant une durée limitée obligerait le Gouvernement et le Parlement à réévaluer le besoin et recadrer éventuellement le dispositif en fonction des résultats obtenus. Philippe Bas, alors président de la commission des lois du Sénat, avait qualifié ce dispositif de **« clause d'autodestruction »** à propos des dispositions de la loi SILT dont les conséquences en termes de libertés publiques suscitaient aussi de nombreuses inquiétudes : « *une évaluation annuelle nous renseignera sur leur utilité marginale. S'il s'avère que ces mesures sont inutiles, le Parlement n'aura pas à les reconduire* ».

[1] *Loi n° 2015-912 du 24 juillet 2015* relative au renseignement.
[2] *Loi n° 2020-1671 du 24 décembre 2020* relative à la prorogation des chapitres VI à X du titre II du livre II et de l'article L. 851-3 du code de la sécurité intérieure.
[3] *Loi n° 2017-1510 du 30 octobre 2017* renforçant la sécurité intérieure et la lutte contre le terrorisme *(article 5)*.
[4] *Puis jusqu'au 30 juin 2021 par la loi n° 2020-1671 du 24 décembre 2020.*
[5] *Loi n° 2019-1479 du 28 décembre 2019* de finances pour 2020 *(article 154)*.
[6] *Loi n° 2021-998 du 30 juillet 2021* relative à la prévention d'actes de terrorisme et au renseignement *(article 13)*.

Une durée de trois ans semble une durée raisonnable pour tester et être en cohérence avec l'entrée en vigueur de la future législation européenne sur l'intelligence européenne.

> **Proposition n° 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.**

L'expérimentation envisagée par les rapporteurs doit être une **véritable expérimentation qui concerne non seulement la technologie, mais également le cadre juridique mis en place**. Il s'agirait d'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].

De ce fait, il est important de prévoir en même temps que l'expérimentation 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.**

Les rapporteurs souhaitent **qu'un seul comité procède à l'évaluation de l'ensemble des expérimentations** pour nourrir sa réflexion et bénéficier d'une vision globale.

Un tel comité existe par exemple depuis 2018 pour évaluer l'algorithme national Parcoursup[2]. Ce comité est composé de six membres,

---

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

[2] *Voir le XI. de l'article L. 612-3 du code de l'éducation créé par la loi n° 2018-166 du 8 mars 2018* relative à l'orientation et à la réussite des étudiants.

choisis au regard de leur expertise et de leur expérience, notamment dans les domaines des sciences humaines, sociales et éthiques, mais également en sciences informatiques et algorithmiques. Il est actuellement présidé par l'ancienne présidente de la CNIL et actuelle présidente de l'Autorité nationale des jeux, Isabelle Falque-Pierrotin.

Les expérimentations menées par la DGSI à des fins de renseignement seraient en revanche **exclues de ce dispositif d'évaluation publique**, mais soumises au contrôle de la Commission nationale de contrôle des techniques de renseignement (CNCTR) dans le cadre habituel applicable aux techniques de renseignement (DPR), ainsi qu'au contrôle de la délégation parlementaire au renseignement qui a pour mission de contrôler l'action du Gouvernement en matière de renseignement et d'évaluer la politique publique en ce domaine.

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

En accompagnement de cette phase d'expérimentation, il semble nécessaire de **favoriser le débat dans la société française** en informant les citoyens sur ce que sont les techniques de reconnaissance biométrique, les bénéfices attendus, en citant des exemples de situations concrètes, et les risques encourus, **afin que chacun puisse comprendre quels sont les choix à opérer collectivement, en mettant en balance les différents droits et libertés à protéger.** Il est important que les discussions sur la reconnaissance biométrique prennent en compte la complexité des enjeux et ne soient pas polarisées par le modèle chinois.

Cela permettrait également une réflexion sur les usages commerciaux de ces techniques qui se développent à bas bruit pour faciliter la vie quotidienne, en particulier chez les jeunes. Pour ces derniers, cette réflexion pourrait être menée dans le cadre de l'article L. 312-9 du code de l'éducation qui prévoit la dispense dans les établissements scolaires d'une « *formation à l'utilisation responsable des outils et des ressources numériques* ».

> **Proposition n° 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.**

### *C. CRÉER UN CADRE DE CONTRÔLE ET DE REDEVABILITÉ*

Le déploiement d'une technologie de reconnaissance biométrique devrait faire l'objet d'un contrôle *a priori* et *a posteriori*. Comme le souligne Caroline Lequesne-Roth, **il en va de « la démocratie technologique »** qui *« se construira ainsi par l'élaboration d'un régime de transparence et de redevabilité algorithmique forte. ( ...) Concernant la reconnaissance faciale, les autorisations préalables, le contrôle par des tiers des usages et les audits algorithmiques sont autant de composantes essentielles au respect des règles ».*

Il s'agit tout d'abord d'instaurer une **autorisation au cas par cas du déploiement de la technologie de reconnaissance biométrique.** La demande d'autorisation devrait comporter les informations nécessaires pour apprécier le bien-fondé de la demande. Comme en matière de déploiement de drones[1], il pourrait s'agir des informations suivantes : le service responsable des opérations ; la finalité poursuivie ; la justification de la nécessité de recourir au dispositif, permettant notamment d'apprécier la proportionnalité de son usage au regard de la finalité poursuivie ; les caractéristiques techniques du dispositif de reconnaissance faciale nécessaire à la poursuite de la finalité ; le cas échéant, les modalités d'information du public ; la durée souhaitée de l'autorisation ; le périmètre géographique concerné.

En cas d'utilisation par les forces de sécurité intérieure, il apparaît nécessaire de distinguer selon qu'il s'agit d'un cadre de police judiciaire ou de police administrative. Dans le cadre judiciaire, et conformément au droit de la procédure pénale, **le pouvoir d'autorisation pourrait être dévolu au magistrat**, juge d'instruction ou procureur de la République selon le cadre procédural dans lequel serait demandé l'acte. Dans le cadre préventif, l'autorisation de déploiement pourrait être délivrée par **le préfet,** comme en matière de drones. Le cadre actuel de l'article 90 de la loi du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés* serait maintenu : en sus de l'autorisation, le traitement devrait faire l'objet d'une analyse d'impact relative à la protection des données (AIPD) et être **adressée à la CNIL avec demande d'avis**.

Pour les acteurs privés, compte tenu de la particulière sensibilité des techniques de reconnaissance biométrique, il semble indispensable de **rétablir une autorisation préalable de la CNIL** si cette technique est destinée à être déployée dans un espace accessible au public, et de sortir ainsi de l'ambigüité actuelle qui les oblige à établir une analyse d'impact relative à la protection des données (AIPD), mais non à saisir la CNIL, contrairement aux pouvoirs publics.

Enfin, afin de conserver une vision globale des recours aux techniques de reconnaissance biométrique, quelle que soit l'autorité ayant

[1] *Article L. 242-5 du code de la sécurité intérieure.*

délivré l'autorisation, les rapporteurs préconisent **un recensement national de ces autorisations.**

> **Proposition n° 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.**
>
> **Proposition n° 11 : Soumettre le déploiement des technologies de reconnaissance biométrique par les acteurs privés dans les espaces accessibles au public à l'autorisation de la CNIL.**
>
> **Proposition n° 12 : Prévoir le recensement au niveau national des actes autorisant le déploiement des technologies de reconnaissance biométrique.**

Enfin, il convient de réaffirmer le rôle de la CNIL comme autorité de **contrôle *a posteriori* du bon usage des dispositifs de reconnaissance biométrique et des éventuels détournements de finalité en dehors du cadre défini**. Cette compétence générale suppose que des moyens humains, financiers et institutionnels adéquats lui soient accordés pour procéder aux contrôles nécessaires et, au besoin, imposer les correctifs, voire l'arrêt de dispositifs illégaux. Elle pourrait bénéficier dans cette tâche de l'appui technique du Pôle d'expertise de la régulation numérique (PEReN).

Une fois encore, en matière de renseignement, l'autorité de contrôle serait la CNCTR qui a pour mission de veiller à ce que les techniques de renseignement soient légalement mises en œuvre sur le territoire national.

> **Proposition n° 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

**On l'a vu, les cas d'usage de la reconnaissance faciale 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 ainsi être

opérées, les risques pour les libertés étant dans une large mesure conditionnées par celles-ci.

Il convient avant tout d'aborder **l'application de l'intelligence artificielle aux images sans utilisation de données biométriques**. Une distinction doit ensuite être réalisée, au sein des technologies recourant aux données biométriques, entre **authentification et identification**. Au sein de ces ensembles, et comme le souligne le professeur Caroline Lequesne-Roth, maître de conférences à l'Université Côte d'Azur, la différence de risque pour les libertés fondamentales se caractérise en termes de degré : une opération d'identification comporte un risque accru par rapport à une opération d'authentification, car la première implique la collecte et le traitement d'un très grand volume de données biométriques, dont certaines appartenant à des personnes n'étant pas concernées par les finalités du traitement. L'authentification permet quant à elle une correspondance ciblée entre les gabarits de personnes s'étant préalablement enregistrées dans le système.

Enfin, il convient d'aborder la différence entre **usage public et usage privé,** où la nature des risques diverge entre ceux que présente une surveillance publique et ceux qu'implique une surveillance privée.

### *A. DISTINGUER TECHNOLOGIES DE RECONNAISSANCE BIOMÉTRIQUE ET TECHNOLOGIES CONNEXES*

**La vidéoprotection**, autorisée par les dispositions législatives et règlementaires du code de la sécurité intérieure, **doit être distinguée de la vidéoprotection dite « intelligente », dans laquelle les images sont traitées par des logiciels d'intelligence artificielle.** Il convient cependant, au sein de cette seconde catégorie, de ne pas confondre la reconnaissance biométrique de personnes, à partir des caractéristiques de son visage par exemple, des autres techniques de traitements des images par intelligence artificielle n'utilisant pas de données biométriques.

**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.

Ces nouvelles technologies offrent des perspectives opérationnelles regardées de près par les forces de sécurité, qui estiment que, en matière de sécurité, **le traitement automatisé des images issues des systèmes de vidéoprotection permettrait de gagner un temps conséquent en autorisant les enquêteurs à se concentrer sur les séquences d'intérêt**.

**Dans la perspective des Jeux Olympiques de 2024** par exemple, où les tensions en matière de sécurité et de gestion de flux seront accrues, **les forces de sécurité intérieure estimeraient utiles de pouvoir, à partir des images issues des systèmes de vidéoprotection** :

- détecter des matériaux dangereux, interdits ou atypiques nécessitant une levée de doute sur leur nature et leur dangerosité ;

- détecter les changements de rythme ou de direction d'une foule, d'un groupe ou d'un individu au sein d'une foule, ou d'un véhicule ou d'un type de véhicule au sein d'une circulation ;

- mesurer les flux et la densité de personnes et de véhicules pour assurer le respect de la règlementation en matière de sécurité publique, civile ou sanitaire ;

- détecter certaines caractéristiques des personnes, comme par exemple le port de dispositifs occultant le visage d'un individu ou d'un groupe d'individus au sein d'une foule, pour permettre le suivi des personnes considérées comme de potentielles menaces[1].

Dans cette même perspective, la SNCF et la RATP souhaiteraient pouvoir mettre en place des systèmes permettant d'une part d'améliorer la sécurité des biens et des personnes, par exemple en détectant des comportements ou mouvements de foule anormaux, la présence d'objets délaissés potentiellement dangereux de personnes sur les voies, d'obstacles devant un bus ou de personne dans un angle mort et, d'autre part, d'améliorer la gestion des flux et la qualité de service des usages en mesurant l'affluence à bord des trains, en analysant les flux de voyageurs en gare, et en transmettant ces informations en temps réel aux voyageurs.

**À ce jour cependant, ni l'utilisation des techniques de reconnaissance biométrique ni celle des autres techniques de traitement des images ne sont prévues par la législation**.

**D'aucuns considèrent que les techniques de traitement des images ne concernant pas des données biométriques permettant l'authentification ou l'identification des personnes peuvent être déployées à cadre législatif constant**, dès lors que ces traitements s'inscrivent dans les mêmes finalités que celles attribuées aux systèmes de vidéoprotection.

