Lignes directrices sur la reconnaissance faciale

Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Convention 108

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Lignes directrices sur la reconnaissance faciale

Adoptées par le Comité consultatif
de la Convention pour la protection
des personnes à l'égard du traitement
automatisé des données à caractère
personnel (Convention 108)

Conseil de l'Europe

Édition anglaise :
Guidelines on facial recognition

Photo couverture : Shutterstock

Couverture et mise en page : Service de la production des documents et des publications (SPDP), Conseil de l'Europe

Imprimé dans les ateliers du Conseil de l'Europe

Table des matières

ORIENTATIONS À L'INTENTION DES LÉGISLATEURS ET DÉCIDEURS 7

Licéité 7

Nécessaire implication des autorités de contrôle 13

Certification 13

Sensibilisation 13

ORIENTATIONS À L'INTENTION DES DÉVELOPPEURS, DES FABRICANTS ET DES FOURNISSEURS DE SERVICES 15

Qualité des données et des algorithmes 15

Fiabilité des outils utilisés 16

Sensibilisation 16

Responsabilité 17

ORIENTATIONS À L'INTENTION DES ENTITÉS UTILISANT DES TECHNOLOGIES DE RECONNAISSANCE FACIALE 19

Légitimité du traitement des données et qualité des données 19

Sécurité des données 23

Responsabilité 23

Cadre éthique 26

DROITS DES PERSONNES CONCERNÉES 27

La reconnaissance faciale est une technologie de traitement automatique d'images numériques contenant les visages de personnes afin de les identifier ou de les authentifier à partir de modèles de visages.

La sensibilité des informations de nature biométrique a été reconnue explicitement avec l'inclusion des données identifiant une personne de façon unique au titre des catégories particulières de données de l'article 6 de la Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[1] (ci-après « Convention 108+ »).

Le contexte du traitement d'images est pertinent pour qualifier la nature sensible des données. Le traitement d'images n'implique pas, en général, un traitement de données sensibles, les images n'étant couvertes par la définition des données biométriques que lorsqu'elles sont traitées par un moyen technique spécifique permettant l'identification ou l'authentification unique d'un individu[2].

Ces lignes directrices traitent de l'utilisation des technologies de reconnaissance faciale, y compris les technologies de reconnaissance faciale à la volée. Les usages qui en sont faits sont variés et nombreux, certains pouvant porter de graves atteintes aux droits des personnes concernées. Les législations qui autorisent une large surveillance des personnes peuvent être considérées comme contraires au droit au respect de la vie privée[3].

L'intégration de technologies de reconnaissance faciale dans les systèmes de surveillance existants fait courir des risques sérieux aux droits au respect de la vie privée et à la protection des données à caractère personnel, ainsi qu'à d'autres droits fondamentaux puisque leur utilisation n'impose pas toujours que les personnes dont les données biométriques sont ainsi traitées en soient informées ou y coopèrent. C'est le cas par exemple avec la possibilité d'accéder à des images numériques de personnes sur internet.

---

1. Version consolidée de la convention modernisée, intégrant les changements introduits par le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 223), disponible à l'adresse suivante : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0.
2. Paragraphe 59 du rapport explicatif de la Convention 108+ disponible à l'adresse suivante : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac91b.
3. Déclaration du Comité des Ministres sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux, adoptée le 11 juin 2013, disponible à l'adresse suivante : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c801b.

Afin de prévenir de telles atteintes, les Parties à la Convention 108+ s'assureront que le développement et l'utilisation de la reconnaissance faciale respectent le droit à la vie privée et le droit à la protection des données personnelles, renforçant ainsi les droits de l'homme et les libertés fondamentales par la mise en œuvre des principes consacrés par la convention dans le contexte particulier des technologies de reconnaissance faciale.

Ces lignes directrices[4] fournissent un ensemble de mesures de référence que les gouvernements, les développeurs en reconnaissance faciale, les fabricants, les prestataires de services et entités utilisatrices devraient suivre et appliquer pour garantir que cette technologie ne nuise pas à la dignité humaine, aux droits de l'homme et aux libertés fondamentales de toute personne, notamment au droit à la protection des données à caractère personnel.

Ces lignes directrices ont une portée générale et couvrent l'utilisation des technologies de reconnaissance faciale dans les secteurs privé comme public. Elles n'excluent pas non plus que des mesures protectrices supplémentaires soient requises dans l'application des cadres légaux selon les cas d'utilisation particulière de la technologie. Elles présentent une évaluation des diverses utilisations dans différents secteurs en prenant en compte leurs finalités et leur impact potentiel sur le droit à la protection des données et d'autres droits fondamentaux.

Dans ces lignes directrices, les « finalités d'application de la loi » incluent la prévention, les enquêtes et les poursuites de crimes et l'exécution des peines. Cela comprend aussi le maintien de l'ordre par la police (ci-après appelé « finalités d'application de la loi »).[5] L'utilisation du libellé « autorités chargées de l'application de la loi » peut être comprise comme couvrant plus largement les services du procureur général et/ou d'autres organes publics et/ou privés autorisés par la loi à traiter des données à caractère personnel pour les mêmes finalités (ci-après dénommées « autorités chargées de l'application de la loi »).

Rien dans ces lignes directrices ne saurait être interprété comme excluant ou limitant les dispositions de la Convention 108[6]. Les présentes lignes directrices tiennent également compte des nouvelles garanties de la Convention 108+.

