Université Paris Dauphine-PSL

Éthique et sciences des données

Quelle régulation de la reconnaissance faciale ?

Auteurs :
Rekia Abdellaoui
Marina Chau
Elise Chin
Mathilde Da Cruz
Aliou Diallo
Emilie Greff

1er décembre 2021

Table des matières

1 Reconnaissance faciale et cadre actuel **2**
1.1 Définitions . . . 2
1.2 Réglementation actuelle . . . 2
1.2.1 France . . . 2
1.2.2 Europe . . . 2
1.3 Vers un encadrement des expérimentations de reconnaissance faciale . . . 3
1.3.1 Un cadre expérimental précisé par des exigences nécessaires . . . 3

2 Reconnaissance faciale : une technologie potentiellement faillible **4**
2.1 Un exemple de démarche expérimentale : ALICEM . . . 4
2.2 La Méconnaissance faciale . . . 5
2.2.1 Les problèmes algorithmiques . . . 5
2.2.2 La discrimination dans la reconnaissance faciale . . . 6
2.2.3 Les failles exploitables de la reconnaissance faciale . . . 6

3 Utilisation de la reconnaissance faciale dans l'espace public : opportunités et menaces **7**
3.1 Authentification . . . 7
3.1.1 Qu'est-ce que c'est ? . . . 7
3.1.2 Quelques cas d'usages et leurs avantages . . . 7
3.1.3 Risques possibles engendrés . . . 8
3.2 Identification . . . 8
3.2.1 Qu'est-ce que c'est ? . . . 8
3.2.2 Quelques cas d'usages et leurs avantages . . . 8
3.2.3 Quelques risques, notamment pour la liberté des citoyens . . . 8

Introduction

Notre visage est sans doute l'élément qui nous caractérise le plus, bien au delà de notre nom ou notre date de naissance. C'est par notre visage que nous sommes reconnus (voire authentifiés) par ceux qui nous connaissent, et c'est par notre visage que nous sommes en partie décryptés par ceux qui ne nous connaissent pas et qui pourront nous identifier à un sexe, un âge, une couleur de peau. C'est probablement à cause de cette singularité que le sujet de la reconnaissance faciale, particulièrement celui de son encadrement, fait beaucoup débat dernièrement. En effet, cette technologie étant assez nouvelle, les limites sont encore floues. Pour Cédric O, le secrétaire d'état chargé du numérique, « elle entre dans nos vies sans que son cadre d'utilisation n'ait encore été clarifié ». Il est donc important de « définir très clairement le cadre et les garanties pour éviter la surveillance généralisée ». En effet, l'objectif serait de tirer le meilleur parti des avancées technologiques, sans remettre en cause certains de nos principes fondamentaux. A ces fins se pose la question de la régulation de la reconnaissance faciale. Nous verrons d'abord quel encadrement est déjà proposé, notamment en France et en Europe. Nous verrons ensuite qu'outre les problèmes évidents de surveillance généralisée et de droit à l'anonymat, il existe également des failles liées à la technologie en elle-même, notamment à son algorithme. Enfin, nous discuterons des opportunités et menaces des deux fonctions de la reconnaissance faciale, l'authentification et l'identification.

1 Reconnaissance faciale et cadre actuel

1.1 Définitions

— **Données biométriques :** La CNIL [1] les définit comme les caractéristiques physiques ou biologiques permettant d'identifier une personne : ADN, contour de la main, empreintes digitales... L'article 4 du RGPD parle des données à caractère personnel résultant d'un traitement technique spécifique relatives aux caractéristiques, physiologiques ou comportementales qui permettent ou confirment son identification unique [3] ;
— **L'identification** est une phase qui consiste à établir l'identité d'une personne [3] ;
— **L'authentification** est une phase qui permet d'apporter la preuve de l'identité. Elle intervient après la phase d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?" [3].

La **reconnaissance faciale** est donc une méthode qui, à partir de données biométriques du visage, permet d'identifier un individu (au sein d'une base de données de références) ou de l'authentifier (vérifier qu'elle est bien celle qu'elle déclare être). Elle peut être utilisée à des fins de contrôle et de surveillance dans l'espace public, comme des fins récréatives dans l'espace privé ou encore à des fins commerciales [3].