L'article L. 252-1 du code de la sécurité intérieure prévoit en effet que l'installation des systèmes de vidéoprotection est subordonnée à une autorisation du préfet du département, et que « *les systèmes installés sur la voie publique ou dans des lieux ouverts au public* ***dont les enregistrements sont utilisés dans des traitements automatisés*** *[…]* » sont autorisés par la CNIL. Dans une décision du 27 juin 2016, le Conseil d'État a ainsi procédé à une **appréciation de la compatibilité entre la finalité de vidéoprotection et un traitement ultérieur réalisé à partir des images de vidéoprotection** pour juger si le traitement proposé devait être autorisé[2].

---

[1] *Des blackblocs par exemple.*

[2] *Conseil d'État, 10ème et 9ème chambres réunies, 27/06/2016, n° 385091. La décision est consultable à l'adresse suivante : https://www.legifrance.gouv.fr/ceta/id/CÉTATEXT000032790103.*

**Les finalités des systèmes de vidéoprotection**

**Les systèmes de vidéoprotection**, visés par l'article L. 251-2 du code de la sécurité intérieure, filment la voie publique et les lieux et établissements ouverts au public. Ils se distinguent des dispositifs de vidéosurveillance qui filment des lieux privés ou des lieux de travail non ouverts au public (locaux d'entreprises, de commerces, d'hôtels réservés aux salariés, *etc.*).

Les dispositifs de vidéoprotection poursuivent des finalités limitativement énumérées. Pour les dispositifs mis en œuvre sur la **voie publique**, qui ne peuvent être opérés que par les autorités publiques compétentes, il s'agit de :

1° la protection des bâtiments et installations publics et de leurs abords ;

2° la sauvegarde des installations utiles à la défense nationale ;

3° la régulation des flux de transport ;

4° la constatation des infractions aux règles de la circulation ;

5° la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ;

6° la prévention d'actes de terrorisme ;

7° la prévention des risques naturels ou technologiques ;

8° le secours aux personnes et la défense contre l'incendie ;

9° la sécurité des installations accueillant du public dans les parcs d'attraction ;

10° le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile ;

11° la prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets.

S'agissant des systèmes mis en place dans des **lieux et établissements ouverts au public**, ils ne peuvent avoir pour finalité que d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol.

Les commerçants peuvent enfin mettre en œuvre sur la voie publique, après information du maire et des autorités publiques compétentes, un système de vidéoprotection aux fins d'assurer la protection des abords immédiats de leurs bâtiments et installations, dans les lieux particulièrement exposés à des risques d'agression ou de vol, dans les conditions définies par un décret en Conseil d'État.

**L'installation d'un système de vidéoprotection est subordonnée à une autorisation du représentant de l'État dans le département** et, à Paris, du préfet de police. Cette autorisation est donnée, sauf en matière de défense nationale, **après avis de la commission départementale de vidéoprotection**[1].

*Source : Commission des lois du Sénat*

[1] *Article L. 252-1 du code de la sécurité intérieure.*

Selon les informations recueillies par les rapporteurs au cours de leurs auditions, le Conseil d'État aurait cependant, dans un avis rendu le 12 octobre 2021, non publié, estimé que **les traitements des images issues de la vidéoprotection par le biais 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 déduit qu'une **base législative explicite est nécessaire pour encadrer le recours à l'intelligence artificielle sur des images issues de l'espace public, y compris sans utilisation de données biométriques**.

Si ces dispositifs sont, pour certaines finalités, moins fiables que les logiciels utilisant des données biométriques, ils permettent cependant de limiter par rapport à ces derniers les impacts sur les libertés individuelles et la vie privée ainsi que le sentiment de surveillance. Les rapporteurs considèrent donc qu'ils doivent être déployés en priorité pour répondre aux enjeux de sécurité car ils peuvent, dans un grand nombre de cas, constituer une réponse satisfaisante et suffisante.

Les rapporteurs estiment en conséquence légitime **d'établir, à titre expérimental, une base législative qui permettrait aux opérateurs de dispositifs de vidéoprotection sur la voie publique ou dans des espaces ouverts au public et aux personnes publiques destinataires des images en étant issues de mettre en œuvre des traitements d'images par intelligence artificielle, sans traitement de données biométriques, pour l'exercice de leurs missions et dans la limite des finalités accordées au dispositif de vidéoprotection concerné**[1].

Cette base législative permettrait ainsi, par exemple :

- aux forces de sécurité intérieure de détecter des comportements anormaux sur la voie publique ou d'effectuer le suivi d'une personne sur la voie publique, en temps réel ou *a posteriori*, à partir d'éléments non biométriques comme son habillement par exemple ;

- aux collectivités territoriales d'utiliser l'intelligence artificielle pour les assister dans leurs missions. Deux exemples peuvent plus particulièrement être évoqués. Dans le cadre de leurs pouvoirs de police, les communes pourraient souhaiter détecter à l'aide de l'intelligence artificielle les dépôts sauvages d'ordures. Les autorités organisatrices de la mobilité, quant à elles, pourraient bénéficier de l'intelligence artificielle pour mettre en place des systèmes d'aide à la conduite, en détectant les obstacles devant

[1] *Écartant ce faisant l'obligation prévue par le RGPD de garantir aux personnes concernées la possibilité de s'opposer au traitement de leurs données.*

un véhicule de transport public ou les personnes présentes dans un angle mort ;

- aux acteurs privés de détecter les incidents (incivilités, fraude, délinquance) afin d'améliorer leur gestion des agressions ou des vols dans des lieux et établissements ouverts au public ou dans les abords immédiats de bâtiments et d'installations particulièrement exposés à ces risques.

Pour ce faire, **la base législative des traitements d'images de vidéoprotection à partir d'un logiciel d'intelligence artificielle n'utilisant pas de données biométriques pourrait être adossée aux dispositions législatives régissant la vidéoprotection**. La mise en œuvre de ces traitements ne serait possible **que s'ils s'inscrivent dans les mêmes finalités** que celles attribuées au système de vidéoprotection mis en place, **après consultation de la CNIL dans le cas où le traitement a pour finalité la prévention ou la détection des infractions pénales**. **L'autorisation préfectorale** des systèmes de vidéoprotection devrait être modifiée pour intégrer cette nouvelle fonctionnalité et **l'information du public assurée**.

Seraient ainsi vérifiées la proportionnalité du traitement mis en place et l'intérêt légitime du responsable du traitement, la conformité des finalités envisagées aux finalités du dispositif de vidéoprotection, l'adéquation des données collectées, ainsi que les modalités d'exercice des droits d'accès et de rectification des personnes concernées.

Ainsi, certains usages comme ceux visant à classifier les personnes ou à détecter leurs émotions ou leurs humeurs afin d'afficher des publicités ciblées par exemple, qui ne s'inscrivent pas dans les finalités attribuées aux systèmes de vidéoprotection et ne se rattachent pas à un « *intérêt légitime* » au sens du RGPD, ne pourraient pas être mis en œuvre sans le consentement des personnes concernées.

> **Proposition n° 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.**

Il pourrait également être envisagé de **permettre, sur la base de lignes directrices établies par la CNIL quant à l'évaluation de leur proportionnalité et leur nécessité, le déploiement de caméras couplé à des logiciels d'intelligence artificielle à des fins de traitement statistiques d'un groupe de personnes**. Ce type de dispositif, qui ne produit que des informations agrégées ou des décisions concernant un ensemble de personnes, est moins intrusif et engendre des risques moindres que ceux

ayant pour objet ou pour effet une prise de décision ou des conséquences au niveau individuel.

Deux cas doivent être distingués :

**- si la finalité poursuivie est la production d'indicateurs et qu'il existe en conséquence un délai entre la captation des données par le dispositif permettant la production de résultats statistiques et leur exploitation par le responsable de traitement**, alors le traitement entre dans le champ des traitements de données à des fins statistiques au sens du RGPD et de la loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*. Il est en conséquence possible d'écarter le droit d'opposition des personnes concernées par le traitement. Leur utilisation dans l'espace public devrait cependant faire l'objet d'une règlementation particulière ;

**- si ces traitements sont utilisés à l'appui d'une décision qui concerne le même groupe de personnes que celui dont les données ont été exploitées, alors ils ne sont pas considérés comme étant réalisés à des fins statistiques** au sens de la loi « Informatique et Libertés », et ne peuvent en conséquence actuellement pas fonder une exclusion du droit d'opposition des personnes. Les rapporteurs considèrent que ces traitements pourraient être autorisés lorsqu'ils sont réalisés par des personnes publiques ou des personnes privées concourant à des missions de service public dans le cadre de leurs missions, et que le droit d'opposition des personnes pourrait être écarté dans ce cadre dans la mesure où son exercice risquerait « *de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités* »[1].

> **<u>Proposition n° 15 :</u> 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.**

### *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 également être effectuée en leur sein, cette fois-ci entre authentification et identification**.

[1] *Article 78 de la loi n° 78-17 du 6 janvier 1978* relative à l'informatique, aux fichiers et aux libertés *et article 116 du décret n° 2019-536 du 29 mai 2019* pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Cette distinction apparaît justifiée au regard de la différence de degré entre les risques encourus. L'authentification 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.

**Le consentement donné par la personne doit cependant être libre, spécifique, éclairé et univoque**. Cela implique l'**existence d'une alternative valable** à l'usage de l'authentification biométrique et l'**absence de rapport de subordination**[1].

**Deux modalités d'authentification des personnes peuvent être envisagées** :

**- la personne dispose d'un support dans lequel est stocké son gabarit biométrique**. Le système effectue alors une comparaison entre le gabarit stocké et celui extrait à l'instant *t* du visage de la personne concernée – c'est l'exemple du système PARAFE pour lequel le gabarit de la personne est conservé dans son passeport ;

**- le gabarit de la personne est extrait lors de son enrôlement dans le dispositif et ensuite conservé au sein d'une base de données**. Le gabarit capté lorsque la personne se présente au contrôle d'accès est alors comparé avec ceux de la base de données (*white list*).

**Ces usages peinent cependant à se développer**, la CNIL rappelant l'enjeu de proportionnalité lié au traitement de données sensibles, le risque associé aux biais existant dans les traitements de reconnaissance faciale, et le risque de capter les données de personnes non consentantes qui passeraient devant une caméra sur laquelle est appliqué le traitement, et ce en dépit des précautions d'affichage et d'information mises en place. Il pourrait en ce sens être pertinent de **donner une base légale à l'usage de cette technologie**, car selon le retour d'expérience des expérimentations conduites en la matière, comme par exemple lors du tournoi de tennis de Roland-Garros de 2020, un système de sécurité utilisant la reconnaissance faciale est souvent perçu par les utilisateurs comme un service rendu. **Cette base légale imposerait aux personnes souhaitant mettre en œuvre un tel dispositif** :

- 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 ;

---

[1] *Tribunal administratif de Marseille, 27 février 2020, n° 1901249. Ce jugement est consultable à l'adresse suivante : http://marseille.tribunal-administratif.fr/Media/TACAA/Mediatheque-marseille/jurisprudence-TA/Selection-jurisprudence-2020/1901249.*

- les modalités de **recueil du consentement** des personnes concernées, qui pourrait lorsque cela s'y prête, être donné pour une durée limitée ;

- **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 s'authentifiant au moment de leur présentation au contrôle d'accès ;

- le **maintien d'un contrôle humain**, en particulier lorsque le gabarit de la personne capté au moment du contrôle est comparé avec une base de données (*white list*).

**Proposition n° 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.**

À ce jour, **l'utilisation obligatoire de traitements de données biométriques à des fins de contrôle d'accès aux lieux et aux outils de travail est par principe interdit**, en raison de son caractère particulièrement intrusif.

**Par exception, un tel contrôle peut être mis en place si l'employeur en justifie, de manière très concrète, le besoin par rapport à d'autres solutions de contrôle moins intrusives**. Pour ce faire, l'employeur doit :

- **justifier d'un contexte spécifique rendant nécessaire un niveau de protection élevé**. La CNIL cite comme exemple, sur son site internet, la manipulation de machines ou produits particulièrement dangereux, l'accès à

des fonds ou des objets de valeurs, à du matériel ou des produits faisant l'objet d'une règlementation spécifique (comme des substances psychotropes et leurs précurseurs, des produits chimiques pouvant être utilisés pour la fabrication d'armes, *etc.*) ;

**- démontrer l'insuffisance ou l'inadéquation des moyens moins intrusifs comme un badge ou un code d'accès**. La CNIL cite comme exemple un environnement dans lequel une identification forte est nécessaire pour prévenir une usurpation d'identité en cas de vol de badge ou d'interception des codes d'accès.