4. Ces lignes directrices sont fondées sur le rapport de Sandra Azria et Frédéric Wickert « La reconnaissance faciale : état de lieux et enjeux » de 2019, disponible à l'adresse suivante : https://rm.coe.int/t-pd-2019-05rev-rapport-reconnaissance-faciale-fr-2-/168098d305.
5. Les finalités d'application de la loi correspondent aux « finalités de police » dans le Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police (T-PD(2018)01), Comité consultatif de la Convention 108, disponible à l'adresse : https://rm.coe.int/t-pd-201-01-guide-pratique-sur-lutilisation-de-donnees-a-caractere-per/16807927d6.
6. Évidemment, pour les Parties à la Convention qui sont États membres du Conseil de l'Europe, rien dans ces lignes directrices ne peut, en outre, être interprété comme excluant ou limitant les dispositions de la Convention européenne des droits de l'homme (STE n° 5).

Orientations à l'intention des législateurs et décideurs

Licéité

Comme le prévoit l'article 6 de la Convention 108+, le traitement de catégories particulières de données, telles que les données biométriques, n'est autorisé que s'il repose sur une base juridique appropriée et si des garanties complémentaires et appropriées sont inscrites dans la loi nationale. Ces garanties doivent être adaptées aux risques encourus et aux intérêts, droits et libertés à protéger.

Dans certaines législations[7], l'interdiction de ce traitement est une règle et sa mise en œuvre n'est autorisée qu'à titre exceptionnel, dans des cas spécifiques (par exemple, avec le consentement explicite des personnes, pour protéger leurs intérêts vitaux ou lorsque le traitement est nécessaire en raison d'un intérêt public prépondérant) et sous réserve de garanties correspondant aux risques encourus.

La nécessité d'utiliser des technologies de reconnaissance faciale doit être évaluée en même temps que la proportionnalité à la finalité visée et son impact sur les droits des personnes concernées.

Les différents cas d'utilisation doivent être classés par catégorie et un cadre juridique applicable au traitement de données biométriques par le biais de la reconnaissance faciale devrait être mis en place. Un tel cadre juridique devrait, en fonction de chaque utilisation différente, notamment traiter :

- de l'explication détaillée de l'utilisation spécifique et de la finalité poursuivie ;
- de la fiabilité minimale et de la précision[8] de l'algorithme employé ;
- de la durée de conservation des photos utilisées ;
- de la possibilité de contrôler ces critères ;
- de la traçabilité du processus ;
- des garanties.

7. Voir l'article 9 du Règlement général sur la protection des données de l'Union européenne (RGPD, Règlement (UE) 2016/679 du 27 avril 2016).
8. La précision de l'algorithme peut être exprimée par une évaluation des erreurs faux positifs ou faux négatifs produites par le logiciel.

Limitation stricte de certaines utilisations par la loi

Le niveau d'intrusion de la reconnaissance faciale et l'atteinte aux droits à la vie privée et à la protection des données qui en découle vont varier en fonction de l'utilisation particulière qui en sera faite et il y aura des cas où la législation nationale devra limiter strictement son utilisation, voire l'interdire complètement, lorsque la décision aura été prise dans le cadre d'un processus démocratique.

Dans les environnements non contrôlés[9], le recours aux technologies de reconnaissance faciale à la volée devrait être soumis à un débat démocratique comprenant la possibilité d'un moratoire en attendant une analyse complète du fait de son caractère intrusif pour la vie privée et la dignité des personnes, associé à un risque d'impact préjudiciable sur d'autres droits de l'homme et libertés fondamentales.[10]

L'utilisation de la reconnaissance faciale dans le seul but de déterminer la couleur de la peau, les convictions religieuses ou autres convictions, le sexe, l'origine raciale ou ethnique, l'âge, l'état de santé ou la condition sociale d'une personne devrait être interdite à moins que des garanties appropriées soient prévues par la loi afin de prévenir tout risque de discrimination.[11]

De même, la reconnaissance des affects[12] peut également être effectuée par le biais des technologies de reconnaissance faciale pour prétendument détecter les traits de personnalité, les sentiments profonds, la santé mentale ou l'engagement des travailleurs à partir d'images des visages. Recourir à la reconnaissance de l'affect, par exemple pour le recrutement du personnel, ou l'accès à l'assurance, ou encore à l'éducation peut présenter des risques très préoccupants, au niveau tant individuel que sociétal, et devrait être interdit.

9. La notion d'« environnement non contrôlé » couvre les lieux librement accessibles aux personnes, qu'elles peuvent aussi traverser, y compris les espaces publics et quasi publics tels que les centres commerciaux, les hôpitaux ou les écoles.
10. Voir les Lignes directrices sur l'intelligence artificielle et la protection des données disponibles à l'adresse : https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b8.
11. Elle pourrait par exemple être autorisée pour un projet de recherche médicale, sous réserve de garanties appropriées inscrites dans la loi.
12. La reconnaissance des affects est l'utilisation de la technologie pour tenter d'identifier ou de classifier les émotions humaines.

Base juridique dans différents contextes

Le cadre juridique applicable au traitement de données biométriques par le biais de la reconnaissance faciale devrait aborder et prendre en compte, outre les éléments figurant à la partie 1 :

- les différentes phases de l'utilisation des technologies de reconnaissance faciale, y compris les phases de création et de déploiement des bases de données ;
- les secteurs dans lesquels ces technologies sont utilisées ; le caractère intrusif de certains types de technologies de reconnaissance faciale, comme le fait qu'il s'agisse de reconnaissance faciale à la volée, ou non, tout en fournissant des indications claires sur leur licéité.