1.2 Réglementation actuelle

1.2.1 France

La **reconnaissance faciale** est tout d'abord un traitement de données de l'image d'une personne, laquelle constitue une **donnée personnelle**. Outre les textes européens (détaillés ci-dessous), la réglementation française s'appuie sur la **loi « informatique et liberté »** et des dispositions spécifiques telles par exemple celles relatives aux caméras de surveillance qui sont régies par **le Code de la sécurité intérieure** (autorisation préfectorale requise pour tout système de vidéo de protection sur la voie publique). L'autorité de contrôle (la CNIL) formule aussi des exigences préalables à tout usage (lignes rouges infranchissables, rappels des principes éthiques, démarche expérimentale pour éviter les effets cliquets) et en vérifie le respect. Elle a adopté des règlements et délibérations sur certains cas d'usage, notamment le condtrôle d'accès des locaux professionnels, surveillance des lycées ou des festivals, etc. [2]

1.2.2 Europe

La législation européenne prévoit une protection des données à caractère personnel correspondant à un commencement d'encadrement des technologies.

Elle est regroupée principalement sur deux textes, adoptés en avril 2016 composant le paquet européen : le **RGPD**, règlement relatif à la protection des données sur la collecte, le traitement et la conservation des données à caractère personnel et à la libre circulation de ces données et **la directive Police Justice** relative à la protection des personnes physiques qui traite notamment de l'utilisation 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 sanction pénales.

1. Commission nationale de l'informatique et des libertés

En parallèle de ces textes ont été votés des dispositions applicables à l'usage des images faciales dans le cadre de la sécurité et du contrôle aux frontières.

Il s'agit du règlement dit « **ESS** » **du 30 novembre 2017** portant création d'un système d'entrée et de sortie pour enregistrer les données relatives aux entrées sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières des états membres et portant détermination des conditions d'accès à l'ESS à des fins répressives et modifiant notamment la convention d'application de l'accord de Schengen [2].

La prohibition du traitement des données biométriques et donc de la reconnaissance faciale est le principe instauré par la législation européenne.

Elle prévoit toutefois de nombreuses exceptions mais en encadre strictement l'utilisation :
- En cas de consentement libre et éclairé de la personne concernée par le traitement ;
- Pour la sauvegarde des intérêts vitaux de la personne, ou l'existence d'un motif d'intérêt public important tel par exemple les dispositifs de reconnaissance faciale aux points d'identification dans un aéroport ;
- Utilisation intégrée à un système personnel (pour permettre de déverrouiller un smartphone).

Seuls par exemple les passagers ayant préalablement consenti et procédé à leur enregistrement pourront utiliser le portique équipé du système biométrique.

La réglementation européenne dans le cadre des exceptions repose sur une démarche de conformité : **AIPD Analyse d'Impact sur la Protection des Données** ; consultation de l'autorité de contrôle dans les cas sensibles ; « privacy by design » et « privacy by default » (prise en compte de la protection dès la conception du produit et du service, par défaut respect du plus haut niveau de protection) [2].

En conclusion si la prohibition des traitements de données sensibles est le principe, il y est en revanche prévu de nombreuses exceptions, mais strictement encadrées pour protéger les libertés des citoyens.

1.3 Vers un encadrement des expérimentations de reconnaissance faciale

Depuis quelques années, la reconnaissance faciale est de plus en plus mise en avant par les pouvoirs publics comme instrument de sécurité. L'utilisation de cette technologie fait débat auprès des concitoyens. La CNIL a défini, dans une notice explicative en date du 15 novembre 2019, que l'utilisation de la reconnaissance faciale par les pouvoirs publics devrait passer par une phase d'expérimentation. Elle a défini trois exigences qui devront encadrer toutes démarches expérimentales avec la reconnaissance faciale, afin de garantir le respect des droits à la vie privée des citoyens, ainsi que leur confiance vis-à-vis de ces dispositifs.

1.3.1 Un cadre expérimental précisé par des exigences nécessaires

La CNIL, dans sa notice explicative de 2019, a proposé trois exigences essentielles afin d'encadrer toute démarche expérimentale avec la reconnaissance faciale. En premier lieu, **une réflexion sur les lignes rouges à ne pas dépasser lors de l'expérimentation** : elle est

réalisée dans le but de définir des frontières qui circonscrivent le champ du souhaitable (politiquement, socialement) comme celui du possible. En effet, la reconnaissance faciale ne peut être utilisée, même à titre expérimental, si elle ne répond pas à un impératif particulier d'assurer un haut niveau de fiabilité quant à l'authentification ou identification des personnes concernées. L'intérêt de recourir à cette technologie peut être **légitime, mais pas forcément souhaitable**. Il est donc important de réaliser des tests avec d'autres types de technologies moins intrusives et d'en comparer les performances.