Tout en conservant le principe d'une interdiction de l'usage de la biométrie pour l'accès à certains lieux sans alternative non biométrique, il pourrait être envisagé d'ouvrir la même exception aux personnes publiques que celle offerte aux employeurs pour la sécurisation de certaines zones très spécifiques.

Cette exception, dont **l'usage devrait être extrêmement limité dans l'espace et dans le temps**, devrait s'accompagner de **garanties fortes,** telles que l'autorisation par une entité distincte sur la base d'une étude d'impact, l'agrément préalable des personnes pouvant accéder à la zone concernée pendant la période où est déployé le dispositif, la suppression des gabarits de référence dès la fin de l'évènement, et l'absence de conservation des gabarits captés lors des contrôles d'accès.

**Proposition n° 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.**

### *C. DISTINGUER, AU SEIN DES DISPOSITIFS D'IDENTIFICATION BIOMÉTRIQUES, L'IDENTIFICATION EN TEMPS RÉEL DE CELLE RÉALISÉE* A POSTERIORI

#### 1. L'identification *a posteriori* sur la base de caractéristiques biométriques

Distinctes des opérations d'authentification où le consentement et l'information des personnes sont facilités, **les opérations d'identification à distance sur la base de données biométriques doivent faire l'objet d'un encadrement extrêmement strict au regard des risques encourus**. Elles doivent être circonscrites dans le temps et dans l'espace et subordonnées à des circonstances exceptionnelles.

Des distinctions doivent toutefois là encore être réalisées. La principale 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 second 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**.

Ces différentes caractéristiques des systèmes de reconnaissance biométrique ont un impact important sur leurs possibilités opérationnelles et leur niveau d'atteinte aux libertés individuelles. Il convient donc, là encore, d'étudier les différents cas d'usage envisageables.

*a) Permettre une utilisation de la biométrie dans les fichiers de police dans le cadre d'enquêtes judicaires ou d'opérations de renseignement*

Depuis 2012, le fichier du traitement des antécédents judiciaires (TAJ) permet deux types d'exploitation de la reconnaissance faciale en tant qu'outil d'aide à l'enquête judiciaire : la recherche à partir d'une photo-question et la création d'une fiche personne auteur ou victime anonyme. Il s'agit du seul fichier de police dans lequel cette recherche par reconnaissance faciale est possible.

**Les différents fichiers de police fonctionnent en effet en silo et sont principalement basés sur des données alphanumériques** (noms, prénoms, date et lieu de naissance), sans qu'une action forte de recoupement des différents fichiers ne soit menée pour lutter contre la fraude et tenter d'assurer l'exactitude des données enregistrées. Une personne peut ainsi être répertoriée dans plusieurs fichiers – voire plusieurs fois dans un même fichier – sous différentes identités, sans qu'il soit possible de rapprocher ces identités.

À l'inverse, **dans l'Union européenne, un effort est réalisé depuis 2015 pour favoriser l'interopérabilité des différents fichiers et permettre ce faisant leur fiabilisation**. La construction de cette fiabilisation se base sur un système de rapprochement des données biométriques présentes dans les fichiers, qu'il s'agisse des empreintes digitales ou des images des visages des personnes.

**Un effort similaire devrait être réalisé en France. La mise en place de modules de reconnaissance biométrique au sein de davantage de fichiers de police permettrait ainsi de fiabiliser les données enregistrées**, en évitant qu'une même personne soit répertoriée sous différentes identités ou qu'une personne fasse usage d'une identité qui n'est pas la sienne pour éviter les contrôles. Un préalable à cette ouverture consiste en l'alimentation des fichiers concernés par les empreintes digitales et des images du visage de

la personne concernée, conformément d'ailleurs aux propositions actuelles de modifications du droit européen[1].

**Il pourrait en premier lieu être intéressant d'intégrer un module de reconnaissance faciale au fichier des personnes recherchées (FPR).** L'intégration d'un tel module serait d'autant plus pertinente que l'introduction à terme d'une fonctionnalité de reconnaissance faciale dans le Système d'information Schengen ou Fichier Schengen (SIS)[2], homologue européen du FPR, est déjà prévue[3]. Cela permettrait notamment aux enquêteurs de mettre en relation le FPR et le TAJ, afin d'une part de vérifier si l'individu inscrit au TAJ fait l'objet de fiches de recherches et, d'autre part, de détecter si un individu inscrit au FPR dispose d'antécédents.

**Les autres fichiers pouvant intégrer un module de reconnaissance faciale devraient être définis par le Gouvernement à l'issue d'un travail de consultation des différents services opérationnels**, au regard des principes de nécessité et de proportionnalité. Au cours des auditions des rapporteurs, ont notamment été cités :

- le **fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT)** ;

- le **fichier de gestion de l'information et de prévention des atteintes à la sécurité publique (GIPASP)**, géré par la gendarmerie nationale ;

- le **fichier de centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux (CRISTINA)**, fichier de souveraineté géré par la direction générale de la sécurité intérieure (DGSI).

**Le choix des fichiers concernés pourrait reposer notamment sur les finalités des traitements ainsi que sur la nature et la gravité des faits ayant conduit à l'inscription dans le fichier**. La mise en place de ces modules au sein des différents fichiers nécessiterait la prise de décrets en Conseil d'État.

Certains acteurs ont également appelé à l'ouverture de modules de reconnaissance faciale au sein de fichiers regroupant une part bien plus large

---

*[1] La Commission européenne a adopté le 8 décembre 2021 une proposition de paquet législatif appelé « Code de coopération policière de l'UE », qui comprend une proposition de directive du Parlement européen et du Conseil relative à l'échange d'informations entre les services répressifs des États membres, une proposition de règlement du Parlement européen et du Conseil relatif à l'échange automatisé de données dans le cadre de la coopération policière (« Prüm II »), modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil (les « décisions Prüm ») et les règlements (UE) 2018/1726, 2019/817 et 2019/818 du Parlement européen et du Conseil, et une proposition de recommandation du Conseil relative à la coopération policière opérationnelle.*

*[2] Ce fichier comprenant déjà les empreintes digitales et les photographies des personnes qu'il répertorie.*

*[3] Voir le règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du Système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission.*

de la population française, comme par exemple le fichier des permis de conduire ou celui des titres électroniques sécurisés (TES), qui contient des données personnelles pour la création et la gestion des cartes nationales d'identité et des passeports des Français. **Cela permettrait à l'évidence une identification plus efficace des personnes dans un cadre judiciaire ou de renseignement mais les rapporteurs considèrent qu'une telle ouverture serait disproportionnée.** Ils sont en conséquence favorables à un **ciblage strict sur des fichiers spécifiques d'ores et déjà consacrés au suivi d'objectifs par les forces de sécurité intérieure.** Ils considèrent également que les modules ainsi créés ne devraient être **accessibles qu'aux forces de sécurité nationales dans un cadre judiciaire ou dans un cadre de renseignement** et non pour effectuer des contrôles d'identité des personnes dans l'espace public.

> **Proposition n° 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.**

En complément, il serait nécessaire de bénéficier de **retours sur la pertinence des réponses proposées aux forces de sécurité intérieure dans leur utilisation du module de reconnaissance faciale du TAJ**. Ainsi, si le résultat de la recherche par reconnaissance faciale au sein du TAJ est repris dans un procès-verbal d'investigation, il n'a pas été possible aux rapporteurs d'obtenir une évaluation de l'utilité pour l'enquête judiciaire des réponses proposées.

**Cette absence de retour est préjudiciable**. Les rapporteurs recommandent donc que soit mis en place un **dispositif de suivi de la pertinence des résultats proposés lors des recherches effectuées**. Cela pourrait simplement consister en une page supplémentaire dans l'application demandant à l'enquêteur d'évaluer la pertinence des résultats proposés dans le cas d'une recherche par photo-question, ou d'un suivi des remontées ultérieures en cas de création d'une fiche auteur ou victime anonyme.

> **Proposition n° 19 : Évaluer l'efficacité des modules de reconnaissance faciale dans le TAJ ainsi que, le cas échéant, dans les autres fichiers de police où un tel module serait mis en place.**

*b) La reconnaissance* a posteriori *d'une personne dans un cadre judiciaire ou pour certaines finalités de renseignement*

Lors des enquêtes judiciaires, un grand nombre d'images peut être obtenu, issues par exemple de systèmes de vidéoprotection ou de smartphones de témoins. L'exploitation de ces images est rendue complexe en raison de leur nombre.

Ainsi, l'exploitation de ces images de manière automatisée permettrait de rendre le travail des enquêteurs bien plus efficace. Au-delà d'une exploitation basée sur un signe distinctif d'une personne (habillement, sac à dos, *etc.*), l'utilisation de la reconnaissance faciale pour les infractions les plus graves permettrait de déterminer plus rapidement d'éventuels suspects, les itinéraires empruntés et leurs modalités de fuite. Elle pourrait également permettre de reconstituer l'itinéraire d'une victime en cas de disparition inquiétante par exemple.

L'aide à l'exploitation de ces images par un logiciel de reconnaissance faciale devrait impérativement s'effectuer avec **l'autorisation et sous le contrôle du magistrat en charge de l'enquête ou de l'instruction**, de manière **subsidiaire**, pour des cas précis limités aux **enquêtes sur les infractions les plus graves**, sur des **images se rapportant à un évènement précis**, limité dans le temps et dans l'espace.

> **Proposition n° 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.**

**En matière de renseignement, l'exploitation des images a également une grande importance**. Ces images peuvent provenir de deux sources :

- des différentes techniques de renseignement mises en œuvre par les services, après autorisation de la commission nationale de contrôle des techniques de renseignement (CNCTR) ;

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

**L'autorisation d'exploitation des renseignements collectés par le biais des techniques de renseignement** est souvent incluse dans l'autorisation de déploiement de la technique. 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**. La direction générale de la sécurité intérieure (DGSI) a en conséquence initié des programmes de recherche afin de développer des outils d'analyse d'images, y compris des outils comportant des systèmes de reconnaissance faciale. La loi n° 2021-998 du 30 juillet 2021 *relative à la prévention d'actes de terrorisme et au renseignement* ayant permis aux services de renseignement de conserver les données pendant une durée plus longue à des fins de recherche et développement, la performance de ces outils pourra être améliorée[1].

En ce qui concerne **l'exploitation des images issues de la voie publique, en particulier issues de la vidéoprotection**, la direction générale de la sécurité intérieure a indiqué aux rapporteurs qu'il pourrait lui être **utile d'utiliser des systèmes de reconnaissance faciale afin, *a posteriori*, d'identifier une personne recherchée ou de reconstituer son parcours**. Un tel usage se révèlerait en particulier pertinent dans le cadre de la mission de **prévention de toute forme d'ingérence étrangère[2]**, aux fins de détecter la présence sur le sol national d'agents de services étrangers, qui entrent en France sous fausse identité.

Cette même possibilité pourrait également être ouverte pour la promotion de l'indépendance nationale, l'intégrité du territoire et la défense nationale[3], la prévention du terrorisme[4] 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[5].

**<u>Proposition n° 21 :</u> 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.**

[1] *Article L. 822-2 du code de la sécurité intérieure.*
[2] *2° de l'article L. 811-3 du code de la sécurité intérieure.*
[3] *1° de l'article L. 811-3 du code de la sécurité intérieure.*
[4] *4° de l'article L. 811-3 du code de la sécurité intérieure.*
[5] *5° de l'article L. 811-3 du code de la sécurité intérieure.*

### 2. L'identification en temps réel sur la base de caractéristiques biométriques

Dans quelques **cas très spécifiques et circonscrits**, il pourrait être envisagé, **à titre d'exception**, d'autoriser l'utilisation de la reconnaissance biométrique sur la voie publique en temps réel dès lors que celle-ci serait strictement nécessaire, adaptée et proportionnée pour la prévention d'une menace grave et imminente pour la vie ou la sécurité des personnes, en cas de menace grave et imminente pour la sécurité nationale ou dans le cadre d'une enquête judiciaire pour une infraction suffisamment grave.

**Dans le cadre d'enquêtes judiciaires en premier lieu**, 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**. Les infractions concernées pourraient par exemple être limitées aux crimes menaçant ou portant atteinte à l'intégrité physique des personnes.

**Dans un cadre administratif**, il pourrait être envisagé de déployer des systèmes de reconnaissance biométrique en temps réel sur la voie publique à des fins de prévention du terrorisme, 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.