Intégration des images numériques aux technologies de reconnaissance faciale

Les législateurs et les décideurs veilleront à ce que les images disponibles en format numérique ne puissent pas être traitées pour en extraire des modèles biométriques[13], ou pour être intégrées dans des systèmes biométriques, afin de reconnaître la personne figurant sur les images numériques, sans base juridique spécifique pour le nouveau traitement lorsque ces images ont été capturées à d'autres fins (à partir de médias sociaux par exemple).

Comme l'extraction de modèles biométriques à partir d'images numériques implique le traitement de données sensibles, il convient de sécuriser la base juridique éventuelle envisagée ci-dessous qui varie selon les secteurs et les utilisations.

Plus précisément, utiliser des images numériques qui ont été téléchargées à partir d'internet, y compris sur les médias sociaux ou sur des sites de gestion de photos en ligne, ou qui ont été capturées via des caméras de vidéosurveillance, ne peut être considéré comme licite au seul motif que ces données personnelles ont été rendues manifestement disponibles par les personnes concernées.

Les législateurs et les décideurs devraient veiller à ce que les bases de données d'images numériques existantes, initialement utilisées à d'autres fins, ne puissent servir à extraire des modèles biométriques et à les intégrer dans des systèmes biométriques que lorsque cela est nécessaire pour des finalités

13. Un modèle biométrique est une représentation numérique des caractéristiques uniques qui ont été extraites d'un échantillon biométrique et sont stockées dans une base de données biométriques.

légitimes prépondérantes, et que cela est prévu par la loi et absolument nécessaire et proportionné à ces finalités (d'application de la loi ou médicales, par exemple).

Utilisation des technologies de reconnaissance faciale dans le secteur public

En règle générale, le consentement ne devrait pas être le fondement juridique utilisé pour la reconnaissance faciale effectuée par les autorités publiques compte tenu du déséquilibre des pouvoirs entre les personnes concernées et ces autorités. Pour la même raison, le consentement ne devrait pas, en règle générale, être le fondement juridique utilisé lorsque la reconnaissance faciale est appliquée par des entités privées autorisées à accomplir des tâches similaires à celles des autorités publiques.

La licéité de l'utilisation des technologies de reconnaissance faciale sera fondée sur les finalités du traitement biométrique tel que prévu par la loi et les garanties nécessaires complétant la Convention 108+.

Législateurs et décideurs doivent fixer des règles spécifiques pour le traitement biométrique par le biais des technologies de reconnaissance faciale pour des finalités d'application de la loi. Elles garantiront que ces utilisations soient absolument nécessaires et proportionnées à ces finalités et prescriront les garanties nécessaires à fournir.

Autorités chargées de l'application de la loi

Le traitement des données biométriques par le biais des technologies de reconnaissance faciale à des fins d'identification dans un environnement contrôlé[14] ou non contrôlé devrait, en règle générale, être limité à des finalités d'application de la loi. Il devrait être effectué uniquement par les autorités compétentes en matière de sécurité.

Les lois peuvent prévoir différents tests de nécessité et de proportionnalité selon que l'objectif est la vérification ou l'identification, compte tenu des risques potentiels pour les droits fondamentaux et pour autant que les images des personnes soient légalement collectées.

Aux fins d'identification, l'absolue nécessité et la proportionnalité doivent être respectées tant dans la création de la base de données (liste de surveillance)

14. La notion d'« environnement contrôlé » couvre les cas dans lesquels la technologie biométrique ne peut être utilisée qu'avec la participation de la personne concernée.

que dans le déploiement des technologies de reconnaissance faciale (à la volée) dans un environnement non contrôlé.

Les lois devraient prévoir des paramètres et des critères clairs auxquels les autorités chargées de l'application de la loi devraient adhérer lors de la création de bases de données (listes de surveillance) dans le cadre de finalités d'application de la loi spécifiques, légitimes et explicites (par exemple, soupçon d'infraction grave ou risque pour la sécurité publique).

Compte tenu du caractère intrusif de ces technologies, dans la phase de déploiement de technologies de reconnaissance faciale à la volée dans des environnements non contrôlés, la loi doit garantir que les autorités chargées de l'application de la loi démontrent que divers facteurs, notamment le lieu et le moment du déploiement de ces technologies, justifient l'absolue nécessité et la proportionnalité des utilisations.

Autres autorités publiques

Les législateurs et les décideurs établiront des règles spécifiques pour le traitement biométrique par les technologies de reconnaissance faciale pour d'autres intérêts publics substantiels par des autorités publiques qui ne poursuivent pas des finalités d'application de la loi.

Les lois peuvent prévoir différents tests de nécessité et de proportionnalité selon que l'objectif est la vérification ou l'identification, compte tenu des risques potentiels pour les droits fondamentaux et pour autant que les images des personnes soient légalement collectées.

Compte tenu du caractère potentiellement intrusif de ces technologies, législateurs et décideurs doivent veiller à ce qu'une base légale explicite et précise pour le traitement des données biométriques fournisse les garanties nécessaires. Cette base légale devra comprendre l'absolue nécessité et la proportionnalité de leur utilisation et prendre en compte la vulnérabilité des personnes concernées ainsi que la nature de l'environnement dans lequel ces technologies sont utilisées à des fins de vérification.

Par exemple, assurer la sécurité dans des environnements contrôlés ou non contrôlés, y compris les écoles ou autres bâtiments publics, ne devrait pas, en règle générale, être considéré comme absolument nécessaire et proportionné lorsque des mécanismes moins intrusifs existent.

