LES BRÈVES - LEGAL INFORMATION
PROPOSED BY DS GROUP

30 mars 2021

Règlementation de la reconnaissance faciale : la position du Conseil de l'Europe (28 janvier 2021)

L'utilisation des technologies de reconnaissance faciale, **aussi bien dans le secteur privé que public**, fait débat. Son essor est remarquable, notamment depuis le développement de cette technologie pour procéder au déverrouillage des smartphones, tablettes et ordinateurs.

Pour la Cnil, la reconnaissance faciale est « une technique qui permet à partir des traits de visage d'**authentifier une personne**, c'est-à-dire de vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès) ou d'**identifier une personne**, c'est-à-dire de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données ».

- **Les données biométriques**

La technologie même de la reconnaissance faciale est basée sur le traitement de données biométriques.

La donnée biométrique est définie par la Cnil comme une « **caractéristique physique ou biologique permettant d'identifier une personne** » (iris, voix, visage, empreintes digitales, ADN, démarche…). Cette technologie repose sur un modèle de référence appelé « **gabarit** ». Le gabarit se sert des caractéristiques du visage (distance entre les yeux, couleur des yeux, etc.) analysées à partir de photos ou d'enregistrements vidéo. Le gabarit utilise donc **des données biométriques.**

- **Deux textes européens s'appliquent déjà à la reconnaissance faciale**

Bien que déjà encadrée partiellement par le **RGPD** et la **directive dite Police-Justice**, la reconnaissance faciale ne fait pas encore l'objet d'une règlementation dédiée au niveau européen. Dans leurs domaines respectifs, ces deux textes **interdisent par principe le traitement des données biométriques** (articles 9 du RGPD et 10 de la directive Police-Justice).

Le traitement de données biométriques est autorisé dans des **cas très restreints :**

- en cas de « nécessité absolue » (directive Police-Justice), ou
- dans le cadre de l'une des dix exceptions prévues par le RGPD, par exemple lorsque la personne a donné son consentement au traitement de ses données biométriques ou encore pour la médecine du travail.

Mais comment gérer les usages du quotidien, face à un cadre si restrictif ? C'est justement là qu'intervient l'exemption pour usage domestique (art. 2 de la loi Informatique et Libertés sur le

principe d'exemption domestique). L'utilisation de la reconnaissance faciale pour déverrouiller un smartphone relève, pour la Cnil, de cette exemption, si « le gabarit est stocké dans l'appareil, sous le seul contrôle » de l'utilisateur.

Les utilisations de la reconnaissance faciale hors de l'usage domestique sont soumises au RGPD et, le cas échéant, à la directive Police-Justice.

- **De nouvelles questions juridiques soulevées par l'utilisation de la reconnaissance faciale**

La Cnil a déjà autorisé deux banques, la Société Générale en 2017 et Boursorama en 2018, à recourir à la reconnaissance faciale pour l'identification des prospects lors d'une ouverture en ligne de comptes bancaires. Dans les deux cas, les garanties mises en place par les banques étaient suffisantes. Notamment, les gabarits générés étaient **conservés uniquement le temps de la comparaison** entre la photographie fournie par le prospect et la photographie figurant sur sa pièce d'identité.

A l'inverse, d'autres projets ont été bloqués par la Cnil ou par les tribunaux français qui peuvent examiner la **proportionnalité** du recours à la reconnaissance faciale. Ainsi, le tribunal administratif de Marseille a rejeté l'expérimentation de la région PACA sur un dispositif d'accès par reconnaissance faciale aux établissements scolaires. Ce dispositif visait à accroître la sécurité et la fluidité des entrées des élèves. Le tribunal administratif a considéré que le **consentement** des élèves n'était pas suffisamment libre et éclairé au regard de la relation d'autorité qui les reliaient à l'établissement scolaire[1].