**La détection de personnes d'intérêt sur un périmètre géographique limité et pour une période précisément déterminée** correspond au dispositif mis en place par les polices du Pays de Galles et de Londres. **L'utilisation de caméras mobiles distinctes de celles des systèmes de vidéoprotection devrait dans ce cas être privilégiée** : cela permettrait 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

[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****.*

ce cadre devront être intégrées au cas par cas pour chaque déploiement, sur la base de la probabilité qu'elles se trouvent sur le lieu concerné.

**Dans un cadre de renseignement enfin**, il pourrait être envisagé de déployer des dispositifs de reconnaissance biométrique **sur les systèmes de vidéoprotection**, mais toujours dans un **cadre géographique et temporel extrêmement limité**, **en cas de menaces imminentes pour la sécurité nationale**. L'objectif poursuivi serait alors de retrouver un objectif qui aurait été momentanément perdu. Afin de garantir la confidentialité des photographies utilisées, il conviendrait que les flux de vidéoprotection concernés soient transmis en temps réel aux services de renseignement qui réaliseraient eux-mêmes l'interrogation des images par le logiciel de reconnaissance biométrique. La capacité à procéder à une exploitation de ces enregistrements ne doit en effet pas se faire au détriment de la confidentialité des enquêtes de renseignement, au risque de fragiliser l'action des services.

**Le déploiement de ces logiciels devrait être effectué avec l'autorisation et sous le contrôle d'une autorité qui devrait être** :

- le magistrat en charge de l'enquête ou de l'instruction dans le cas d'un déploiement dans un cadre judiciaire ;

- le préfet en cas de déploiement en matière de police administrative, sur la base de justifications du caractère adapté, proportionné et subsidiaire du déploiement envisagé. Il pourrait dans ce cadre être envisagé, sur le modèle de l'encadrement de l'usage des drones par la loi n° 2022-52 du 24 janvier 2022 *relative à la responsabilité pénale et à la sécurité intérieure*, de prévoir un nombre maximal de caméras pouvant être simultanément utilisées ;

- la CNCTR en cas de déploiement à finalité de renseignement.

**La proportionnalité des moyens impose également que l'usage de dispositifs de reconnaissance biométrique en temps réel ne puisse faire l'objet d'aucune autre alternative**, et soit donc strictement subsidiaire.

**Plusieurs autres garanties pourraient être envisagées**, comme :

- une minimisation des données utilisées et leur sécurisation ;

- une supervision humaine systématique ;

- une traçabilité des usages.

En tout état de cause, une **information du public** adaptée aux spécificités du déploiement devra être réalisée, complétant une information plus générale menée par le Gouvernement.

**<u>Proposition n° 22 :</u> 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 site 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, 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.**

### *D. UN USAGE DE LA RECONNAISSANCE BIOMÉTRIQUE PAR LES ACTEURS PRIVÉS FONDÉ SUR LE CONSENTEMENT DES USAGERS*

S'agissant des usages privés de la reconnaissance biométrique, les rapporteurs considèrent qu'ils devraient être extrêmement limités. **Ils ne peuvent, de manière générale, se fonder que sur le consentement des personnes**. Celui-ci doit être libre, spécifique, éclairé et univoque.

Les rapporteurs s'interrogent toutefois sur la propension des consommateurs à partager leurs données biométriques avec des acteurs privés pour accéder à des services commerciaux. Ce type d'usage s'inscrit dans le processus actuel de numérisation massive des processus à des fins de

fluidification. Ils engagent les consommateurs à accéder aux guides de bonnes pratiques existants, notamment pour le paramétrage des logiciels applicatifs sur smartphone afin d'en limiter le caractère intrusif.

À titre exceptionnel et comme exposé précédemment, l'utilisation obligatoire de traitement de données biométriques à des fins de contrôle d'accès aux lieux et aux outils de travail peut être mis en place par l'employeur si ce dernier en justifie, de manière très concrète, le besoin par rapport à d'autres solutions de contrôle moins intrusives (*white list*).

**Sous cette réserve, les rapporteurs considèrent que ces cas d'usage sont suffisants** et recommandent en particulier d'interdire toute identification sur la base de données biométriques en temps réel ou en temps différé par des acteurs privés[1].

**Proposition n° 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

### *A. LA NÉCESSAIRE CRÉATION D'UN TIERS DE CONFIANCE EUROPÉEN*

Les rapporteurs sont convaincus que, s'agissant de la reconnaissance faciale, **la protection de l'autonomie technologique de la France, et plus largement de l'Europe, et la sauvegarde des libertés publiques sont les deux faces d'une même médaille**. En imposant le recours à des algorithmes développés à l'étranger, sans transparence sur leurs modalités de développement, la perte de notre autonomie technologique actuelle amplifierait significativement les risques d'atteintes aux libertés provoqués par une technologie déjà très intrusive en elle-même.

Pour combler ce besoin de protection de notre indépendance technologique, les rapporteurs plaident tout d'abord pour **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**. Sur le modèle du NIST, cette agence pourrait utilement

[1] *Hors cas de contrôle d'accès sur les lieux ou aux outils de travail dans les conditions définies ci-dessus (*white list*).*

fournir une évaluation indépendante aux développeurs quant à la performance de leurs algorithmes, et ce dans un cadre respectueux du RGPD. Surtout, l'institution d'une telle autorité **réduirait considérablement la dépendance à l'extérieur de l'Union européenne** pour ce qui est de la certification des algorithmes de reconnaissance faciale.

Il convient de noter que les acteurs du secteur de la reconnaissance faciale appellent eux-mêmes de leur vœux la création d'une telle autorité, à l'instar de l'Alliance pour la confiance numérique qui a indiqué défendre la mise en place d'un centre européen d'expertise en intelligence artificielle dont l'une des missions serait d'apporter une expertise technique indépendante, apte à juger de manière objective la qualité technique des applications utilisant une intelligence artificielle.

Sur le plan méthodologique, les rapporteurs proposent de dupliquer les procédés utilisés outre-Atlantique, en ayant recours à des « **données séquestrées** ». De manière à préserver l'intégrité du processus d'évaluation, les développeurs qui soumettraient leurs algorithmes n'auraient ainsi accès à la base de données utilisées ni pour entraîner leurs algorithmes ni pendant la phase de test. Afin d'assurer une protection effective des données à caractère personnel utilisées, les rapporteurs n'estiment en revanche **pas souhaitable que les jeux de données soient mis directement à disposition des développeurs**.

La condition *sine qua non* pour qu'une telle autorité puisse fonctionner est qu'elle dispose d'une base de données conséquente. Pour ce faire, les rapporteurs plaident pour la **constitution d'une base de données à l'échelle européenne**. Sous réserve de garanties appropriées, celle-ci pourrait notamment être alimentée *via* un mécanisme de mise à disposition des images détenues par les administrations publiques des États membres, sur le modèle de ce que prévoit la proposition de règlement du Parlement européen et du Conseil *sur la gouvernance européenne des données*, actuellement en cours de discussion, pour la réutilisation de données publiques par des acteurs privés. Les contributions altruistes ou, passé un certain délai, l'usage des photos de personnes décédées pourraient également être des options à explorer.

En tout état de cause, **la mise en place de mécanismes adaptés d'information des citoyens serait indispensable, de même que le fait de leur confier la possibilité de demander à tout moment le retrait de leurs données de la base**.

**<u>Proposition n° 24 :</u> 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 européen 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.**

### *B. 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*

#### 1. La mise en place d'un cadre juridique stable et spécifique à la recherche et au développement

Conscients des difficultés auxquelles sont actuellement confrontés les développeurs dans ce domaine, les rapporteurs soutiennent **la mise en place d'un cadre juridique stable et adapté aux besoins de la recherche et du développement**. Comme cela a été souligné au cours des auditions, l'obligation de recueil du consentement de l'intégralité des personnes concernées par le traitement constitue un obstacle de taille dans la mesure où une base de données doit parfois contenir des millions d'images pour être performante. Cela est d'autant plus problématique qu'une nouvelle expression du consentement est systématiquement requise pour réutiliser lesdites données dans un nouveau projet de recherche.

Afin de lever cet obstacle sans pour autant remettre en cause la logique légitime de recueil régulier du consentement des usagers, les rapporteurs proposent d'assouplir les conditions de réutilisation des données en autorisant le recours à un consentement « *groupé* ». Ces modalités de recueil seraient autorisées pour des seules fins de recherche et de développement visant des finalités proches du traitement initial, au besoin en créant une dérogation au RGPD dans la future législation européenne sur l'intelligence artificielle.

Afin de faciliter l'appropriation par les acteurs du cadre légal particulièrement complexe applicable à la recherche et au développement en matière de reconnaissance faciale, il pourrait par ailleurs être utile que **la CNIL formalise sa doctrine en la matière dans un document unique.**

**Proposition n° 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.**

**Proposition n° 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.**

### 2. Faciliter l'accès à des jeux de données des organismes de recherche publique

Les difficultés rencontrées par les organismes de recherche publique pour accéder à des jeux de données constituent une importante source de préoccupation et contribuent sans nul doute au développement limité de cette branche de recherche en France. Pour les résoudre, les rapporteurs proposent d'anticiper une éventuelle adoption de la proposition de règlement *sur la gouvernance européenne des données* précité, en créant dès à présent, sur une base législative, **un mécanisme de mise à disposition de données biométriques détenues par l'administration à des organismes de recherche publique**.

Compte tenu de la sensibilité de ces données et conformément à ce que prévoit ladite proposition de règlement, cette mise à disposition serait subordonnée à un **avis favorable de la CNIL** et ne pourrait intervenir que dans **un environnement de traitement des données sécurisé, fourni par l'État et sans possibilité d'en exporter les données**. Dans la mesure où les organismes de recherche ne disposent pas toujours de l'expertise juridique suffisante en la matière, les rapporteurs estiment par ailleurs nécessaire de

mettre en place **un service au sein de l'État dédié à l'accompagnement des démarches correspondantes auprès de la CNIL,** et ce afin de garantir un taux de recours élevé à ce dispositif.

**<u>Proposition n° 27 :</u> 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.**

**<u>Proposition n° 28 :</u> 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.**

### *C. CONSERVER LA MAÎTRISE TECHNOLOGIQUE DES ALGORITHMES EN ASSURANT LA TRAÇABILITÉ DES DONNÉES UTILISÉES ET LA SÉCURITÉ DES INFRASTRUCTURES D'HÉBERGEMENT*

Les rapporteurs entendent enfin insister sur deux aspects incontournables de la protection de notre souveraineté technologique dans le champ de la reconnaissance faciale :

- **l'indispensable traçabilité des données d'apprentissage** : les rapporteurs recommandent la création d'un dispositif de labellisation des logiciels de reconnaissance biométrique prenant notamment en compte l'origine et la traçabilité des données d'apprentissage. Alors que de nombreux algorithmes présents sur le marché proviennent de l'étranger et ont parfois été développés dans une certaine opacité, un tel mécanisme permettrait la valorisation des algorithmes développés sur le sol national ou européen, à partir de base de données d'entraînement dont l'origine est connue ;

- **la nécessité de sécuriser les infrastructures d'hébergement des données** utilisées dans le cadre des expérimentations menées par les autorités publiques : pour ce faire, il semble opportun que l'ANSSI s'assure régulièrement, par exemple sur une base annuelle, de la bonne protection contre les cyberattaques des bases de données qui seront utilisées dans le cadre des expérimentations préconisées par les rapporteurs.

**<u>Proposition n° 29 :</u> Créer un dispositif de labellisation des logiciels de reconnaissance biométrique, en prenant notamment en compte l'origine et la traçabilité des données d'apprentissages.**

**<u>Proposition n° 30 :</u> Prévoir un contrôle régulier par l'ANSSI de la sécurité des infrastructures d'hébergement des données biométriques utilisées par la puissance publique à des fins expérimentales.**

# EXAMEN EN COMMISSION

_____

MARDI 10 MAI 2022

**M. François-Noël Buffet, président**. – Nous allons maintenant examiner le rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles.

Je cède la parole aux rapporteurs.

**M. Arnaud de Belenet, rapporteur**. – Monsieur le président, mes chers collègues, avec clairvoyance et sagesse, notre commission a décidé, en octobre 2020, de lancer une mission d'information sur la reconnaissance faciale. Cette décision reposait sur trois constats.