Utilisation des technologies de reconnaissance faciale dans le secteur privé

L'utilisation des technologies de reconnaissance faciale par des entités privées autres que celles autorisées à accomplir des tâches similaires à celles des autorités publiques, exige, conformément à l'article 5 de la Convention 108+, le consentement explicite, spécifique, libre et éclairé des personnes concernées dont les données biométriques sont traitées.

Compte tenu de l'exigence d'un tel consentement, l'utilisation des technologies de reconnaissance faciale ne peut avoir lieu que dans des environnements contrôlés à des fins de vérification, d'authentification ou de catégorisation[15].

En fonction de la finalité, une attention particulière doit être accordée à la qualité du consentement explicite de la personne concernée lorsqu'il constitue la base juridique du traitement.

Pour garantir que le consentement est donné librement, les personnes concernées devraient se voir offrir des solutions alternatives à l'utilisation des technologies de reconnaissance faciale (par exemple, l'utilisation d'un mot de passe ou d'un badge d'identification) mais l'alternative proposée devrait aussi être facile à utiliser car, si elle semblait trop longue ou compliquée par rapport à la technologie de reconnaissance faciale, le choix ne serait pas véritable.

Si le consentement est donné pour une finalité spécifique, les données personnelles ne devraient pas être traitées d'une manière incompatible avec cette finalité. De même, en cas de divulgation de données à un tiers, cette divulgation devrait également être soumise à un consentement particulier.

Les entités privées ne doivent pas déployer de technologies de reconnaissance faciale dans des environnements non contrôlés tels que des centres commerciaux, spécialement pour identifier des personnes présentant un intérêt, à des fins de marketing ou de sécurité privée.

Le fait de traverser un environnement où les technologies de reconnaissance faciale sont utilisées ne peut être considéré comme un consentement explicite.

15. La catégorisation biométrique signifie « le processus qui consiste à établir si les données biométriques d'un individu appartiennent à un groupe ayant une caractéristique prédéfinie afin de prendre une mesure spécifique ».

Nécessaire implication des autorités de contrôle

Conformément à l'article 15, paragraphe 3, de la Convention 108+, les autorités de contrôle doivent être consultées sur toute proposition de mesure législative ou administrative impliquant le traitement de données à caractère personnel par le biais des technologies de reconnaissance faciale. Il est nécessaire d'associer systématiquement les autorités de contrôle et, en particulier, de les consulter sur toute expérimentation ou projet de déploiement.

Ces autorités devront ainsi être consultées systématiquement et préalablement aux projets envisagés. De même, elles devraient avoir accès aux évaluations d'impact réalisées ainsi qu'à tous les audits, rapports et analyses effectués dans ce cadre.

Législateurs et décideurs devraient assurer une coopération efficace entre les différentes autorités de contrôle qui surveillent les divers aspects de ces traitements de données si d'autres autorités sont responsables de veiller à la conformité de ces activités de traitement avec la loi.

Certification

Législateurs et décideurs devraient faire appel à différents mécanismes pour garantir la responsabilité des développeurs, des fabricants, des fournisseurs de services ou des entités qui utilisent ces technologies.

La mise en place d'un mécanisme de certification indépendant et qualifié en matière de reconnaissance faciale et de protection des données pour démontrer la pleine conformité des traitements effectués serait un élément essentiel pour renforcer la confiance des utilisateurs.

Une telle certification pourrait être mise en œuvre selon le domaine d'application de l'intelligence artificielle utilisée par la technologie de reconnaissance faciale : un type pour catégoriser les structures (conception de l'algorithme, intégration de l'algorithme, etc) et un autre pour catégoriser les algorithmes (reconnaissance de l'ordinateur, recherche intelligente, etc.).

Sensibilisation

La sensibilisation des personnes concernées et la compréhension par le grand public des technologies de reconnaissance faciale et de leur impact sur les droits fondamentaux devraient être activement soutenues par des activités accessibles et pédagogiques.

L'idée est de donner accès à des concepts simples qui pourraient alerter les personnes concernées avant qu'elles décident d'utiliser une technologie de reconnaissance faciale, les aider à comprendre ce que signifie l'utilisation de données sensibles telles que les données biométriques et comment fonctionne la reconnaissance faciale ainsi que les alerter sur les dangers potentiels, notamment en cas d'utilisation abusive.

Législateurs et décideurs devraient faciliter la participation du public dans le développement et l'utilisation de ces technologies ainsi que dans la mise à disposition de garanties adéquates pour protéger les droits fondamentaux en jeu lors de l'utilisation des technologies de reconnaissance faciale.

Orientations à l'intention des développeurs, des fabricants et des fournisseurs de services

Cette partie des lignes directrices porte spécifiquement sur les questions liées aux phases de développement et de fabrication des technologies de reconnaissance faciale. Lorsque les développeurs, les fabricants et les prestataires de services traitent des données biométriques pour leurs propres besoins au cours des phases de développement, ils seront en outre concernés par la partie III des lignes directrices sur les entités utilisant cette technologie.

Qualité des données et des algorithmes

Représentativité des données utilisées

Comme d'autres instruments juridiques applicables, la Convention 108+ prévoit, dans son article 5, une obligation d'exactitude des données. C'est pourquoi les développeurs et les fabricants de technologies de reconnaissance faciale, tout comme les organisations qui les utilisent, devront prendre les mesures nécessaires pour garantir que les données de reconnaissance faciale sont exactes. En particulier, ils devront éviter les erreurs d'étiquetage en testant suffisamment leurs systèmes et en identifiant et éliminant les disparités dans la précision, notamment en ce qui concerne les variations démographiques de la couleur de la peau, l'âge et le sexe, et éviter ainsi toute discrimination involontaire.