Au niveau européen, la tendance est également à un encadrement strict. Les recommandations du CEPD sur les traitements de données personnelles par des dispositifs vidéo (Lignes directrices n°3/2019 du 29 janvier 2020) ont récemment été reprises, précisées et complétées par le Conseil de l'Europe au sein de ses **lignes directrices sur la reconnaissance faciale** publiées fin janvier 2021.

- **Prise de position du Conseil de l'Europe sur l'utilisation des technologies de reconnaissance faciale**

Le 28 janvier 2021, le Conseil de l'Europe a publié ses lignes directrices qui se décomposent en quatre parties :

- la première s'adresse aux législateurs et décideurs des Etats membres ;
- la deuxième s'adresse aux développeurs, aux fabricants et aux fournisseurs de services de technologies de reconnaissance faciale ;
- la troisième s'adresse aux entités utilisatrices de ces technologies ;
- la dernière est consacrée aux droits des personnes concernées.

Il s'agit d'un **ensemble de mesures de référence** que les entités précitées devront appliquer, qu'elles aient recours à cette technologie dans un secteur privé ou public.

1. <u>Recommandations à destination des législateurs et décideurs nationaux</u>

Côté nouveautés, les lignes directrices recommandent aux législateurs nationaux **d'interdire l'utilisation de la reconnaissance faciale « dans le seul but de déterminer la couleur de peau, les convictions** religieuses ou autres convictions**, le sexe, l'origine raciale ou ethnique, l'âge, l'état de**

[1] TA Marseille, 27 févr. 2020, n° 1901249, Association La Quadrature du Net, AJDA 2020. 492

santé, ou la condition sociale d'une personne (…), à moins que des garanties appropriées soient prévues par la loi afin de prévenir tout risque de discrimination ».

Les lignes directrices préconisent **l'interdiction de « lier la reconnaissance de l'affect, par exemple au recrutement de personnel, à l'accès à l'assurance ou à l'éducation »**. Par « reconnaissance de l'affect », le texte vise l'utilisation de la reconnaissance faciale pour l'identification ou la catégorisation des **émotions humaines** (traits de personnalité, sentiments intérieurs ou santé mentale par ex.).

Le Conseil de l'Europe affirme qu'est illicite l'utilisation d'images numériques téléchargées sur internet ou captées via des caméras de vidéosurveillance pour en extraire des modèles biométriques**, au seul motif que ces données personnelles ont été rendues manifestement disponibles par les personnes concernées**. Cette affirmation répond au scandale Clearview dont le logiciel de reconnaissance faciale repose sur la captation de photos disponibles sur internet (notamment sur Facebook et YouTube). A partir de ces images publiques, le logiciel produit des gabarits qui viennent enrichir sa base de données.

Dans le **secteur privé**, l'utilisation de la reconnaissance faciale suppose le consentement des personnes et doit avoir lieu dans des **environnements contrôlés** « à des fins de vérification, d'authentification ou de catégorisation »[2].

➔ Une entreprise ne peut pas installer de dispositif de reconnaissance faciale dans un espace public traversé par des personnes, comme un centre commercial.

Pour s'assurer du **caractère libre du consentement**, les personnes concernées doivent pouvoir refuser l'usage de la reconnaissance faciale et donc se voir proposer une **solution alternative** qui soit « **aussi facile à utiliser** »**.**

➔ **Le contrôle d'accès aux locaux** peut reposer sur la reconnaissance faciale si le salarié y consent. Pour autant, une alternative (un badge d'indentification ou un code d'accès) doit être offerte.

2. <u>Recommandations à destination des développeurs, fabricants et fournisseurs de services</u>

Les développeurs sont tenus à des obligations d'**exactitude des données**, de **fiabilité des outils utilisés** et de **sensibilisation** des utilisateurs de leurs technologies de reconnaissance faciale.

Mais surtout, le texte suggère l'instauration d'une obligation de transparence à l'égard des **pourcentages de fiabilité de reconnaissance** des algorithmes de reconnaissance faciale.

➔ Les développeurs devront rendre publiques leurs relevés de **pourcentage de fiabilité** : les **mettre 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.

Si une telle obligation venait à être consacrée en droit français, elle permettrait aux prospects et aux entreprises utilisatrices de logiciels de reconnaissance faciale de comparer facilement les différents fournisseurs de services afin d'opter pour celui proposant l'**algorithme le plus fiable**.

[2] 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 » (définition tirée des lignes directrices du Conseil de l'Europe).

3. Recommandations à destination des entités utilisatrices

Des obligations de **transparence et de loyauté** sont mises à la charge des entités utilisatrices. A ce titre, elles devront inclure les informations suivantes au sein de leurs politiques de protection de la vie privée ou de leurs matériels d'information :

- Si, et dans quelle mesure, les données de reconnaissance faciale peuvent être transmises à des tiers (et, le cas échéant, l'identité de ces tiers) ;
- La conservation, la suppression ou la désidentification des données de reconnaissance faciale ;
- Les points de contact à destination des particuliers ;
- La mise à jour publique de leur politique en cas de changement significatif survenant dans leurs pratiques de collecte, d'utilisation et de partage.

Les lignes directrices imposent également aux entreprises et entités utilisatrices **le respect des principes de limitation de la finalité du traitement, de minimisation et d'exactitude des données collectées et de limitation de leur durée de stockage**.

Les entités utilisatrices d'un dispositif de reconnaissance faciale doivent mettre en place des **mesures organisationnelles** :

- mise en place de **comités internes de révision** chargés d'évaluer et d'approuver tous les traitements impliquant des données de reconnaissance faciale,
- **publication de rapports** de transparence sur l'utilisation concrète des technologies de reconnaissance faciale et,
- **extension contractuelle des exigences à leurs sous-traitants**.

En outre, elles doivent veiller à ce que « les **intervenants humains continuent de jouer un rôle décisif** dans les actions prises sur la base des résultats de ces technologies ».

➔ Une entreprise ne pourra pas donc pas, sur la base d'une surveillance par reconnaissance faciale du temps de travail d'un employé, retirer de manière automatique les heures non travaillées calculées par le logiciel de reconnaissance faciale effectif dans les bureaux.

Enfin, des **analyses d'impact** particulièrement détaillées et préalables à tout traitement de données personnelles sont obligatoires. Elles devront intégrer :

- les **mesures d'atténuation** nécessaires des risques pour les droits fondamentaux des personnes concernées ;
- le cas échéant, des explications détaillées sur **l'absolue nécessité et la proportionnalité** du déploiement de ces technologies dans des environnements non contrôlés ;
- l'**implication des parties prenantes** (y compris les personnes concernées) pour procéder à l'évaluation de l'impact potentiel du traitement de leur point de vue ;
- la **publication des conclusions** de l'analyse d'impact afin de recevoir l'opinion du public.

4. Effectivité des droits des personnes

Les entités utilisatrices doivent s'assurer de l'effectivité des droits des personnes concernées : **droit à l'information, droit d'accès, droit d'obtenir la connaissance du raisonnement, droit de rectification en cas de fausses concordances** et droit à un recours effectif.

En outre, les personnes concernées disposent d'un **droit à ce que leur avis soit pris en compte** si la reconnaissance faciale est destinée à permettre de prendre une décision fondée uniquement sur un traitement automatisé l'affectant de manière significative.

*

La reconnaissance faciale étant une technologie particulièrement intrusive, la position stricte du Conseil de l'Europe au sein d'un texte dédié se comprend aisément. Désormais, les entreprises développant ou utilisant des technologies de reconnaissance faciale disposent donc d'un **cadre de référence** à respecter pour garantir leur conformité au droit de la protection des données personnelles.

Pour toutes autres informations, veuillez contacter l'auteure, Inès Jousset[3] ou notre équipe Propriété Intellectuelle, Technologie, Data.

Inès Jousset
Avocate Collaboratrice
jousset@dsavocats.com
Paris

Sylvain Staub
Avocat Associé
staub@dsavocats.com
Paris

[3] Cette brève a été rédigée avec le concours de Louis Mutz, Stagiaire DS Avocats