Le premier est le développement rapide des technologies de reconnaissance biométrique, désormais considérées comme matures par les industriels. Il semblait impératif que le législateur s'en saisisse, afin de ne pas être dépassé par les déploiements réalisés par des acteurs privés.

Le deuxième est la proposition de règlement européen sur l'intelligence artificielle à venir qui, basé sur une approche par les risques, propose une réglementation spécifique pour ces technologies, qui sont aujourd'hui régies exclusivement par le droit des données personnelles.

Le troisième est l'extrême polarisation du débat, entre les tenants d'un moratoire et ceux qui plaident en faveur de l'efficacité opérationnelle de ces technologies, avec toujours d'excellents arguments.

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 », lequel est ensuite comparé avec un ou plusieurs autres, 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 ».

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 événements ou locaux sensibles, d'assurer la sécurité et le bon déroulement

d'événements 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 aujourd'hui extrêmement limités. Il s'agit pour l'essentiel du dispositif de rapprochement par photographie opéré dans le traitement d'antécédents judiciaires (TAJ) et du système PARAFE, qui permet 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 Aéroport 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 très nombreuses. Elles ont trait tant aux libertés publiques qu'à notre souveraineté technologique, les deux thématiques étant bien entendu interdépendantes.

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

Étant des 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 le fondement 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 des intérêts vitaux ou sur la base d'un intérêt public important. Sur le fondement 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.

**M. Marc-Philippe Daubresse, rapporteur**. – Ces constats étant posés, nous allons maintenant vous présenter les pistes que nous préconisons au terme de nos travaux, après avoir rencontré près de 120 personnes et procédé à quatre déplacements, notamment à Nice et à Londres. Je pense que les très nombreux entretiens que nous avons conduits, auprès de juristes, d'industriels ou de développeurs, de représentants des forces de sécurité intérieure ou d'associations de défense des droits sur internet, nous ont permis d'avoir une vision des choses globale et équilibrée.

Dans un premier temps, il nous semble indispensable de définir collectivement un cadre qui comprenne à la fois des lignes rouges, des interdits écartant le risque d'une société de surveillance – à cet égard, le titre de notre rapport est clair –, une méthodologie et un régime de contrôle. C'est bien d'ailleurs ce que nous ont demandé de faire la Commission nationale de l'informatique et des libertés (CNIL) et plusieurs acteurs que nous avons auditionnés.

Nous pensons que nous disposons d'une « fenêtre de tir » avant que le règlement européen sur l'intelligence artificielle actuellement en discussion n'entre en vigueur – les arbitrages sur certains points restent encore un peu flous –, pour dessiner les contours d'une reconnaissance biométrique « à la française » et essayer d'influer sur le législateur européen.

Dans la mesure où nous avons affaire à des techniques susceptibles d'apporter des changements profonds à la société – c'est un sujet éminemment politique –, il nous semble indispensable de faire comme en matière de bioéthique et de fixer dans la loi de grands interdits, qui seraient applicables à tous, acteurs publics comme privés, ce qui n'est pas la démarche actuelle de la réglementation européenne.

Pour être clairs, nous préconisons d'interdire le recours aux technologies de reconnaissance biométrique dans quatre cas.

Le premier est la notation sociale. La proposition de règlement sur l'intelligence artificielle nous semble assez frileuse de ce point de vue, puisqu'elle ne s'intéresse qu'aux acteurs publics. Il nous semble nécessaire de protéger les consommateurs de méthodes intrusives et d'empêcher le recours à la notation sociale par surveillance de leurs comportements, notamment dans les espaces de vente, de restauration ou les centres de loisirs.

Le deuxième est la catégorisation d'individus en fonction de l'origine ethnique, du sexe ou de l'orientation sexuelle – c'est une position constante de notre commission –, sauf dans le cadre de la recherche scientifique, de manière très encadrée et sous réserve de garanties appropriées.

La troisième interdiction est l'analyse d'émotions, qui se pratique déjà, par exemple dans certains cabinets de recrutement, sauf à des fins de santé ou de recherche scientifique et, une fois encore, sous réserve d'un cadre et de garanties appropriés.

La quatrième et dernière ligne rouge concerne l'utilisation 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, nous pensons qu'il faut interdire clairement cette surveillance biométrique lors de manifestations sur la voie publique et aux abords des lieux de culte, mais nous pouvons envisager de l'accorder dans un certain nombre de cas où il peut y avoir péril – on pense aux jeux Olympiques, par exemple.

Nous préconisons également de poser quelques principes : 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 humaine ; et le principe de transparence, pour que l'usage des technologies de reconnaissance biométrique ne se fasse pas à l'insu des personnes.

Une fois ces lignes rouges posées, nous sommes favorables à l'adoption d'une loi d'expérimentation sur le modèle de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme (SILT), soumise à une évaluation annuelle.

L'expérimentation pourrait être autorisée pour trois ans, le Gouvernement et le Parlement devant réévaluer le besoin et recadrer éventuellement le dispositif en fonction des résultats obtenus. Philippe Bas, alors président de notre commission, avait qualifié ce type de dispositif de « clause d'autodestruction »...

Pour que cette phase d'expérimentation soit utile, serait mise en place une évaluation publique et indépendante afin de connaître l'efficacité de la technologie dans le cas d'usage testé. Cette évaluation serait conduite par un comité composé de scientifiques et de spécialistes des questions éthiques qui pourrait fonctionner comme le comité qui rend chaque année un rapport sur l'algorithme Parcoursup. Cela n'empêchera en rien notre président de commission de créer une mission de contrôle tout au long de cette expérimentation.

Enfin, pour que les Français s'emparent du sujet – c'est loin d'être une question seulement technique, malgré sa grande technicité –, nous préconisons de rendre accessible une information claire sur les techniques de reconnaissance biométrique, les bénéfices qui en sont attendus et les risques encourus.

Le troisième volet de nos recommandations sur la création d'un cadre *ad hoc* porte sur l'indispensable contrôle du respect des règles.

Chaque usage devrait être autorisé *a priori*. L'utilisation par les forces de sécurité intérieure serait autorisée soit par un magistrat, soit par le préfet, selon que l'on s'insère dans un cadre de police judiciaire ou administrative. Pour une utilisation par un acteur privé dans un lieu accessible au public, la CNIL – pour éviter de multiplier les acteurs – serait chargée de l'autorisation.

La CNIL serait ainsi systématiquement consultée : pour les usages publics, parce que les analyses d'impact doivent 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.

Enfin, nous souhaitons que la CNIL exerce un 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.

**M. Jérôme Durain, rapporteur**. – La méthodologie et le cadre général ayant été présentés par Arnaud de Belenet et Marc-Philippe Daubresse, un raisonnement cas d'usage par cas d'usage s'impose. Nous avons en effet considéré que les déploiements potentiels devaient être distingués en fonction des risques pour les libertés qu'ils impliquent.

Une première distinction doit être réalisée entre vidéosurveillance intelligente, sans utilisation de données biométriques, et reconnaissance biométrique. Les traitements des images issues de la voie publique par des logiciels d'intelligence artificielle ne disposent pas aujourd'hui d'un cadre juridique propre ; plusieurs opérateurs de transport, notamment, s'en sont plaints. Certaines communes ont d'ores et déjà mis en place des systèmes de détection automatique des dépôts sauvages d'ordures, par exemple, mais il existe un débat juridique sur la possibilité de les déployer.

L'application de l'intelligence artificielle aux images issues de la vidéosurveillance nous semble constituer un changement d'échelle susceptible de porter atteinte aux libertés individuelles, ce qui nécessite une base législative explicite – le Conseil d'État semble aussi de cet avis. 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.

Nous vous proposons donc d'établir, à titre expérimental, une base législative qui permettrait aux opérateurs des systèmes de vidéosurveillance 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 vidéosurveillance déployé.

S'agissant maintenant des techniques de reconnaissance biométrique, les dispositifs d'authentification, qui permettent un contrôle sécurisé et fluidifié des accès, nous semblent devoir être autorisés lorsqu'ils sont basés sur le consentement des personnes. Dans certains cas très particuliers et à titre expérimental, ils pourraient également être rendus obligatoires pour accéder à des zones nécessitant une sécurisation exceptionnelle.

Les opérations d'identification, quant à elles, doivent faire l'objet d'un encadrement extrêmement strict au regard des risques encourus. Il convient là encore d'opérer une distinction entre l'exploitation en temps réel, c'est-à-dire permettant un usage immédiat des résultats pour procéder à un contrôle de la personne concernée, et l'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 tout d'abord de l'identification *a posteriori*, nous proposons, en premier lieu, d'autoriser l'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 révélerait 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.

Il convient maintenant d'aborder la question la plus sensible, celle de l'identification biométrique à distance en temps réel. Marc-Philippe Daubresse vous l'a dit : nous ne souhaitons pas voir son usage se généraliser, afin d'écarter tout risque d'avènement d'une société de surveillance. Nous avons donc envisagé son déploiement par exception, dans trois cas circonscrits.

Premier cas : dans le cadre d'une enquête judiciaire, en vue de faciliter l'interpellation d'une personne venant de commettre une infraction grave ou de permettre 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 être par exemple limitées aux crimes menaçant ou portant atteinte à l'intégrité physique des personnes.

Deuxième cas : dans un cadre administratif, en vue de sécuriser de grands événements 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.

Troisième cas : le renseignement, en cas de menace imminente pour la sécurité nationale.

Nous proposons d'entourer ces éventuels déploiements de solides garanties, que nous développons en détail dans le rapport. Nous pensons particulièrement à la nécessité d'une autorisation et d'un contrôle par une autorité distincte en fonction des usages – magistrat, préfet ou Commission nationale de contrôle des techniques de renseignement (CNCTR) –, au caractère strictement subsidiaire de ces usages, à leur traçabilité, à une supervision humaine systématique de technologies qui doivent se cantonner

à un rôle d'aide à la décision, ou, enfin, à une information du public adaptée aux spécificités du déploiement.

Enfin, l'usage des technologies de reconnaissance biométrique par les acteurs privés doit être extrêmement limité et se fonder, de manière générale, sur le consentement des personnes. En particulier, nous recommandons d'interdire toute identification sur la base de données biométriques en temps réel ou en temps différé par des acteurs privés, hors cas de contrôle d'accès aux lieux ou aux outils de travail de personnes spécialement habilitées par l'inscription sur une *white list*.

**M. Arnaud de Belenet, rapporteur**. – Le dernier axe de nos travaux se concentre sur la question de la protection de la souveraineté technologique française et européenne, qui va de pair avec la sauvegarde des libertés publiques. L'usage d'algorithmes développés en Europe à partir de données traçables et hébergées sur notre sol est, de notre point de vue, infiniment préférable au recours à des algorithmes étrangers dont on ne sait le plus souvent rien des conditions de création et d'entraînement.

La France dispose d'un écosystème de recherche et de développement très performant dans le champ de la reconnaissance biométrique, avec des entreprises de rang mondial. Pourtant, ces dernières évoluent dans un cadre juridique et matériel peu propice à la recherche et au développement et qui entrave leur capacité d'innovation.

Le premier obstacle réside dans un cadre juridique applicable particulièrement touffu, si bien que les entreprises n'arrivent pas toujours à distinguer ce qui est autorisé de ce qui ne l'est pas. Le règlement européen sur l'intelligence artificielle permettra de clarifier les choses, mais, dans l'attente, il est plutôt un facteur d'incertitude supplémentaire. Le second obstacle est celui de la constitution des jeux de données qui servent 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 pourtant essentiel au développement de l'algorithme. Cela est même quasiment impossible pour des laboratoires de recherche publique aux moyens parfois limités.

Pour lever ces obstacles, nous proposons tout d'abord 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. L'utilisation d'un algorithme inefficace ou biaisé démultiplie, en effet, les risques de discrimination en particulier et d'atteinte aux libertés publiques en général. Pour donner à cette autorité les moyens de son action, il nous paraît essentiel de créer une base d'images à l'échelle européenne qui lui permettra de procéder aux évaluations. Sous réserve de garanties appropriées, celle-ci

pourrait être alimentée 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, nous plaidons enfin pour un cadre juridique spécifique et adapté à cette activité. Cela se traduirait, par exemple, par des mécanismes sécurisés de mise à disposition de données biométriques détenues par l'État aux laboratoires de recherche publique. Bien évidemment, ce cadre juridique dérogatoire devrait s'accompagner de fortes garanties ; nous proposons par exemple de subordonner cette réutilisation de données publiques à un avis favorable de la CNIL.