En outre, afin de garantir à la fois la qualité des données et l'efficacité des algorithmes, ces derniers devront être développés à partir d'ensembles de données synthétiques basés sur des photos suffisamment diverses d'hommes et de femmes, de couleurs de peau et de morphologies différentes, de tous âges et sous différents angles de prise de vue. Des procédures de retour en arrière devraient être prévues en cas de défaillance du système si les caractéristiques physiques ne correspondent pas aux normes techniques.

Les données biométriques qui révèleraient inutilement mais inévitablement d'autres données sensibles telles que des informations sur un type de maladie ou de handicap physique devraient être soumises à des garanties complémentaires appropriées.

Durée de vie des données

Un système de reconnaissance faciale nécessite un renouvellement périodique des données (photos des visages à reconnaître) pour entraîner et améliorer l'algorithme utilisé.

Chaque algorithme a un pourcentage de fiabilité de reconnaissance, tant lors de son développement que de son utilisation. Il semble donc important de dater et d'enregistrer ce pourcentage pour suivre son évolution. Si sa fiabilité se détériore, il faudra renouveler les photos utilisées pour l'entraînement du système et donc en obtenir de plus récentes. Cela permettra également d'éviter les conséquences des changements sur les visages (dus au vieillissement, aux accessoires – piercing ou autres – ou à d'autres modifications).

Ces relevés de pourcentage de fiabilité pourraient être facilement mis à la disposition des personnes ou des clients intéressés ou entités ayant recours aux technologies de reconnaissance faciale, sous la forme d'un tableau de bord par exemple, pour faciliter leur choix d'acquisition et de déploiement d'une technologie spécifique.

Fiabilité des outils utilisés

La fiabilité des outils utilisés dépend de l'efficacité de l'algorithme. Cette efficacité dépend de différents facteurs, tels que : faux positifs, faux négatifs, performances sous différents éclairages, fiabilité lorsque les visages sont détournés de l'appareil photo, impact des accessoires recouvrant les visages.

Étant donné que l'utilisation d'un système de reconnaissance faciale pourrait avoir des conséquences négatives très importantes pour une personne, le meilleur niveau de fiabilité possible devrait être assuré.

Sensibilisation

Les entreprises qui développent et vendent des technologies de reconnaissance faciale devraient prendre des mesures raisonnables – par exemple, émettre des recommandations et des conseils – pour aider les entités qui utilisent

leur technologie à respecter transparence et vie privée (en leur fournissant des éléments de langage pour leur politique de protection de la vie privée ou en recommandant une signalisation claire et facile à comprendre indiquant qu'une technologie de reconnaissance faciale est déployée dans un espace particulier).

Responsabilité

Les entreprises qui développent et vendent des technologies de reconnaissance faciale devraient adopter des mesures spécifiques visant à garantir la conformité des traitements avec les principes de protection des données telles que :

- intégrer la protection des données dans la conception et l'architecture des produits et services de reconnaissance faciale, ainsi que dans les systèmes informatiques internes et prévoir l'utilisation d'outils spécialisés incluant la suppression automatique des données brutes après extraction des modèles biométriques ;
- offrir un certain niveau de flexibilité dans la conception de ces technologies afin d'adapter les garanties techniques en tenant compte des principes de limitation de la finalité, de minimisation des données et de limitation de la durée du stockage ;
- mettre en œuvre un processus de révision interne destiné à identifier et à atténuer l'impact potentiel sur les droits et les libertés fondamentales avant que les technologies de reconnaissance faciale soient mises à disposition ;
- intégrer une approche de la protection des données dans leurs pratiques organisationnelles, notamment avec un personnel spécialisé, une formation des employés au respect de la vie privée et par des études d'impact sur la protection des données lors du développement ou de la modification de produits et services de reconnaissance faciale.

Orientations à l'intention des entités utilisant des technologies de reconnaissance faciale

Les entités[16] doivent se conformer à tous les principes et dispositions applicables en matière de protection des données lorsqu'elles traitent des données biométriques dans le cadre de leur utilisation des technologies de reconnaissance faciale. Elles doivent être en mesure de démontrer que cette utilisation est absolument nécessaire et proportionnée dans le contexte spécifique de leur utilisation et qu'elle n'interfère pas avec les droits des personnes concernées.

Les entités peuvent se prévaloir des exceptions prévues par la législation applicable conformément à l'article 11 de la Convention 108+ (qui stipule que toute exception doit être prévue par la loi, poursuivre un but légitime spécifique, respecter l'essence des droits et libertés fondamentales et constituer une mesure nécessaire et proportionnée dans une société démocratique).

Les entités qui utilisent les technologies de reconnaissance faciale doivent veiller à ce que l'utilisation volontaire de la technologie n'ait pas d'impact sur les personnes qui viendraient à entrer en contact avec elle non intentionnellement.

Légitimité du traitement des données et qualité des données

Les entités s'appuieront sur des bases juridiques différentes selon leurs secteurs et les finalités de l'utilisation des technologies de reconnaissance faciale mentionnées dans la partie I.

16. Dans cette partie des lignes directrices, le terme « entités » recouvre les responsables du traitement des données et, le cas échéant, les sous-traitants, dans le secteur tant public que privé.

