Conseil de l'Europe | Lignes directrices sur la reconnaissance faciale

Le Comité consultatif de la Convention 108+ du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données (en vigueur à Monaco depuis le 1er avril 2009) a adopté le 28 janvier 2021, des Lignes directrices sur la reconnaissance faciale[1].

La reconnaissance faciale y est définie comme *« une technologie de traitement automatique d'images numériques contenant les visages de personnes afin de les identifier ou de les authentifier au moyen de modèles de visages ».* La reconnaissance faciale est un traitement de données biométriques, qui implique des données sensibles.

Les lignes directrices sont destinées aux gouvernements, développeurs, fabricants, prestataires de services et entités utilisatrices de la reconnaissance faciale.

Sont évaluées de manière détaillée les diverses utilisations de cette technologie dans le secteur privé et le secteur public, en tenant compte de leurs finalités et de leur impact potentiel sur les droits des personnes à la protection des données personnelles et d'autres droits fondamentaux, garantis par la Convention Européenne des Droits de l'Homme.

1 T-PD(2020)03rev4. Les lignes directrices du Comité consultatif sont fondées sur le Rapport de Sandra AZRIA et Frédéric WICKERT, La reconnaissance faciale : état de lieux et enjeux, 13 novembre 2019, T-PD(2019)05rev (aspects techniques et juridiques). Elles sont à rapprocher de celles de la CNIL, qui avait appelé à un débat démocratique sur ce sujet en 2018, Reconnaissance faciale – Pour un débat à la hauteur des enjeux, 15 novembre 2019.

> Objet des lignes directrices

- Fournir un ensemble de mesures de référence pour garantir que la technologie de reconnaissance faciale ne nuise pas à la dignité humaine, aux droits de l'Homme et aux libertés fondamentales de toute personne, notamment le droit à la protection des données à caractère personnel.

> Destinataires des lignes directrices

- Législateurs et décideurs
- Développeurs, fabricants et fournisseurs de services
- Entités utilisatrices de technologies de reconnaissance faciale

> L'essentiel des lignes directrices

- Est recommandée la mise en place d'un cadre juridique applicable au traitement de données biométriques au moyen de la reconnaissance faciale, **en fonction de l'utilisation qui en est faite** (les cas d'usage étant multiples), comportant l'explication détaillée de l'utilisation spécifique et de la finalité poursuivie, la

fiabilité minimale et la précision de l'algorithme employé (évaluation des erreurs faux positifs ou faux négatifs produites par le logiciel), la durée de conservation des photos utilisées, la possibilité de contrôler ces critères, la traçabilité du processus, les garanties. (pp. 3-4)

- Utiliser la reconnaissance faciale en vue de la reconnaissance des affects (tenter d'identifier ou de catégoriser les émotions humaines, détecter les traits de personnalité, les sentiments intérieurs, la santé mentale ou l'engagement des travailleurs à partir d'images des visages) comporte des risques très préoccupants, au niveau individuel et sociétal, et **la lier au recrutement de personnel, à l'accès à l'assurance, à l'éducation** devrait être **interdit**. (p. 4)

- L'utilisation d'images numériques téléchargées sur internet (y compris sur les médias sociaux ou sur des sites de gestion de photos en ligne) ou capturées via des caméras de vidéosurveillance, **au seul motif** que ces données personnelles ont été rendues manifestement disponibles par les personnes concernées, est **illicite**. (p. 5)

- 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, est **prohibée**, **à moins que** des garanties appropriées soient prévues par la loi afin de prévenir tout risque de discrimination. (p. 5)

- S'agissant du déploiement de technologies de reconnaissance faciale à la volée (captation indifférenciée des visages) dans les environnements non contrôlés (espaces publics et quasi-publics tels que les centres commerciaux, les hôpitaux et les écoles), la loi doit garantir que les autorités publiques démontrent que divers facteurs, notamment le lieu et le moment du déploiement de ces technologies, justifient l'**absolue nécessité** et la **proportionnalité** des utilisations. (p. 6)