Nous proposons, enfin, d'intituler ce rapport : « La reconnaissance biométrique dans l'espace public : trente propositions pour écarter le risque d'une société de surveillance. »

Avec Marc-Philippe Daubresse et Jérôme Durain, nous avons su conjuguer nos cultures politiques différentes sans débats houleux et de manière, pour tout dire, naturelle.

**M. Jean-Yves Leconte**. – Si nous voulons encadrer efficacement une technologie, il nous faut d'abord la maîtriser.

Il y a dix ans, la reconnaissance faciale consistait à vérifier la concordance entre le visage d'une personne et une photo d'identité sans avoir besoin de l'identifier.

Mais, aujourd'hui, avec l'intelligence artificielle et les réseaux sociaux, cette identification peut se faire sans aucun contrôle. Par ailleurs, l'intelligence artificielle a besoin de toutes les données possibles pour apprendre. Même en Europe, si nous voulons la développer, nous aurons besoin des données extérieures.

À Kiev, où je me suis rendu voilà deux semaines avec quelques collègues, on nous a dit que l'intelligence artificielle était d'ores et déjà utilisée pour repérer les doubles passeports. C'est un outil de défense qui existe.

Le RGPD est une bonne chose, mais l'Europe doit veiller à ne pas être dépassée. Je le confirme : certaines entreprises développent par exemple des robots de défense en passant par des entreprises extérieures à l'Union européenne.

**M. François-Noël Buffet, président**. – A été évoquée la mise en place un suivi formel par la commission des lois : s'agissant d'un domaine relevant de la souveraineté et des libertés individuelles, nous n'y manquerons pas.

Je mets désormais les 30 propositions aux voix.

*La commission, à l'unanimité, adopte les 30 propositions et autorise la publication du rapport d'information.*

# LISTE DES DÉPLACEMENTS

**MARDI 21 FÉVRIER 2022**

*Orly*

*16 h 40* Parcours d'embarquement par biométrie – **MM. Thierry CROS, Erwan LE ROUX** et **Maxime CARETTE**

- Process enregistrement sur la zone 48
- Process embarquement

*17 h 00* Présentation du système PARAFE

- Process départ ORLY 4 – **MM. Thierry CROS** et **Alexis MARTY**

*17 h 30* Biométrie et Processus Passager – **MM. Quentin DEVOUGE**, **Thierry CROS** et **Maxime CARETTE**

*17 h 50* PARAFE et Entry Exit System (EES) – **Mme Marie-Eve ALBERTELLI**, **MM. Thierry CROS** et **Alexis MARTY**

*18 h 10* Prise en compte des enjeux RGPD dans les systèmes utilisant la biométrie – **Mme Cécile OCHS**

**JEUDI 17 MARS 2022**

*Nice*

*10 h 00 – 12 h 30* Visite du Centre de supervision urbain et présentation de l'utilisation de la vidéoprotection par la ville de Nice – Centre opérationnel de commandement de la police municipale

Échanges avec l'équipe projet de l'expérimentation de reconnaissance faciale menée pendant le carnaval de Nice en 2019 :

**Mme Véronique BORRÉ**, directrice générale adjointe Proximité et Sécurités, Ville de Nice

**Mme Karine CHOMAT**, déléguée à la protection des données, Ville de Nice

**M. Nicolas MAILLAN**, responsable de l'unité vidéoprotection et radio au sein de la direction des systèmes d'information, Ville de Nice

**M. Grégory PEZET**, responsable du centre de supervision urbain de la ville de Nice (policier municipal)

*12 h 45 – 14 h 15* Déjeuner de travail

**M. Anthony BORRÉ**, premier adjoint de la ville de Nice, délégué à la Sécurité, au logement et à la rénovation urbaine

**Mme Véronique BORRÉ**, directrice générale adjointe Proximité et Sécurités

**M. Xavier LATOUR**, conseiller délégué à l'enseignement supérieur, la recherche et la formation continue, professeur de droit public, doyen de la Faculté de droit et science politique, Université Côte d'Azur, CERDACFF

*15 h 00 – 16 h 00* Présentation des travaux de l'Institut national de recherche en sciences et technologies du numérique (Inria) en matière de reconnaissance faciale – Inria Sophia Antipolis

**Mme Maureen CLERC**, directrice du centre de recherche Inria Sophia Antipolis - Méditerranée

**Mme Antitza DANTCHEVA** et **François BREMOND**, chercheurs de l'équipe STARS (Spatio-Temporal Activity Recognition Systems)

**M. Jean-Pierre MERLET**, responsable scientifique du projet HEPHAISTOS (HExapode, PHysiologie, AssISTance et Objets de Service)

**Mme Sandrine MAZETIER**, directrice des affaires publiques

*16 h 15 - 17 h 30* Présentation des travaux du Sophia Antipolis Accenture Labs sur la reconnaissance faciale

**Mme Anne GROEPPELIN**, directrice du Sophia Antipolis Accenture Labs

**M. Emmanuel VIALE**, directeur exécutif d'Accenture Technology Innovation

**M. Cyrille BATALLER**, directeur exécutif d'Accenture Applied Intelligence

**M. Thomas MORETTI**, senior manager, expert Identité et biométrie

*17 h 30 – 18 h 30* Table ronde d'entreprises qui développent des solutions utilisant la reconnaissance faciale

**M. Fabien AILI**, directeur Vérification d'identité, Biométrie & IA de Docaposte

**M. Alan FERBACH**, président directeur général de Videtics

**Mme Olena KUSHAKOVSKA**, directrice générale de SAP Labs France et représentante d'ICAIR (Conseil de recherche industrielle pour l'intelligence artificielle)

**M. Denis LACROIX**, président d'Amadeus Sas

**M. Thomas MORETTI**, senior manager, expert Identité et biométrie

**MARDI 29 MARS 2022**

*Thales à Meudon*

*14 h 30 – 15 h 00* Présentation générale de THALES et des activités liées à la biométrie et à l'identité numérique

**M. Fabrice BOURDEIX**, vice-président Stratégie et Politique Produit DIS

**M. Jean-Claude PERRIN**, directeur Stratégie & Marketing Identity & Biometric Solutions (IBS)

*15 h 00 – 15 h 30* Les technologies de reconnaissance faciale et leurs applications

**M. Philippe FAURE**, directeur ligne de produits biométriques

*15 h 30 – 16 h 00* Démonstrations des kiosques Entry Exit Systems – Face Pods

*16 h 00 – 16 h 30* Les développements menés par THALES en matière d'algorithmes appliqués à la biométrie et la reconnaissance faciale

**Mme Sandra CREMER**, responsable Recherche Algorithme Biométrie

*16 h 30 – 17 h 00* Biométrie et éthique : l'approche *True Biometrics* de THALES et les initiatives de réglementations européennes

**M. Benoît JOUFFREY**, directeur technique DIS

**M. Jean-Claude PERRIN**, directeur Stratégie & Marketing Identity & Biometric Solutions (IBS)

**Mme Kadie-Ann FYFFE**, spécialiste en communication

**JEUDI 7 ET VENDREDI 8 AVRIL 2022**

*Londres*

- Jeudi 7 avril 2022 -

*9 h 30 – 11 h 00* Entretien avec la Mayor's Office for Policing And Crime (MOPAC) - London City Hall

**M. Kenny BOWIE**, chef de « Planning, Design and Resources »

**M. James BOTTOMLEY**, chef de « MPS oversight and performance »

**Mme Sophie LINDEN**, maire adjoint pour la police et le crime

*12 h 00 – 15 h 00* Déjeuner de travail - New Scotland Yard

*Metropolitan Police* :

**Mme Lindsey CHISWICK**, directrice du renseignement au MPS « Director of Intel »

**Mme Amanda BODDY**, constable, staff officer auprès de la directrice

**M. Jamie TOWNSEND**, detective chief inspector, expert en la matière et responsable de la reconnaissance faciale pour la police métropolitaine depuis 2019

**M. Rex NICHOLLS**, avocat, solicitor pour la police métropolitaine spécialisé dans la reconnaissance faciale, la protection des données et le droit

*South Wales Police* :

**M. Scott LLOYD**, chief inspector et responsable du projet RF de la SWP

*16 h 00 – 18 h 00* Entretien universitaire - ESRI

**Pr Peter FUSSEY**, University of Essex

*20 h 00* Diner à la Résidence de France

**Mme Catherine COLONNA**, ambassadrice de France au Royaume-Uni

**Mme Nathalie SKIBA**, attachée de sécurité intérieure

**Mme Estelle CROS**, magistrate de liaison

**Mme Minh-hà PHAM**, responsable du service culturel

- Vendredi 8 avril 2022 -

*10 h 00 – 12 h 00* Réunion avec les représentants du Home Office

**M. Jeremy JONES**, responsable politique au sein du département en charge de la biométrie et de la criminalistique

**M. Alex J.G. MACDONALD**, responsable politique au sein du département en charge de la biométrie et de la criminalistique

*12 h 30 – 15 h 00* Déjeuner de travail avec des représentants de l'Information Commissioner's Office (ICO)

**M. Anthony LUHMAN**, directeur « Enquêtes à haute priorité, Insight, Intelligence et Gestion des relations »

**M. James HAYWARD**, chef de groupe « Demandes de renseignements prioritaires »

# LISTE DES PERSONNES ENTENDUES PAR LA COMMISSION

**M. Cédric O**, Secrétaire d'État chargé de la transition numérique et des communications électroniques

# LISTE DES PERSONNES ENTENDUES PAR LES RAPPORTEURS

**M. Jean-Michel MIS**, député, auteur du rapport « *Pour un usage responsable et acceptable par la société des technologies de sécurité* »

**M. Renaud VEDEL**, coordonnateur national pour l'intelligence artificielle

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

**M. Paul HEBERT**, directeur adjoint de la conformité

**Mme Nacéra BEKHAT**, cheffe du service des affaires économiques, direction de la conformité

**M. Félicien VALLET**, ingénieur expert, service de l'expertise technologique, direction de la technologie et de l'innovation

**Défenseur des droits (DDD)**

**Mme Sarah BENICHOU**, adjointe au directeur de la promotion de l'égalité et de l'accès au droit

**M. Gaëtan GOLDBERG**, chargé de mission numérique, droits et libertés

**Mme France de SAINT-MARTIN**, conseillère parlementaire

**Conseil national du numérique**

**M. Jean CATTAN**, secrétaire général

**Comité national pilote d'éthique du numérique (CNPEN)**

**M. Claude KIRCHNER**, directeur

**Secrétariat général de la défense et de la sécurité nationale (SGDSN)**

**M. Nicolas DE MAISTRE**, directeur de la protection et de la sécurité de l'État

**Mme Catherine MUNSCH**, conseillère juridique

**M. Gwénaël JÉZÉQUEL**, conseiller du secrétaire général

**M. François MURGADELLA**, chef du pôle Développement technologies de sécurité

**Direction des libertés publiques et des affaires juridiques (DLPAJ) du ministère de l'intérieur**

**Mme Pascale LÉGLISE**, directrice

**M. Éric TISON**, sous-directeur des libertés publiques

**M. Cyriaque BAYLE**, adjoint au sous-directeur des libertés publiques

**Mme Léa QUIAU**, cheffe du bureau du droit des données et des nouvelles technologies à la sous-direction des libertés publiques

**Direction générale de la gendarmerie nationale (DGGN)**

**Colonel Joël DROMARD**, chargé de mission au pôle stratégique capacitaire de la direction des opérations et de l'emploi (DGGN – Issy-les-Moulineaux), officier de cohérence opérationnel sur les programmes relatifs aux fichiers

**Colonel Frédérick REHAULT**, chef de la division des fichiers au service central de renseignement criminel de la gendarmerie nationale (Pôle judiciaire de la gendarmerie nationale – Pontoise), directeur d'un programme relatif aux investigations biométrique