Transparence et loyauté

Les technologies de reconnaissance faciale pouvant être utilisées sans la coopération des personnes concernées ni leur volonté, la transparence et la loyauté du traitement sont de la plus haute importance et devront être dûment prises en compte par les entités qui y ont recours.

Les entités devront fournir toutes les informations nécessaires sur le traitement, comme stipulé par l'article 8 de la Convention 108+.

Les facteurs qui détermineront si la transparence est assurée comprennent, par exemple, les informations données aux personnes, le contexte de la collecte, les attentes raisonnables quant à la manière dont les données seront utilisées, si la reconnaissance faciale est simplement une caractéristique d'un produit ou d'un service ou une partie intégrante du service lui-même. Les personnes devront également être informées de la manière dont la collecte, l'utilisation ou le partage des données de reconnaissance faciale est susceptible de les affecter, en particulier lorsque ces données concernent des personnes en situation de vulnérabilité. En particulier, les droits et les recours juridiques dont bénéficient les personnes concernées doivent également être indiqués.

Les politiques de protection de la vie privée en matière de reconnaissance faciale ou le matériel d'information concernant les technologies devraient inclure, outre les informations prévues à l'article 8 de la Convention 108+, les informations suivantes[17] :

- si et dans quelle mesure les données de reconnaissance faciale peuvent être transmises à des tiers (et, le cas échéant, des informations sur l'identité des partenaires contractuels tiers qui reçoivent les données dans le cadre de la fourniture du produit ou du service) ;
- la conservation, la suppression ou la désidentification des données de reconnaissance faciale ;
- les points de contact mis à la disposition des particuliers pour leur permettre de poser des questions sur la collecte, l'utilisation et le partage des données de reconnaissance faciale ;

17. Sur ce point, voir les recommandations du Forum sur l'avenir de la protection de la vie privée *(Future of Privacy Forum)* Privacy principles for facial recognition technology in commercial applications disponible à l'adresse : https://fpf.org/2018/09/20/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/.

- lorsque les pratiques de collecte, d'utilisation et de partage changent de manière significative, les entités doivent mettre à jour leur politique de protection de la vie privée ou rendre publics ces changements à la lumière de leur contexte et de son impact sur les personnes.

Au cas où les bases de données sont constituées par les autorités chargées de l'application de la loi à des fins d'identification ou de vérification, l'obligation de transparence peut être proportionnellement limitée pour ne pas porter préjudice à leurs objectifs, conformément à l'article 11 de la Convention 108+ et sous réserve de ses exigences.

Lorsque les technologies de reconnaissance faciale à la volée sont déployées dans un environnement non contrôlé, les autorités chargées de l'application de la loi peuvent adopter une approche par étape pour fournir les informations nécessaires aux personnes concernées qui passent par cet environnement.

Dans la première étape, l'information contiendra les éléments lisibles et intelligibles nécessaires concernant la finalité du traitement, l'autorité qui utilise la technologie, la durée du traitement et le périmètre concerné et sera disposée à proximité du lieu où ces technologies sont déployées.

Dans la deuxième étape, l'information, affichée aux points d'entrée du lieu de déploiement, fournira toutes les indications nécessaires requises conformément à l'article 8 de la Convention 108+.

L'utilisation secrète des technologies de reconnaissance faciale à la volée par les autorités chargées de l'application de la loi ne pourrait être possible que si elle est absolument nécessaire et proportionnée pour prévenir un risque imminent et important pour la sécurité publique, qui doit être documenté avant cette utilisation.

Limitation de la finalité, minimisation des données et limitation de la durée de conservation

Les données à caractère personnel faisant l'objet d'un traitement sont collectées pour des finalités explicites, déterminées et légitimes et ne sont pas traitées de manière incompatible avec ces finalités, conformément à l'article 5, paragraphe 4, de la Convention 108+.

En outre, avant tout traitement ultérieur, les entités devront examiner si les finalités du nouveau traitement sont compatibles avec les finalités initialement définies. Dans le cas contraire, le nouveau traitement nécessitera une base juridique distincte.

Les entités doivent se conformer au principe de minimisation des données qui exige que seules les informations requises soient traitées et non toutes les informations dont elles disposent.

Les entités doivent également fixer une période de conservation qui ne peut excéder ce qui est nécessaire à la finalité spécifique du traitement et garantir la suppression des modèles biométriques une fois cette finalité atteinte. Lors de la détermination de cette période, la nature biométrique des données à caractère personnel doit être prise en compte.

Dans le cadre du déploiement des technologies de reconnaissance faciale à la volée, les entités doivent en outre veiller à ce que des délais de conservation différents s'appliquent aux diverses phases du traitement :

- s'il n'y a pas de correspondance entre les modèles biométriques, le modèle biométrique des personnes passant dans un environnement non contrôlé ne peut être conservé et doit être automatiquement supprimé ;
- s'il y a une concordance, les modèles biométriques peuvent être conservés pendant une durée strictement limitée prévue par la loi assortie des garanties nécessaires et les rapports de concordance comprenant des données à caractère personnel peuvent également être conservés pendant une durée limitée ;
- et, dans tous les cas, une fois atteinte la finalité pour laquelle les technologies de reconnaissance faciale à la volée ont été déployées, les listes de surveillance et les modèles biométriques seront détruits.

Exactitude

Les entités doivent veiller à ce que les modèles biométriques et les images numériques soient exacts et tenus à jour. Par exemple, la qualité des images et des modèles biométriques contenus dans les listes de surveillance doit être vérifiée afin d'éviter d'éventuelles fausses correspondances, car des images de mauvaise qualité peuvent entraîner une augmentation du nombre d'erreurs. Cela est directement lié aux sources des images compilées dans la liste de surveillance qui exigent le respect absolu des principes de protection des données, tel que le principe de limitation de la finalité.