En deuxième lieu, il est **important de placer le respect des personnes au cœur de la démarche expérimentale** : l'expérimentation doit être construite en prenant en compte le respect des droits à la personne (droit à l'information, droit d'opposition, etc.). Le recueillement du consentement des personnes à l'expérimentation est obligatoire. Le dispositif qui encadre la démarche doit être transparent, et doit garantir la sécurité des personnes concernées. Enfin, on retiendra aussi que les démarches expérimentales doivent avoir une finalité précise et ne doivent pas, en aucun cas, accoutumer les personnes à des techniques de surveillance intrusives.

Enfin, la dernière exigence de la CNIL quant à l'expérimentation des technologies de reconnaissance faciale, requiert un cadre juridique qui **garantit la sincérité des expérimentations conduites**. Cela nécessite une méthode expérimentale rigoureuse, avec une limitation dans le temps, et une identification exacte des objectifs poursuivis. L'expérimentation doit être conduite avec prudence face aux risques potentiels de l'utilisation de la reconnaissance faciale. Toutefois, prudence ne rime pas avec bridage technologique : une véritable démarche expérimentale permettra de tester et de parfaire des solutions techniques respectueuses du cadre juridique, lorsqu'elles se présenteront, et intégrant directement les contraintes.

2 Reconnaissance faciale : une technologie potentiellement faillible

2.1 Un exemple de démarche expérimentale : ALICEM

Au courant de l'année 2018, le gouvernement a annoncé un projet d'application nommé "Application de lecture de l'identité d'un citoyen en mobilité" (ALICEM) au public. Cette annonce a provoqué de vives réactions au sein du public. En effet, pour pouvoir se connecter et accéder aux services publics en ligne qu'elle propose, les citoyens doivent utiliser la reconnaissance faciale pour s'inscrire. En résumé, la personne voulant accéder à ses comptes administratifs (Amélie, ANTS, etc.) n'a pas le choix de passer ou non par ce dispositif de reconnaissance faciale et le consentement dont se revendique le gouvernement n'est donc pas valable.

C'est donc sans surprise que cette application a fait réagir la CNIL. Le 18 octobre 2018, la CNIL a publié la délibération n°2018-342 [4], portant un avis sur le projet ALICEM. Dans cette délibération, comme la reconnaissance faciale est obligatoire et qu'il n'existe aucune autre alternative pour se créer une identité via ALICEM, la CNIL annonce clairement : "le consentement au traitement des données biométriques ne peut être regardé comme libre et comme étant par suite susceptible de lever l'interdiction posée par l'article 9.1 du RGPD". Malgré cet avis, et les autres propositions alternatives de la CNIL (identification par données biométriques), le gouvernement n'a pas fait suite.

Le projet ALICEM suit une démarche expérimentale encadrée par la loi, toutefois, on peut se poser quelques questions quant au respect des exigences de la CNIL. En effet, en **imposant la reconnaissance faciale pour les utilisateurs d'ALICEM**, il y a un risque de **normaliser cette technologie** comme un outil d'identification, en passant outre la seule condition qui devrait être acceptable pour son utilisateur : **le consentement libre et explicite**. De plus, comme exigé par la CNIL, l'expérimentation doit avoir une finalité précise, légitime et souhaitable (par exemple : assurer un haut niveau de fiabilité dans l'identification/authentification de personnes), et assurer la sécurité des données des utilisateurs. Hors la finalité d'ALICEM par le gouvernement reste ambiguë. Dans son rapport intitulé : "État de la menace liée au numérique en 2019", l'ancien ministre de l'intérieur Christophe Cazenave affirme que l'anonymat d'internet : "L'anonymat protège tous ceux qui répandent des contenus haineux et permet à des faux-comptes de se multiplier pour propager toutes sortes de contenus."

ALICEM est donc vu par le gouvernement comme un outil potentiel **pour identifier les citoyens sur internet** : cet outil permettrait donc de lutter contre l'anonymat en ligne, pourtant fondamental pour l'exercice de nos droits sur internet. Ainsi, la Quadrature du net a déposé un recours devant le Conseil d'État en 2019 pour demander l'annulation du décret autorisant la création de l'application mobile intitulée "ALICEM" pour motif de banalisation de cette technologie.