**Direction générale de la police nationale (DGPN)**

**M. Jérôme LEONNET**, directeur général adjoint de la police nationale

**Mme Adeline CHAMPAGNAT**, conseillère technologies au cabinet

**M. Jérôme PLANCHÉRIA**, pôle juridique du cabinet

**M. Alex GADRÉ**, conseiller juridique au cabinet

**Direction générale de la sécurité intérieure (DGSI)**

**M. Nicolas LERNER**, directeur général

**Mme Caroline BOUSSION**, conseillère juridique

**Préfecture de Police de Paris**

**M. Arnaud MAZIER**, directeur de l'innovation, de la logistique et des technologies (DILT)

**M. Thierry MARKWITZ**, sous-directeur des technologies à la DILT

**M. Philippe DALBAVIE**, conseiller chargé des affaires juridiques et parlementaires au cabinet du Préfet de police

**Pôle d'expertise de la réglementation numérique (PEReN)**

**M. Nicolas DEFFIEUX**, directeur

**M. Florent LABOY**, directeur adjoint

**M. Lucas VERNEY**, expert technique

**Direction générale des douanes et droits indirects (DGDDI)**

**M. Christophe CUIDARD**, sous-directeur adjoint du Réseau à la DGDDI

**Mme Claire-Jeanne TROQUET**, cheffe du bureau « Frontières, sécurité et sureté », sous-direction du Réseau à DGDDI

**M. Martin FLEURY**, chef de cabinet de la directrice générale

**RATP**

**M. Côme BERBAIN**, directeur de l'innovation

**M. John-David NAHON**, chargé des affaires parlementaires et institutionnelles

**M. Emmanuel BRIQUET**, juriste sûreté

**M. Fabrice SABOURIN**, chargé d'études sûreté

**SNCF**

**M. Jean-Franck BERTIN**, directeur de la direction prospective de la direction de la sûreté

**M. Nicolas DESPALLES**, chargé du Programme Vidéo Intelligente

**Mme Laurence NION**, conseillère parlementaire

**Mme Valentine POYLO**, chef du département Propriété intellectuelle – Protection des données

**Conseil national des barreaux (CNB)**

**Maître Laurence ROQUES**, présidente de la commission Libertés et droits de l'homme

**M. Charles RENARD**, chargé de mission affaires publiques

**Ligue des droits de l'homme**

**Mme Maryse ARTIGUELONG**, vice-présidente de la Ligue des droits de l'Homme et de la Fédération internationale des droits de l'Homme, responsable du groupe de travail « Libertés et technologies de l'information et de la communication »

**La Quadrature du net (LQDN)**

**M. Benoît PIÉDALLU**, membre

**M. Bastien LE QUERREC**, membre

**Amnesty International France**

**Mme Anne-Sophie SIMPERE**, chargée de plaidoyer – Programme Libertés

**AFNOR**

**M. Yves LE QUERREC**, président du Comité Stratégique AFNOR Information et Communication Numérique – La Banque Postale

**Mme Julie LATAWIEC**, responsable Développement Numérique

**Mme Marlène OUATTARA**, responsable de l'élaboration du Livre Blanc « Impacts et Attentes pour la Normalisation de la Reconnaissance Faciale »

**Alliance pour la Confiance Numérique (ACN)**

**M. Alban FÉRAUD**, vice-président – Identité numérique (Idemia)

**M. Yoann KASSIANIDES**, délégué général

**Idemia**

**M. Jean-Christophe FONDEUR**, directeur technique

**ID3 Technologies**

**M. Jean-Louis REVOL**, président

**M. Florian AYEL**, responsable du service Recherche au sein du département Solutions d'identité et de sécurité (SIS)

**Amazon France**

**M. Arnaud DAVID**, directeur des affaires publiques chez Amazon Web Services (AWS)

**Microsoft France**

**M. Hector DE RIVOIRE**, responsable des affaires gouvernementales

**M. Philippe BERAUD**, *national security officer*

**Représentation permanente de la France auprès de l'Union européenne (RPFUE)**

**M. Nicolas GONIAK**, conseiller pour les affaires intérieures

**Ville de Baltimore, États-Unis**

**Mme Lisa WALDEN**, conseillère en chef des Affaires policières du département juridique

**Personnalités qualifiées**

**M. Sébastien LE BELZIC**, journaliste, réalisateur du documentaire « *Ma femme a du crédit* »

**M. Olivier TESQUET**, journaliste, auteur

**Professeur Caroline LEQUESNE ROTH**, maître de conférences HDR en droit public à l'Université Côte d'Azur, directrice du Master II « Droit algorithmique et Gouvernance des données »

**Professeur Jean-Luc DUGELAY**, professeur à Eurecom Sophia-Antipolis

**Maître Arnaud DIMEGLIO**, avocat à la Cour, docteur en droit, titulaire des mentions de spécialisation en droit de la propriété intellectuelle, droit des nouvelles technologies, droit de l'informatique et de la communication

## LISTE DES CONTRIBUTIONS ÉCRITES

Commission nationale consultative des droits de l'homme (CNCDH)

Facebook (Meta)

IBM

Foot Unis

# COMPTE RENDU DE L'AUDITION DE M. CÉDRIC O, SECRÉTAIRE D'ÉTAT CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES COMMUNICATIONS ÉLECTRONIQUES

*(Mercredi 16 mars 2022)*

**M. François-Noël Buffet, président**. – La mission d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles a été créée par le bureau de la commission des lois en octobre 2020. Il s'agit d'une mission pluraliste, dont les rapporteurs sont MM. Marc-Philippe Daubresse, Arnaud de Belenet et Jérôme Durain.

En raison de l'ordre du jour législatif particulièrement chargé l'an dernier, la mission a commencé ses travaux il y a seulement quelques semaines. Elle s'est rendue à l'aéroport d'Orly, où lui ont été présentés le dispositif PARAFE et l'expérimentation actuellement menée par Aéroports de Paris (ADP) pour permettre l'enregistrement et l'embarquement des passagers sur la base de la reconnaissance faciale.

Cette mission avait été créée alors que le Gouvernement s'était prononcé, par votre voix, Monsieur le ministre, en faveur de la mise en place d'une expérimentation visant à évaluer l'usage de la reconnaissance faciale à la vidéosurveillance. Depuis, la Commission européenne a publié une proposition de règlement sur l'intelligence artificielle qui renouvellerait, si elle était adoptée, le cadre juridique applicable à la reconnaissance faciale.

Dans ce contexte, l'expérimentation annoncée a été abandonnée et il a été précisé que la sécurité des jeux Olympiques de 2024 serait assurée sans le recours à la reconnaissance faciale. Les autres expérimentations en la matière sont encore embryonnaires : on peut, d'une part, citer le projet Alicem pour ce qui est de l'authentification, qui consiste à vérifier qu'une personne est bien celle qu'elle prétend être. Sur le volet identification d'autre part, qui vise à retrouver une personne parmi un groupe d'individus, des expérimentations ont été conduites par la ville de Nice – où les rapporteurs se déplaceront ce jeudi – ou à l'occasion du tournoi de tennis de Roland-Garros. Pouvez-vous nous fournir de premiers éléments de bilan ?

L'usage de la reconnaissance faciale par la puissance publique suscite des interrogations légitimes en raison des risques induits pour les libertés publiques, notamment la possible fin de l'anonymat sur la voie publique. Nous avons déjà des exemples concrets. Certains pays tels que la Chine ont poussé la logique jusqu'au bout, avec une utilisation de la reconnaissance faciale dans le cadre de mécanismes de « crédit social » restreignant particulièrement les libertés. De plus, la fiabilité des algorithmes sous-jacents semble encore imparfaite : soit que leur usage débouche sur des

taux de faux positifs ou de faux rejets trop importants, soit que ces algorithmes présentent des biais discriminatoires.

Votre audition, qui intervient au début des travaux de notre mission d'information, vise donc à nous éclairer sur la position du Gouvernement quant au développement des usages de la reconnaissance faciale. Nous les observons actuellement, mais ont-ils vocation à prospérer ? Quels pourraient être les usages les plus pertinents ? Quelle est la position de la France quant à l'encadrement de la reconnaissance faciale envisagé par le règlement européen sur l'intelligence artificielle ?

Nos échanges font l'objet d'une retransmission vidéo en direct et en différé sur le site internet du Sénat.

**M. Cédric O, secrétaire d'État auprès du ministre de l'économie, des finances et de la relance et du ministre de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques**. – La question de la reconnaissance faciale est hautement politique et fait l'objet d'une intense attention médiatique, compte tenu de sa sensibilité. Notre cadre de régulation est constitué par le règlement général sur la protection des données (RGPD). À ce jour, le Gouvernement n'a pas de position arrêtée sur nos choix collectifs en matière de technologies. Il y a deux ou trois ans, j'avais souhaité des expérimentations pour nourrir un débat national ; malheureusement, ces expérimentations n'ont pas pu être menées et le débat n'a pas eu lieu : il reste donc devant nous et incombera au prochain gouvernement. Comme vous le savez, j'ai demandé à ne pas être renouvelé dans mes fonctions au-delà du mois d'avril : je puis donc vous faire part de mon appréciation personnelle.

Il s'agit d'un sujet hautement sensible, aux conséquences graves, le cas échéant. Notre débat est surdéterminé par l'exemple chinois, qui constitue bien entendu un contre-exemple absolu. La France et l'Europe luttent contre les dérives de l'utilisation de la reconnaissance faciale : le système de crédit social mis en place en Chine est à cet égard un anti-modèle. Je suis heureux qu'avec le RGPD et le futur règlement sur l'intelligence artificielle, cette possibilité soit explicitement exclue et que l'Europe ait pris les devants pour trouver son propre équilibre entre innovation et régulation.

Ce débat doit donc être dépassionné et nous permettre d'aller dans le détail des technologies, des cas d'usage et de l'encadrement, car l'éventail des possibles est extrêmement large. Il faut commencer par distinguer technologies d'authentification et d'identification : rien de comparable entre une technologie de déverrouillage d'un smartphone et des logiciels de vidéosurveillance qui identifient des personnes dans la rue. L'authentification est utilisée de manière volontaire : dès lors que des alternatives sont ménagées, ses enjeux politiques et éthiques sont moindres que dans le cas de l'identification.

En matière d'identification, les situations sont également très diverses. Doit-on considérer qu'une voiture autonome qui utilise un système de reconnaissance des comportements pour limiter le risque de collision fait usage de la reconnaissance faciale ? Il s'agit pourtant d'un système de recueil de données sans consentement exprès… Tout comme les systèmes d'aide auditive. Autre exemple : la Commission nationale de l'informatique et des libertés (CNIL) a arrêté l'expérimentation menées dans le métro parisien, grace à une solution élaborée par la société Datakalab, pour détecter le port du masque : s'agit-il de reconnaissance faciale ? C'est devenu un terme fourre-tout et certaines associations libertaires jouent sur cette psychose.

Notre débat doit comporter trois dimensions. Nous devons tout d'abord nous interroger sur l'adéquation entre la technologie et le cas d'usage : l'encadrement ne sera pas le même pour faire face à un risque terroriste ou pour déverrouiller un smartphone ; une gradation est nécessaire. Ensuite, prenons conscience que les protocoles techniques et technologiques sont aussi importants que ce qui est écrit dans la loi. Certains protocoles, par nature protecteurs de la vie privée, pourraient être validés pour certaines utilisations ; c'est ce que la CNIL appelle le *privacy by design*. Plus que la captation de la donnée, c'est son traitement qui doit nous intéresser ; autrement, une application maximaliste du RGPD pourrait conduire à interdire les systèmes d'analyse des comportements sur les véhicules autonomes… Enfin, il faut repenser l'encadrement et en débattre, afin de travailler notamment la question des contre-pouvoirs, et de l'acceptabilité et de la transparence de ces technologies.

Des expérimentations, validées par la CNIL, sont aujourd'hui possibles dans le cadre du RGPD, mais il s'agit d'une régulation horizontale qui n'a pas été pensée spécifiquement pour la reconnaissance faciale. D'où l'intérêt du prochain règlement sur l'intelligence artificielle. La France, en tant que présidente du Conseil de l'Union européenne, n'est pas censée avoir de position sur ce projet de règlement ; néanmoins, je puis vous dire que nous sommes à l'aise avec ce projet, même si le diable se cache souvent dans les détails ; la question de l'uniformité de son application aux entreprises européennes et extra-européennes sera essentielle. Nous avons du temps, mais la discussion promet d'être « touffue ».

**M. Marc-Philippe Daubresse, rapporteur**. – Doit-on rester dans une logique d'expérimentations ? Une loi est-elle nécessaire pour cadrer ces expérimentations, en liaison avec le nouveau règlement européen ? Ou doit-on laisser les éléments du puzzle actuel – RGPD, CNIL, prochain règlement européen – en l'état ?