En cas de fausses correspondances, les entités prendront toutes les mesures raisonnables pour les corriger à l'avenir et garantir l'exactitude des images numériques et des modèles biométriques.

Sécurité des données

Toute faille dans la sécurité des données peut avoir des conséquences particulièrement graves pour les personnes concernées puisqu'une divulgation non autorisée de données sensibles ne peut être corrigée.

Des mesures de sécurité robustes, aux niveaux tant technique qu'organisationnel, devraient donc être mises en place pour protéger les données de reconnaissance faciale et les jeux d'images contre la perte et un accès ou une utilisation non autorisé de ces données à toutes les étapes du traitement, que ce soit lors de la collecte, de la transmission ou de la conservation.

Les entités prendront des mesures pour prévenir les attaques spécifiques aux technologies, y compris les attaques de présentation et les attaques de morphing.

Toute violation de la sécurité des données susceptible de porter gravement atteinte aux droits et aux libertés fondamentales de la personne concernée doit être notifiée à l'autorité de contrôle et, le cas échéant, aux personnes concernées.

Les mesures de sécurité devraient évoluer dans le temps et en fonction de l'évolution des menaces et des vulnérabilités identifiées. Elles devraient également être proportionnées à la sensibilité des données, au contexte dans lequel une technologie de reconnaissance faciale spécifique est utilisée et à ses finalités, à la probabilité qu'elle nuise aux personnes, ainsi qu'à d'autres facteurs pertinents.

Des pratiques strictes de conservation et d'élimination des données de reconnaissance faciale, fondées sur des procédures sûres, avec des périodes de conservation les plus courtes possibles, contribuent également à réduire les risques d'atteinte à la sécurité.

Responsabilité

Les entités prendront toutes les mesures appropriées pour se conformer à leurs obligations et pour être en mesure de démontrer que le traitement des données sous leur contrôle est conforme à ces obligations, comme le prévoit l'article 10 de la Convention 108+.

Les mesures organisationnelles suivantes doivent être prises en compte par les entités utilisant les technologies de reconnaissance faciale :

- la mise en œuvre de politiques, de procédures et de pratiques transparentes afin de garantir que la protection des droits des personnes concernées sous-tend l'utilisation des technologies de reconnaissance faciale ;
- la publication de rapports de transparence sur l'utilisation spécifique des technologies de reconnaissance faciale ;
- la mise en place et l'élaboration de programmes de formation et de procédures d'audit pour les personnes chargées du traitement des données de reconnaissance faciale ;
- la création de comités de révision internes chargés d'évaluer et d'approuver tout traitement impliquant des données de reconnaissance faciale ;
- l'extension contractuelle aux prestataires de services tiers, aux partenaires commerciaux ou à d'autres entités utilisant la technologie de reconnaissance faciale des exigences applicables (et un refus d'accès aux tiers qui ne s'y conformeraient pas) ;
- dans le secteur public : contraintes d'évaluation préalable dans les procédures de marchés publics avec les fournisseurs d'outils de reconnaissance faciale, évaluation des niveaux minimaux de performance en termes de précision, notamment en ce qui concerne les finalités d'application de la loi.

Les entités prendront les mesures techniques nécessaires pour garantir la qualité des données biométriques en suivant les normes techniques convenues au niveau international, en fonction du contexte dans lequel elles sont utilisées.

Les entités qui utilisent des technologies de reconnaissance faciale devraient veiller à ce que les intervenants humains continuent de jouer un rôle décisif dans les actions prises à partir des résultats de ces technologies. Elles devraient adopter des mesures organisationnelles pour contrôler les intervenants humains qui prennent des décisions pouvant avoir un impact significatif sur les personnes.

Analyse d'impact sur la protection des données

Les entités qui ont recours aux technologies de reconnaissance faciale doivent procéder à des analyses d'impact préalables au traitement, car l'utilisation de ces technologies implique le traitement de données biométriques et présente des risques élevés pour les droits fondamentaux des personnes concernées.

Au cours de la préparation de l'analyse d'impact, elles ne se contenteront pas de reconnaître les risques découlant du traitement potentiel, mais considéreront également les mesures d'atténuation nécessaires pour répondre à ces risques en prenant les mesures techniques et organisationnelles requises. Dans cette évaluation, elles expliqueront, entre autres :

- la licéité de l'utilisation de ces technologies ;
- les droits fondamentaux en jeu dans le traitement biométrique ;
- la vulnérabilité des personnes concernées ;
- la manière dont ces risques peuvent être efficacement atténués.

Plus spécifiquement, si elles envisagent le déploiement des technologies de reconnaissance faciale dans des environnements non contrôlés, les autorités chargées de l'application de la loi devront :

- évaluer et expliquer dans leur évaluation l'absolue nécessité et la proportionnalité du déploiement de ces technologies ;
- aborder le risque pour différents droits fondamentaux, notamment pour le droit à la protection des données, à la liberté d'expression, à la liberté de réunion et à la liberté de circulation ou à la lutte contre la discrimination, en fonction des utilisations potentielles en différents endroits.

L'analyse d'impact pourrait être réalisée par les entités elles-mêmes, par un organisme de contrôle indépendant ou par un auditeur ayant l'expertise nécessaire pour aider à découvrir, à mesurer ou à cartographier les impacts et les risques dans le temps.