La société se divise sur cette problématique : certains voient un intérêt à cette technologie alors que d'autres y perçoivent surtout les risques et dangers qu'elle fait courir aux individus. Malgré la mise en place d'un cadre expérimental par la CNIL, **ce dernier reste fragile et n'est pas toujours respecté**. Hors, on peut se poser des questions quant à l'utilisation par l'état de cette technologie. En effet, cette méthode est très efficace mais elle repose sur une technologie probabiliste, et donc potentiellement défaillante.

2.2 La Méconnaissance faciale

2.2.1 Les problèmes algorithmiques

Malgré l'avancée qu'a connue la reconnaissance faciale durant ces dernières années, elle reste tout de même probabiliste et n'est, à ce jour pas fiable à 100%. En effet cette dernière doit prendre en compte différents facteurs ayant un impact sur un visage comme le vieillissement, la chirurgie plastique, le maquillage, les effets de la consommation de drogues ou de tabac... Nous allons donc voir quelques exemples de la faillibilité de ces algorithmes :

- **Royaume-Uni** : une expérience menée par la police britannique a montré que les faux positifs sont nombreux alors que le taux de reconnaissance est très bas, cela a même entraîné des interventions infondées de la police d'après le Big Brother Watch [2] [12].
- **Londres** : en 2017, lors du carnaval de Notting Hill, une expérience de vidéosurveillance intelligente a causé l'arrestation de 36 personnes dont 35 non recherchées et une mise hors de cause dans une affaire dont le visage est resté dans la base de données des forces de l'ordre [11].
- **Etats-Unis** : en juillet 2018, l'association American Civil Liberties Union a comparé les photos des membres du Congrès à un fichier de 25 000 délinquants pris par la police, grâce au logiciel d'Amazon « Rekognition » : 28 membres du Congrès ont été identifiés comme délinquants, cela a permis de démontrer le manque de fiabilité de cette technologie car

2. Militant contre l'utilisation de la reconnaissance faciale

c'était des faux positifs [1].

— **Michigan** : en juin 2020 à Detroit, un Africain-Américain du nom de Robert Williams avait été identifié comme le malfaiteur d'un vol à l'étalage, suite à son identification par un algorithme de reconnaissance faciale dans une vidéo floue. La police chargée de l'affaire s'est rendue compte de son erreur et a finalement demandé des excuses en le relâchant après plusieurs heures [15].

2.2.2 La discrimination dans la reconnaissance faciale

Les exemples précèdents ont pu démontrer l'envergure des erreurs des algorithmes de la reconnaissance faciale. Néanmoins, les erreurs sont plus présentes à l'encontre des personnes de couleur, et c'est ce que souligne un article de chercheurs du MIT et de l'Université de Stanford.

En effet, lors des expériences, les chercheurs ont pu remarqué qu'un homme blanc a des taux supérieurs ou égaux à 80% de réussite contrairement à une femme noire, dont le taux d'erreur atteignait 34% [6].

Une autre recherche du NIST, National Institute of Standards and Technology, a elle aussi pu démontrer que les deux plus grands problèmes sont l'ethnie et le genre. Cette étude a évalué 189 algorithmes et logiciels de 99 développeurs et a pu démontrer ce qui suit :

— Pour l'appariement un à un, l'équipe a constaté des taux plus élevés de faux positifs pour les visages asiatiques et afro-américains par rapport aux images de caucasiens.

— Parmi les algorithmes développés aux États-Unis, il y avait des taux similaires de faux positifs dans les correspondances un à un pour les Asiatiques, les Afro-Américains et les groupes autochtones. Cependant, une exception notable a été remarqué pour certains algorithmes développés dans les pays asiatiques.

— Pour l'appariement un-à-plusieurs, l'équipe a constaté des taux plus élevés de faux positifs chez les femmes afro-américaines. Cependant, tous les algorithmes ne donnent pas ce taux élevé de faux positifs dans toutes les données démographiques dans le cadre d'une correspondance un-à-plusieurs [7].

2.2.3 Les failles exploitables de la reconnaissance faciale

Comme vu précédemment, l'algorithme de reconnaissance faciale n'est pas toujours fiable car il est probabiliste, mais il existe un autre facteur d'échec de ce dernier et c'est l'homme.

Il existe deux types d'attaques, l'une utilisant l'intelligence artificielle et l'autre tout simplement le maquillage.

L'IA : Des chercheurs ont montré qu'ils peuvent faire croire à un système de reconnaissance faciale qu'il voyait une personne qui n'était pas celle présentée. Pour ce faire, ils ont eu recours à l'apprentissage automatique pour créer une image nous faisant reconnaître un individu A, mais faisant reconnaître à la machine un individu B. Les chercheurs ont employé un CycleGAN, un réseau de neurones particulièrement performant dans la transformation d'images d'un style en un autre. Par exemple, une photographie peut être transformée en tableau d'un peintre au style bien connu. Ils ont donc utilisé 1500 images pour en générer de nouvelles. En même temps, le système de reconnaissance faciale reconnaissait les images. Les chercheurs n'avaient alors plus qu'à comparer le généré avec le reconnu, et ont ainsi pu générer une image trompant le système de reconnaissance. Ce genre d'attaques soulèvent de grandes préoccupations. Pourtant, il y a quelques réserves. En effet les pirates n'auraient pas accès au système de reconnaissance faillible, et ne pourraient donc pas générer d'image induisant en erreur ce système ci. En revanche, les chercheurs pensent qu'avec une probabilité non négligeable une image puisse être générée,

trompant deux systèmes de reconnaissance différents. De plus, ce genre d'attaque est très lourde à réaliser et demande beaucoup de ressources [9].

La technique dazzle : C'est un type de camouflage développé par les forces navales durant la Seconde Guerre mondiale utilisant des motifs d'inspiration cubique pour brouiller les formes, la taille et l'orientation des navires de guerre. Repris sur le visage humain, ce dernier empêche l'algorithme d'accéder au profil biométrique de la personne en peignant de riches pigments dans des formes cubistes sur les principales caractéristiques du visage [14].

3 Utilisation de la reconnaissance faciale dans l'espace public : opportunités et menaces

La reconnaissance faciale remplit deux fonctions distinctes, authentification et identification, et chacune d'elle apporte son lot d'opportunités en terme d'usage mais soulève des enjeux différents.

3.1 Authentification

3.1.1 Qu'est-ce que c'est ?

Comme dit précédemment, l'authentification permet de vérifier l'identité d'une personne. Elle s'applique donc lorsque l'on connaît déjà la personne. Elle est fréquemment utilisée pour l'accès à des services ou des applications dans un cadre purement domestique, comme le déverrouillage des smartphones, ou commercial, avec notamment l'ouverture d'un compte bancaire à distance.

L'authentification par reconnaissance faciale agit non seulement comme une solution de sécurité supplémentaire aux mots de passe et de vérification de l'identité par SMS, mais aussi comme un facteur de certification fort et automatisé. La raison de ce choix réside dans les données en elle-même : l'authentification traite des données biométriques, qui sont uniques, propres et permanentes dans le temps à chaque personne, donc théoriquement difficilement falsifiable.

3.1.2 Quelques cas d'usages et leurs avantages

L'authentification par reconnaissance faciale se développe rapidement en France, et notamment pour le contrôle aux frontières et dans les aéroports. Depuis 2009 avec PARAFE [10] et début octobre 2020 avec MONA [8], les voyageurs peuvent désormais passer par un système de contrôle automatisé des passeports et papiers d'identité sur présentation de leur visage dans certains aéroports et gares de France. Derrière ce système se trouve Idemia, entreprise française spécialisée dans la reconnaissance faciale, et dont la technologie a été vendue au gouvernement chinois et aidera à la gestion de foule pour les Jeux olympiques de 2024. Cette dernière peut représenter une opportunité pour Idemia, et donc la France, de gagner en compétitivité dans la course mondiale à l'intelligence artificielle grâce au cadre expérimental qui lui est offert.

Autre exemple d'authentification pour s'assurer de l'identité d'une personne est l'application Alicem, un outil d'identité numérique avec reconnaissance faciale obligatoire. Les partisans de son développement voient en ces cas d'usages un moyen de sécurisation forte et des opportunités pour expérimenter et perfectionner cette technologie.

3.1.3 Risques possibles engendrés

D'autres arguments sont avancés par les opposants. Technopolice, qui a récemment publié un état des lieux de l'utilisation de la reconnaissance faciale en France [13], souhaite que l'on reste vigilant quant à son application pour prouver son identité et mentionne également un véritable risque d'accoutumance pour la société face aux contrôles automatisés.

Bien que les données ne sont pas récupérées dans le cadre du contrôle automatique dans les aéroports [5], la CNIL rappelle que la reconnaissance faciale n'est jamais un traitement anodin. Les données biométriques sont des données sensibles, qui malgré un usage légitime, consenti et bien cadré, ne sont pas à l'abri en cas de cyberattaque ou d'erreurs [3].

3.2 Identification

3.2.1 Qu'est-ce que c'est ?

Un autre cas d'application de la reconnaissance faciale est l'identification. Si l'authentification vise à faire la comparaison de deux visages pour donner des accès, l'identification elle, consiste en la distinction de personnes parmi d'autres. Cet usage permettrait par exemple de retrouver une personne à travers ses propres caractéristiques physiques dans une foule de personnes.

3.2.2 Quelques cas d'usages et leurs avantages

Grâce à l'identification, les opportunités sont nombreuses quant à l'utilisation de la reconnaissance faciale. Elle permettrait de retrouver des personnes dangereuses pour la population. Cette technologie pourrait être utilisée par les forces de police du pays pour assurer encore mieux leur rôle et garantir davantage la sécurité de la population. Elle servirait, par exemple, à la recherche de délinquants en fuite ou à la reconnaissance de personnes en situation de délit. A ces cas d'usage, nous pourrions aussi noter le suivi du parcours d'un passager dans les transports, le suivi des déplacements d'une personne dans l'espace public et encore de nombreux autres cas d'usage dont la validité n'a pas encore été évaluée.

En outre, grâce à l'identification il serait possible de surveiller toute la population et donc les inciter à ne pas commettre de faute sanctionnable (ce qui implique la sécurité de tous). Les vidéos de surveillance furent utilisées à cet effet lors du Carnaval de Nice qui accueille annuellement environ 200 000 personnes. Etant le plus grand événement de France, il requiert le maximum de précautions et de mesures pour garantir la sécurité de ses invités. Pour l'événement, la technologie n'a pas été appliquée sur l'ensemble des spectateurs en raison des limites imposées par la protection des données.

Malgré tous les avantages que l'on peut tirer de son utilisation, l'identification présente des failles qui pourraient nuire à la population.

3.2.3 Quelques risques, notamment pour la liberté des citoyens

Même si elle présente des opportunités intéressantes, l'identification est la technique la plus controversée de la reconnaissance faciale. En effet, il s'agit ici de bases de données contenant des images (informations/caractéristiques) de beaucoup de personnes. Plusieurs questions relatives à la protection de ces données sont ainsi soulevées : par rapport à la durée de vie des données, aux personnes qui y auront accès, le type de données stockées... La CNIL considère que ce sont des questions qu'il faut se poser avant de mettre en pratique l'usage de cette technologie.

Car, il ne faut pas oublier que le plus important c'est la liberté, la sécurité des personnes et la bonne gestion de leurs données sensibles priment.

Par ailleurs, des inquiétudes sont soulevées par l'incertitude relative liée à l'utilisation de la reconnaissance faciale. Dès lors que le jugement derrière cette technologie n'est pas absolue mais relative, elle représente des risques de défaillance. Prenons le cas par exemple de la reconnaissance d'un délinquant. L'algorithme fournirait en sortie une probabilité significative de la ressemblance. Quand bien même cette probabilité serait de 99%, il reste 1% de chance qu'elle se trompe dans son jugement. Ce trait probabiliste rend la CNIL et les autorités davantage dubitatives à son usage.

Conclusion

La reconnaissance faciale est un marché en pleine expansion, tout particulièrement depuis 2016. Mais cette technologie suscite aujourd'hui autant de craintes que de fantasmes. Afin de ne pas tomber dans des dérives, il est aujourd'hui plus que nécessaire d'encadrer strictement son utilisation. Le champs des possibles de la reconnaissance faciale semble vaste, mais l'Europe et la France en particulier restent relativement frileux sur ce sujet, souhaitant le moins possible reproduire certains usages déraisonnés que l'on peut observer dans d'autres pays. En effet, le marché de la reconnaissance faciale est largement dominé par les entreprises américaines, chinoises et japonaises. Aujourd'hui nous observons parfois dans ces pays des pas en arrière sur le sujet, c'est notamment le cas à San Francisco. En plus de se protéger d'une possible privation de certains de nos droits fondamentaux, il faut rester méfiant sur ces technologies, puisque la reconnaissance faciale reste basée sur des probabilités, et pourrait même être utilisée à mauvais escient, en plus de reproduire certains biais humains (même de manière involontaire). En France, la régulation passe aussi par des expérimentations qui doivent être encadrées et répondre à des exigences citées par la CNIL. Néanmoins, il est important de garder en tête que cela reste des expérimentations, le but n'étant pas d'acclimater la population à l'usage de la reconnaissance faciale de manière ordinaire. Par ailleurs, tout ce qui est possible n'est pas forcément souhaitable. Et en voulant améliorer un petit point avec la reconnaissance faciale, il est possible de s'attirer davantage de problèmes sur un autre sujet par la même occasion. Il faudra donc rigoureusement déterminer quels usages de cette technologie sont réellement souhaitables.

Malgré tout, ces précautions ne suffisent parfois pas, et nous avons déjà pu observer en France des polémiques au sujet de la reconnaissance faciale, par exemple avec ALICEM. Par ailleurs, être si frileux sur certains sujets peut conduire à un retard technologique, ce qui peut également être regrettable.

Quelles que soient les ambitions apportées par les possibilités de la reconnaissance faciale, il faudra veiller à rester dans le cadre de l'article 1er de la loi Informatique et libertés : "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".

Références

[1] *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[2] Pierre Legros Caroline Lequesne Roth Mehdi Kimri. "La Reconnaissance Faciale dans l'espace public - Une cartographie européenne." Thèse de doct. 2020.

[3] CNIL. *Reconnaissance faciale : pour un débat à la hauteur des enjeux*. https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux. Nov. 2019.

[4] *Délibération n° 2018-342 du 18 octobre 2018*. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038477075/. Page consultée le 25 novembre 2021. 2018.

[5] *Le passage rapide aux frontières extérieures (PARAFE)*. https://www.immigration.interieur.gouv.fr/Europe-et-International/La-circulation-transfrontiere/Le-passage-rapide-aux-frontieres-exterieures-PARAFE. Page consultée le 25 novembre 2021. Mai 2020.

[6] *MIT. Study finds gender and skin-type bias in commercial artificial-intelligence systems*. https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212/.

[7] *NIST. NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Déc. 2019.

[8] *Nos passagers ont vécu une première mondiale à Lyon... Lancement de Mona, le nouveau compagnon de voyage basé sur la reconnaissance faciale*. https://www.lyonaeroports.com/actualites/nos-passagers-ont-vecu-une-premiere-mondiale-lyon. Page consultée le 25 novembre 2021. 2020.

[9] *OWDIN. Le hack qui pourrait faire croire à la reconnaissance faciale que quelqu'un d'autre est vous*. https://owdin.live/2020/08/06/le-hack-qui-pourrait-faire-croire-a-la-reconnaissance-faciale-que-quelquun-dautre-est-vous/?fbclid=IwAR0ZwW6Es9W6aRT7dIoaAixs4HGbSLoM6Uay6gyFOOxKp2mpkmm7nsImWLY. Août 2020.

[10] *PARAFE en vol de croisière*. https://www.interieur.gouv.fr/Archives/Archives-des-dossiers/2011-Dossiers/PARAFE-en-vol-de-croisiere. Page consultée le 25 novembre 2021. 2011.

[11] *Police facial recognition trial led to erroneous arrest*. https://news.sky.com/story/police-facial-recognition-trial-led-to-erroneous-arrest-11013418. 2017.

[12] *Stop Facial Recognition*. https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/.

[13] *Tentative d'état des lieux de la reconnaissance faciale en France en 2021*. https://technopolice.fr/blog/tentative-detat-des-lieux-de-la-reconnaissance-faciale-en-france-en-2021/. Page consultée le 25 novembre 2021. Juin 2021.

[14] *VOGUE. Oui, il existe un moyen de déjouer la technologie de reconnaissance faciale, et cela se résume à votre maquillage*. https://www.vogue.com/article/computer-vision-dazzle-anti-surveillance-facial-recognition-technology-moma-ps1. Mars 2018.

[15] *Wrongfully accused by an algorithm.* https://www.seattletimes.com/business/technology/wrongfully-accused-by-an-algorithm/. 2020.