- Pour garantir que le consentement est donné librement, les personnes concernées devraient se voir offrir par les entités privées 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), aussi faciles à utiliser car sinon, le choix ne serait pas authentique. (p. 7)

- 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. (p. 8)

- Les **autorités de contrôle doivent être consultées** sur toute proposition de mesure législative ou administrative impliquant le traitement de données à caractère personnel par des technologies de reconnaissance faciale, sur toute expérimentation ou projet de déploiement éventuel, et avoir accès aux évaluations d'impact réalisées ainsi qu'à tous les audits, rapports et analyses effectués dans ce cadre. (p. 7)

- Pour garantir la responsabilité des développeurs, des fabricants, des fournisseurs de services ou des entités qui utilisent ces technologies, et renforcer la confiance des utilisateurs, devrait être mis en place 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, **selon le domaine d'application de l'intelligence artificielle**, un type pour catégoriser les structures et un autre pour catégoriser les algorithmes. (p. 7)

- Des actions accessibles et éducatives devraient soutenir la **sensibilisation des personnes concernées** et la **compréhension du grand public** des technologies

de reconnaissance faciale et de leur impact sur les droits fondamentaux, pour leur permettre de 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, notamment en cas d'utilisation abusive. (p. 8)

- Concernant les développeurs, les fabricants de technologies de reconnaissance faciale, et les prestataires de services, l'accent est mis sur :
  - la **représentativité des données utilisées** (algorithmes devant être développés à partir d'ensembles de données synthétiques basés sur des photos d'hommes et de femmes suffisamment diverses, de couleurs de peau et de morphologies différentes, de tous âges et sous différents angles de prise de vue, avec des garanties complémentaires s'agissant des informations sur un type de maladie ou de handicap physique),
  - la **durée de vie des données** (photos des visages à reconnaître qui évoluent dans le temps), dont la datation et l'enregistrement du pourcentage de fiabilité de reconnaissance,
  - la **fiabilité des outils utilisés** (faux positifs, faux négatifs, performances sous différents éclairages, fiabilité lorsque les visages ne sont pas orientés vers l'appareil photo, impact des accessoires recouvrant les visages),
  - la **sensibilisation des entités utilisatrices** (recommandations pour leur politique de protection de la vie privée),
  - la **responsabilité** (mesures spécifiques visant à garantir la conformité des traitements avec les principes de protection des données). (pp. 8-10)
- Concernant les entités utilisatrices, l'accent est mis sur :
  - la **transparence** et la **loyauté** du traitement (type d'informations devant être données aux personnes concernées, droits et recours juridiques dont elles disposent, politiques de protection de la vie privée),
  - la **limitation de la finalité** du traitement,
  - la **minimisation** des données (seules les informations requises sont traitées, et non toutes celles à disposition),
  - la **limitation de la durée de conservation** (suppression automatique en l'absence de correspondance entre les modèles biométriques, durée strictement limitée en cas de concordance et la plus courte possible, destruction des listes de surveillance et des modèles biométriques une fois la finalité atteinte), l'exactitude (éviter et corriger les fausses correspondances),
  - la **sécurité** des données (mesures techniques et organisationnelles robustes et évolutives),
  - la **responsabilité** (politiques, procédures et pratiques transparentes, publication de rapports de transparence sur l'utilisation concrète des technologies de reconnaissance faciale, programmes de formation et de procédures d'audit pour les personnes chargées du traitement, comités de révision internes chargés d'évaluer et d'approuver tout traitement impliquant des données de reconnaissance faciale, extension contractuelle des exigences applicables aux prestataires de services tiers, aux partenaires commerciaux ou à d'autres entités utilisant la technologie de reconnaissance faciale, et dans le secteur public, contraintes d'évaluation préalable dans les procédures de marchés publics avec les fournisseurs d'outils de reconnaissance faciale). (pp. 10-13)

> Cadre juridique de la reconnaissance faciale

▪ Cadre européen

L'article 6 de la Convention 108+ n'autorise le traitement de données biométriques que s'il repose sur une **base juridique appropriée**, et si des **garanties complémentaires**, appropriées, adaptées aux risques encourus et aux intérêts, droits et libertés à protéger, sont **inscrites dans la loi nationale**.

▪ Cadre national

L'article 11 de la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, consolidée, autorise les autorités judiciaires et administratives à mettre en œuvre des traitements comportant des données biométriques, **dans le cadre exclusif des missions qui leur sont légalement conférées** (sécurité publique ; infractions, condamnations ou mesures de sûreté ; prévention, recherche, constatation ou poursuite des infractions pénales ; exécution des condamnations pénales ou des mesures de sûreté). La mise en œuvre de ces traitements est décidée par les autorités compétentes après avis motivé de la Commission de contrôle des informations nominatives (CCIN).

L'article 11-1 n'autorise les responsables de traitements autres que les autorités judiciaires et administratives, à mettre en œuvre des traitements automatisés d'informations nominatives comportant des données biométriques que s'ils sont **nécessaires au contrôle de l'identité des personnes,** et poursuivent un **objectif légitime essentiel**, à condition d'assurer le **respect des droits et libertés** des personnes concernées. Une autorisation préalable de la CCIN est requise.

L'article 12 prohibe par principe la mise en œuvre de traitements faisant apparaître, directement ou indirectement, des opinions ou des appartenances politiques, raciales ou ethniques, religieuses, philosophiques ou syndicales, ou encore des données relatives à la santé, y compris les données génétiques, à la vie sexuelle, aux mœurs, aux mesures à caractère social (**données sensibles**). Des exceptions s'appliquent (consentement librement donné, écrit et express de la personne concernée sauf dans le cas où la loi prévoit que l'interdiction ne peut être levée par le consentement de la personne concernée, motif d'intérêt public, diagnostics médicaux, …).

> Exemples d'usages de la reconnaissance faciale[2] (existants ou projetés, légitimes ou non)

- Permettre dans un cadre domestique, l'accès à des services ou à des applications pour déverrouiller un appareil (en substitution de l'authentification par mot de passe),
- Identifier les relations d'une personne sur un réseau social, sur une application photo pour en suggérer l'identification nominative,
- Permettre à un non-voyant de récupérer des informations sur les personnes en face de lui (genre, âge, émotions),
- Reconnaître des enfants disparus aujourd'hui adultes (simulation de vieillissement),
- Reconnaitre une maladie génétique rare,
- Détecter les émotions des personnes (entretien d'embauche, film, jeu vidéo, spectacle, …),
- Déterminer si une personne va commettre un crime d'après les traits de son visage,

2 Sources : Rapport de Sandra AZRIA et Frédéric WICKERT, La reconnaissance faciale : état de lieux et enjeux, op. cit. ; CNIL, Reconnaissance faciale – Pour un débat à la hauteur des enjeux, op. cit.

- Vérifier l'identité d'une personne pour bénéficier de services administratifs (accès sécurisé à des e-services) ou commerciaux (ouverture à distance d'un compte bancaire, distributeurs de billets, …),
- Contrôler l'accès physique à un lieu prédéterminé (entrée de bâtiments…), ou à des points de passage particuliers (frontières, …),
- Identifier sur la voie publique des personnes recherchées,
- Vidéoverbaliser des piétons,
- Suivre le parcours d'un passager à toutes les étapes (déposes bagages, portiques d'embarquement, …), les déplacements d'une personne dans l'espace public (oubli de bagage, commission d'un délit),
- Reconstituer le parcours d'une personne pour identifier ses contacts,
- Rechercher les antécédents judiciaires d'une personne non identifiée dans une base de données (victime, suspecte).