Lors de la préparation de l'analyse d'impact, les entités doivent impliquer les parties prenantes, y compris les personnes concernées, pour évaluer l'impact potentiel de leur point de vue.

De telles analyses d'impact doivent être réalisées à intervalles réguliers.

Si un risque est identifié, les entités concernées devraient pouvoir s'adresser à tout comité d'éthique existant et aux autorités de supervision compétentes pour examiner les risques potentiels.

Une fois l'évaluation terminée, les entités devraient en publier les conclusions afin d'obtenir l'opinion du public sur le déploiement potentiel des technologies de reconnaissance faciale.

Protection des données dès la conception (« *privacy by design* »)

La protection des données dès la conception concerne toute la chaîne de valeurs du traitement par les technologies de reconnaissance faciale. Les entités qui ont recours à ces technologies à des fins d'identification ou de vérification doivent s'assurer que les produits ou services qu'elles utilisent soient conçus pour traiter des données biométriques conformément aux principes de limitation de la finalité, de minimisation des données et de limitation de la durée de conservation, et intégrer toutes les autres garanties nécessaires dans ces technologies.

Lorsque les entités définissent les caractéristiques techniques de ces technologies, elles intègrent ces principes dans leur conception afin de garantir que leur déploiement respectera le droit à la protection des données.

Cadre éthique

Outre le respect des obligations légales, il semble également crucial de donner un cadre éthique à l'utilisation de cette technologie, notamment au regard du risque plus élevé inhérent à l'utilisation qui en est faite dans certains secteurs. Cela pourrait prendre la forme de conseils d'éthique consultatifs indépendants qui pourraient être consultés avant et pendant le déploiement de processus plus longs de ces technologies, permettre de réaliser des audits et publier les résultats de leurs recherches afin de compléter ou d'entériner la conformité de l'entité concernée. Des considérations expressément éthiques peuvent aider à trouver un équilibre approprié entre des intérêts concurrents d'une manière manifestement équitable[18].

En outre, afin d'éviter les violations des droits de l'homme, des comités d'experts de différents domaines de compétence seraient susceptibles de définir les cas les plus potentiellement difficiles lors de l'utilisation des technologies de reconnaissance faciale.

Sur ce sujet, les lanceurs d'alerte ont aussi un rôle important à jouer et les employés des entités utilisant ces technologies devraient pouvoir bénéficier d'un statut de protection approprié, comme le prévoit notamment la Recommandation CM/Rec(2014)7 du Comité des Ministres aux États membres sur la protection des lanceurs d'alerte.

18. Voir les Lignes directrices sur l'intelligence artificielle et la protection des données disponibles à l'adresse : https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b8.

Droits des personnes concernées

La reconnaissance faciale étant fondée sur le traitement de données à caractère personnel, tous les droits prévus à l'article 9 de la Convention 108+ sont garantis aux personnes concernées, notamment le droit à l'information, le droit d'accès, le droit d'obtenir la connaissance du raisonnement qui sous-tend le traitement, le droit d'opposition et le droit de rectification.

Ces droits peuvent être restreints uniquement lorsqu'une telle restriction est prévue par la loi, qu'elle respecte l'essence des droits et libertés fondamentales et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique à des fins légitimes spécifiques (telles que l'application de la loi), conformément à l'article 11 de la Convention 108+.

En cas de limitation des droits des personnes concernées, les autorités chargées de l'application de la loi doivent informer les personnes concernées, entre autres, de leur droit à déposer une plainte auprès des autorités de contrôle et de leur droit général de recours.

En cas de fausses concordances, les personnes concernées peuvent demander la rectification afin d'en éviter une répétition ou une aggravation.

Lorsque l'utilisation des technologies de reconnaissance faciale est destinée à permettre de prendre une décision fondée uniquement sur un traitement automatisé qui affecterait de manière significative la personne concernée, celle-ci doit notamment avoir le droit de ne pas voir ce traitement effectué sans que son avis soit pris en compte.

Dans le cadre du déploiement des technologies de reconnaissance faciale à la volée, si les intervenants humains agissent uniquement en fonction des résultats fournis par ces technologies, on peut considérer qu'il s'agit d'une prise de décision uniquement automatisée qui pourrait affecter considérablement la personne concernée en raison des conséquences de fausses concordances possibles. La personne concernée peut donc demander conformément à l'article 9, paragraphe 1.*a*, de la Convention 108+ que son point de vue soit pris en compte.

La reconnaissance faciale est passée rapidement du statut de nouveauté technologique à celui de réalité incontournable de notre quotidien. Les technologies de reconnaissance faciale progressent rapidement et les algorithmes sont de plus en plus performants. Les usages qui en sont faits sont variés et nombreux, certains pouvant porter de graves atteintes aux droits des personnes concernées, notamment parce que la reconnaissance faciale est une technologie biométrique. Afin de prévenir de telles atteintes, les Parties à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel s'assureront et permettront que le développement et l'utilisation de la reconnaissance faciale respectent le droit à la vie privée et à la protection des données à caractère personnel, renforçant ainsi les droits de l'homme et les libertés fondamentales.

Ces lignes directrices fournissent un ensemble de mesures de référence que les gouvernements, les développeurs en systèmes de reconnaissance faciale, les fabricants, les prestataires de services et organismes utilisateurs devraient appliquer pour garantir que cette technologie ne nuise à la dignité humaine, aux droits de l'homme et aux libertés fondamentales, y compris le droit à la protection des données à caractère personnel, de toute personne.

www.coe.int/dataprotection

PREMS 020121

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 47 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE