vigo

Flash info

Reconnaissance faciale : la CNIL présente les éléments à prendre en compte

Le 15 novembre 2019, la CNIL a présenté dans une note intitulée « Reconnaissance faciale : pour un débat à la hauteur des enjeux » les éléments juridiques, éthiques et techniques devant être pris en compte dans le cadre de l'utilisation et l'expérimentation des systèmes de reconnaissance faciale.

Sa contribution, examinée par les membres du collège de la CNIL le 7 novembre 2019, poursuit quatre objectifs :

- présenter, techniquement, ce qu'est la reconnaissance faciale et son usage ;
- mettre en lumière les risques technologiques, éthiques et sociétaux liés aux systèmes de reconnaissance faciale ;
- rappeler le cadre s'imposant aux dispositifs de reconnaissance faciale et à leurs expérimentations ;
- préciser le rôle de la CNIL dans l'éventuel déploiement, à titre expérimental, de nouveaux dispositifs de reconnaissance faciale.

Définition et cadre des systèmes de reconnaissance faciale

La CNIL définit la reconnaissance faciale comme « *une technique informatique et probabiliste qui permet de reconnaître automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier.* »[1]

Cette reconnaissance faciale doit s'effectuer en deux temps :

- la collecte du visage et sa transformation en un gabarit mathématique ;

- la reconnaissance du visage, par la comparaison du gabarit qui vient d'être collecté avec un ou plusieurs gabarits collectés préalablement.

La reconnaissance faciale peut remplir deux fonctions distinctes :

- **l'authentification d'une personne,** visant à vérifier qu'une personne est bien celle qu'elle prétend être[2] ;
- **l'identification d'une personne** visant à identifier une personne au sein d'un groupe d'individus[3].

Dans les deux cas, tout est affaire de probabilité. Les systèmes de reconnaissance faciale reposent sur une estimation de correspondance entre des gabarits : celui qui est comparé et celui ou ceux servant d'étalon. Comme l'explique la CNIL, *« de la comparaison se déduit une probabilité, plus ou moins forte, que la personne soit bien celle que l'on cherche à authentifier ou à identifier ; si cette probabilité dépasse un seuil déterminé dans le système, celui-ci va considérer qu'il y a correspondance.* »[4]
Par ailleurs, il est également nécessaire de distinguer les contextes dans lesquels les systèmes de reconnaissance faciale peuvent être utilisés. En effet, et à titre d'exemples, les implications ne sont pas les mêmes entre :

- l'utilisation de systèmes de reconnaissance faciale pour déverrouiller un téléphone[5] ;
- l'utilisation à des fins d'identification de personnes recherchées sur la voie publique[6].

C'est en ce sens que la CNIL rappelle qu'un **raisonnement « *cas d'usage par cas d'usage* »[7]** s'impose. Il est nécessaire, comme le rappelle le RGPD, d'apprécier la pertinence et la proportionnalité des données utilisées en fonction de la finalité recherchée par le traitement.

Les risques liés à l'utilisation de systèmes de reconnaissance faciale

La CNIL rappelle que les données issues de la reconnaissance faciale sont des données biométriques, considérées comme sensibles au sens de la législation applicable. En effet,

en permettant « *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* »[8], elles sont relatives *« à l'intimité de la vie privée des personnes* »[9].

Par ailleurs, les données biométriques ne sont ni révocables – car inhérentes à la personne – ni modifiables. Autrement dit, « *tout détournement ou mauvais usage de cette donnée fait ainsi peser des risques substantiels sur la personne dont elle émane : privation de ses accès à des services ou à des lieux, usurpation de son identité à des fins d'escroquerie, voire criminelles.* »[10]

Les traitements biométriques sont donc très encadrés par le RGPD, qui les interdit par principe[11], et par la directive « police-justice »[12], qui ne les permet qu'en cas de nécessité absolue. La Loi Informatique et Libertés s'est d'ailleurs inscrite dans leur continuité[13].

La CNIL insiste sur la sécurisation des données biométriques, qui doit être *« une priorité impérieuse dans la conception de tout projet* »[14], notamment au regard des risques posés par les cyberattaques liées à ces données sensibles. Certaines solutions doivent donc être privilégiées, tel que le stockage en local sur un support détenu par l'utilisateur[15].

En outre, les données nécessaires à la reconnaissance faciale, contrairement à d'autres données biométriques, ont comme caractéristique d'être « disponibles partout », sans-contact : la simple captation de l'image d'une personne peut suffire à l'identifier.

Selon la CNIL, cette capacité d'identification d'une grande quantité de personnes sans qu'elles n'aient à réaliser une quelconque action positive entraîne un changement de paradigme de la surveillance : « *le passage d'une surveillance ciblée de certains individus à la possibilité d'une surveillance de tous aux fins d'en identifier certains* »[16].

Ce changement de paradigme s'accompagne également de la question du traitement des faux positifs et des biais que comporte la technologie.

Le cadre s'imposant aux dispositifs de reconnaissance faciale

Dans le cadre de la mise en place d'expérimentations de dispositifs de reconnaissance faciale par les pouvoirs publics, la CNIL distingue trois exigences essentielles :

- Tracer des lignes rouges avant tout usage expérimental ;
- Placer le respect des personnes au cœur de la démarche ;
- Adopter une démarche sincèrement expérimentale.