Pourquoi le Gouvernement n'a-t-il pas retenu des dispositifs de reconnaissance faciale ou de détection des mouvements pour les jeux Olympiques de Paris de 2024 ? J'ai assisté aux jeux d'Atlanta : la sécurité y était remarquablement assurée. Quels dispositifs envisagez-vous pour assurer la sécurité des jeux de Paris ?

**M. Jérôme Durain, rapporteur**. – La société Clearview vient de proposer à l'Ukraine des logiciels de reconnaissance faciale humanitaires : de diaboliques intentions peuvent parfois prendre des allures d'ange…

Nos industriels ressentent une forte tension entre une réglementation européenne contraignante et le risque que des dispositifs plus performants soient développés par leurs concurrents. Nous risquons aussi d'être débordés par la technologie, car, on le sait, *code is law*. La puissance publique a-t-elle les moyens de ses contrôles ? Comment vérifier qu'il n'y a pas de détournements des cas d'usage ?

**M. Cédric O, secrétaire d'État**. – À titre personnel, il ne me semble pas souhaitable d'avoir deux débats au Parlement – d'abord sur le cadre applicable aux expérimentations, ensuite sur l'élaboration du cadre de droit commun –, sur un sujet aussi hautement inflammable.

Il faut d'abord des expérimentations, car la technologie évolue vite, mais l'identification ne fonctionne pas encore parfaitement et la sécurisation de l'authentification n'est pas non plus totalement garantie à ce stade. Nous avons donc besoin de multiplier les expérimentations, sous le regard du Parlement et de la société civile. Ensuite, nous aurons un débat parlementaire sur nos choix collectifs. Mais pourra-t-on mener de nouvelles expérimentations sans recourir à une nouvelle loi ? Vous serez peut-être amenés à avoir deux débats parlementaires, ce qui me semble sous-optimal, car le temps parlementaire est compté et parce que je doute de notre capacité à discuter de cette question deux fois à un an et demi d'intervalle.

La décision d'avoir recours à l'identification pour les jeux Olympiques de 2024 aurait dû être prise maintenant : le Gouvernement a choisi de ne pas le faire, compte tenu du contexte politique et de la sensibilité du sujet. Cela interdit donc de fait l'utilisation de dispositifs d'identification, mais ne devrait cependant pas nous empêcher d'avancer sur l'authentification de certains personnels pour l'accès aux sites olympiques, par exemple. Nous devrons donc trouver les moyens d'assurer la sécurité des jeux sans recourir à l'identification en temps réel. Cette question aurait nécessité un débat apaisé, ce qui est illusoire en période de campagne présidentielle… Je fais partie de ceux qui pensent qu'il ne faut pas avoir un débat avant le débat, d'autant que les expérimentations nous permettront d'être mieux documentés.

En matière de reconnaissance faciale, le consommateur et le citoyen n'adoptent pas toujours le même comportement : le citoyen se dit totalement opposé à la reconnaissance faciale, alors que le consommateur l'utilise sans même se soucier de la localisation de ses données.

N'oublions pas la question industrielle. À cet égard, le prochain règlement sur l'intelligence artificielle devra bien définir ce qui est interdit et ce qui est autorisé. Si nous interdisons à nos industriels tel ou tel algorithme, nous devrons être en mesure de fermer notre marché à toutes les sociétés

hors Europe qui auront développé des outils similaires avec un niveau de contrainte moindre. Je ne suis pas certain que nos partenaires européens y soient prêts. En outre, comment certifier ce qui se fait en Chine ?

L'Europe est légitime à poser un cadre si ce cadre s'applique à tous. C'est une question de politique commerciale. Souvenons-nous de l'application du RGPD, qui a créé des asymétries compétitives au détriment de nos acteurs européens.

La question du contrôle est au cœur de la régulation du numérique. Les moyens de la CNIL ont connu une augmentation significative et nous avons créé le pôle d'expertise de la réglementation numérique (PEReN) qui rassemble une vingtaine de compétences rares pouvant être sollicitées par l'État et les régulateurs. Je vous invite à aller les voir dans le cadre de votre mission : c'est très rassurant quant à la capacité de la puissance publique à appréhender de tels sujets.

**M. Jérôme Durain, rapporteur**. – La puissance publique ne se trouve-t-elle pas en conflit d'intérêts au regard de ses missions de sécurité et de défense ?

**M. Cédric O, secrétaire d'État**. – C'est un conflit d'intérêts auquel l'État est habitué. La question ne se pose pas dans les mêmes termes qu'il s'agisse d'antiterrorisme ou d'encadrement de pratiques commerciales quotidiennes. Les mécanismes de contrôle doivent être gradués en fonction du caractère plus ou moins intrusif du protocole. Le contexte joue aussi et nous devons pouvoir nous adapter, notamment en cas de guerre ou de conflit : on le voit actuellement en Ukraine avec l'utilisation des drones.

**Mme Marie Mercier**. – Je m'interroge sur la question centrale de la conservation des images, dont certaines sont peut-être stockées dans des *clouds* américains. Le Comité d'éthique pilote du numérique (CEPN) est-il impliqué pour étudier l'acceptabilité de cette conservation ? En particulier, qu'en est-il concernant les mineurs ?

**M. Cédric O, secrétaire d'État**. – La question de la conservation des données se pose en deux sens. Si cette conservation est trop longue, et si l'utilisation des images est illégitime, il est normal que votre attention soit attirée.

En revanche, un protocole qui n'utiliserait les données qu'à des fins de traitement immédiat, sans en conserver aucune, pourrait être moins régulé, à l'instar du système dont je parlais précédemment au sujet des voitures autonomes et des logiciels d'assistance à la conduite. Cette question est éminemment sensible.

Des règles existent déjà, mais elles sont différemment appliquées : l'encadrement du traitement des données des mineurs au sein du RGPD est extrêmement sévère.

Lors des trilogues européens, des conflits se font jour entre la protection des mineurs et les règles relatives à la protection des données. Il faut soit pouvoir identifier les premiers, et donc vérifier l'âge des utilisateurs, ce qui implique de stocker des données, soit traiter les données, comme les contenus consultés et les niveaux de langage utilisés, pour déterminer l'âge vraisemblable des utilisateurs.

Le sujet, qui devient de plus en plus important aux États-Unis comme en Europe, n'est pas simple. Hier, au sein du trilogue sur le DSA (*Digital Service Act*), nous nous sommes demandé s'il fallait interdire le traitement des données des mineurs. Le problème vient aussi du fait que, la plupart du temps, les mineurs ne déclarent pas qu'ils sont mineurs.

Les opérateurs auxquels nous interdirions l'utilisation des données des mineurs nous diraient que, pour identifier les mineurs, ils auraient besoin de connaître l'âge des utilisateurs et de stocker les réponses, à moins qu'ils ne puissent, en traitant les données, inférer l'âge des utilisateurs, ce à quoi la CNIL s'opposerait.

Les États-Unis s'orientent vers la deuxième possibilité, à savoir permettre d'inférer l'âge des utilisateurs. Frances Haugen, avec laquelle j'ai discuté, évoque dans les *Facebook Leaks* le fait qu'il est possible de déterminer, avec une marge d'erreur, l'âge des utilisateurs.

En Europe, nous sommes encore en train de tâtonner sur le sujet.

**M. Jérôme Durain, rapporteur**. – Pour toute une partie de la population, en particulier pour la jeunesse, il n'y a pas de transition numérique : les « numériques natifs » regardent des concerts de Travis Scott sur Fortnite et utilisent des outils que nous ne connaissons pas... Considérez-vous qu'un travail particulier doit être fait concernant les questions éthiques et pédagogiques ? La bataille est-elle déjà perdue, ou les questions se posent-elles autrement pour la dernière génération ?

Les alertes que nous percevons en tant que législateurs ne se posent peut-être pas pour les personnes concernées. Pensez-vous que nous sommes au bon niveau pour permettre la sensibilisation de la jeunesse sur ces questions ?

**M. Cédric O, secrétaire d'État**. – J'aurais tendance à nuancer vos affirmations. Dans le cadre de mes fonctions, j'ai travaillé sur la fracture numérique. La vision de la jeunesse comme maîtrisant l'ensemble des tenants et aboutissants des outils numériques est erronée. Si la plupart des membres de la jeune génération n'ont aucun problème pour utiliser TikTok, Snapchat ou Messenger, dès que l'on demande d'avoir une utilisation administrative ou normée des outils numériques, les choses sont bien différentes : une part importante de la jeunesse ne se connecte à internet que par les smartphones, et n'arrive pas à utiliser un ordinateur. La fracture numérique ne concerne pas que les personnes âgées.

Concernant l'équilibre entre l'expérience utilisateur et la protection des données, la sensibilité des jeunes n'est ni la mienne ni la vôtre. Les jeunes trouveraient sûrement inimaginable de trop favoriser la protection des données au détriment de l'expérience utilisateur.

Sont-ils pour autant suffisamment informés de la réalité des risques inhérents à l'utilisation intensive du numérique ? Souvent, lorsqu'ils deviennent majeurs et qu'ils recherchent un stage, ils s'aperçoivent que certaines photos compromettantes circulent sur internet. Le problème concerne aussi, malheureusement, leurs relations amoureuses. La sensibilisation à ces risques est donc extrêmement importante.

L'ensemble des candidats à l'élection présidentielle souhaite introduire le code à l'école. Mais il doit également être question des usages du numérique et de la grammaire des outils. Savoir comment coder devient indispensable dans le monde d'aujourd'hui ; mais le Conseil national du numérique a récemment souligné l'importance de l'apprentissage de la grammaire des outils numériques pour comprendre comment fonctionnent les fausses informations, la vie privée, ou la parentalité à l'heure numérique. Le futur ou la future Président de la République devra donc adopter une approche holistique pour déterminer le contenu de cet enseignement.

Je reviens sur un point soulevé par Mme Mercier. Le CEPN a vocation à devenir un élément important dans les mois qui viennent. Le Comité consultatif national d'éthique (CCNE) a été utile, même s'il n'a pas résolu tous les problèmes concernant la bioéthique. Certaines questions se poseront même d'ailleurs parfois à la croisée du numérique et de la biologie : il est possible que l'ADN devienne une future matière de stockage de données…

**M. François-Noël Buffet, président**. – La CNIL a pointé l'activité de Clearview. Peut-on apprécier la quantité d'usages illicites des dispositifs de reconnaissance faciale ?

**M. Cédric O, secrétaire d'État**. – Je répondrai clairement : assez difficilement. Les législateurs seront confrontés à un sujet important, qui recoupe le débat que nous avons eu concernant l'anonymat : sur internet, il suffit d'utiliser un VPN pour brouiller la localisation et être soumis à des règles différentes.

Cela ne signifie pas que rien n'est possible : le cadre législatif est extrêmement important. Nos capacités de régulation sont réelles à l'échelle européenne, car le marché est d'une taille suffisante pour déterminer des règles mondiales que les entreprises doivent suivre.

Par ailleurs, bien heureusement, tout le monde n'utilise pas un VPN dans sa vie de tous les jours.

La plasticité du monde numérique doit être prise en compte au moment de trouver les manières de réguler l'activité numérique.

Aujourd'hui, je pense que le recours à ces éléments de reconnaissance faciale est tout de même limité. Mais, notamment pour des utilisations de loisir ou de divertissement, les choses évoluent très vite, et nous pouvons très vite nous retrouver devant le fait accompli d'utilisations quotidiennes, sans pouvoir inverser le cours de la cascade.

**M. Marc-Philippe Daubresse, rapporteur**. – N'avez-vous jamais envisagé de trouver une parade aux VPN ? Le détournement d'adresses IP peut permettre des piratages ou de la diffamation électorale. Cela ne gêne personne que des sociétés proposent de détourner les procédures ?

**M. Cédric O, secrétaire d'État**. – La faisabilité des solutions est sujette à caution.

Je ne dis pas que l'utilisation des VPN est saine, mais le Parlement n'a, par exemple, jamais réussi à interdire Coyote, dont l'utilisation vise notoirement à détourner le droit. Je doute qu'il soit possible d'interdire les VPN.

**M. Marc-Philippe Daubresse, rapporteur**. – Coyote ne regardait que la question de la régulation de la vitesse. Concernant les VPN, les enjeux sont bien plus fondamentaux.

**M. Cédric O, secrétaire d'État**. – Oui, mais les limitations liées aux libertés publiques sont les mêmes.

**M. François-Noël Buffet, président**. – Monsieur le secrétaire d'État, je vous remercie de votre présence.