Tracer des lignes rouges avant tout usage expérimental

La CNIL a déjà eu l'occasion de reconnaître la légitimité et la proportionnalité de certains usages.

Lorsqu'il est nécessaire d'assurer un haut niveau d'authentification, la CNIL a pu admettre certains dispositifs, sous réserve de maîtrise des données biométriques, comme PARAFE (contrôle automatisé aux frontières) ou ALICEM (application mobile permettant l'authentification forte pour accéder à certains services en ligne, en cours de développement). Lorsque d'autres moyens que la reconnaissance faciale pouvaient être mis en place de manière tout aussi efficace, elle les a interdit.

Pour la CNIL, « *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*. »[17].

De ce fait, en cas d'élaboration d'un encadrement expérimental de la reconnaissance faciale, la CNIL souhaite poser, en concertation avec les pouvoirs publics, des « *lignes rouges au-delà desquelles aucun usage, même expérimental, ne peut être admis* »[18].

Placer le respect des personnes au cœur de la démarche

La CNIL rappelle également que la prise en compte des droits à la protection des données et à la vie privée doit être centrale dans la démarche, de sorte que :

- le consentement doit être recueilli dès que le dispositif le permet ;
- les dispositifs permettant la maîtrise des données par les utilisateurs doivent être privilégiés ;
- la transparence et le droit de retrait doivent être assurés « *en toutes circonstances* »[19] ;

- la sécurité des données « *doit être une condition impérieuse de leur traitement* »[20].

La CNIL précise par ailleurs que « *les expérimentations ne sauraient éthiquement avoir pour objet ou pour effet d'accoutumer les personnes à des techniques de surveillance intrusive* »[21] ; cette étape ne pouvant intervenir « *qu'ultérieurement, pour des dispositifs reconnus comme parfaitement légitimes et licites* »[22].

Adopter une démarche sincèrement expérimentale

La CNIL, en permettant ces expérimentations, souhaite se prémunir « *de tout effet cliquet lié à la mise en œuvre de certains dispositifs* »[24].

Pour cela, il est nécessaire de « *garantir la sincérité des expérimentations* »[25], sans préjuger de leur issue, et donc de « *consacrer une méthode expérimentale rigoureuse, inspirée du cadre juridique plus général en la matière et du guide méthodologique récemment élaboré par le Conseil d'État* »[26].

Le rôle de la CNIL dans la régulation des systèmes de reconnaissance faciale

La CNIL rappelle son rôle dans l'élaboration d'une telle régulation : accompagner le gouvernement et le Parlement dans l'élaboration du cadre réglementaire et s'assurer du respect de la loi dans la mise en place des implémentations.

Elle rappelle également son souhait de conseiller les pouvoirs publics en amont sur tout cadre d'expérimentation, mais aussi sur les cas concrets d'expérimentation envisagés. Dans ce cas, elle s'appuiera sur les analyses d'impact réalisées avant la mise en œuvre et sur les bilans périodiques, qui devraient lui être adressés.

Enfin, elle rappelle qu'outre toutes ces étapes préparatoires, elle conserve le pouvoir de contrôler le respect effectif du cadre juridique et d'imposer les correctifs nécessaires ou l'arrêt du dispositif. En tant que régulateur indépendant, la CNIL ne peut pas être partie prenante de l'organisation effective des expérimentations en question ou de leur pilotage.

Emmanuel Daoud, Imane Bello et Paul-Henri Laugier

[1] CNIL, *Reconnaissance faciale – Pour un débat à la hauteur des enjeux*, 15 nov. 2019, p. 3. Disponible sur : https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

[2] Dans ce cas, le système fait une comparaison entre le gabarit préenregistré et le visage d'une personne.

[3] Dans cette hypothèse, le système va faire une comparaison entre le ou les visages et les gabarits dont il dispose, stocké dans une base de données.

[4] CNIL, *préc.*, p. 3.

[5] Ici, le gabarit est stocké sur le terminal de l'utilisateur.

[6] Cette utilisation se caractérise par la confrontation en temps réel de tous les visages captés par la vidéosurveillance avec une base de données des visages des personnes recherchées

[7] CNIL, *préc.*, p. 5.

[8] Eod. Loc., p. 6.

[9] Ibid.

[10] Ibid.

[11] 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*, art. 9.

[12] 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,* art. 10.

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

[14] CNIL, *préc.*, p. 6.

[15] Ibid.

[16] Eod. Loc., p. 7.

[17] Eod. Loc., p. 9.

[18] Ibid.

[19] Eod. Loc., p. 10.

[20] Ibid.

[21] Ibid.

[22] Ibid..

[23] Ibid.

[24] Ibid.

[25] Ibid.

Nous contacter

Coordonnées téléphoniques :
+33 (0)1 55 27 93 93
Adresse email :
vigo@vigo-avocats.com
Adresse du cabinet :
Vigo, cabinet d'avocats 9, rue Boissy d'Anglas Paris 75008 France