Strasbourg, 13 novembre 2019

T-PD(2019)05rev

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL

CONVENTION 108

LA RECONNAISSANCE FACIALE : ÉTAT DES LIEUX ET ENJEUX

par

Sandra Azria et Frédéric Wickert

DG I – Droits de l'Homme et État de droit

Les opinions exprimées dans ce document sont de la responsabilité des auteurs et ne reflètent pas nécessairement la politique officielle du Conseil de l'Europe.

ASPECTS TECHNIQUES

Par Frédéric Wickert
Conférencier/Consultant/Conseiller/Formateur en Intelligence artificielle
Fondateur d'A.I. SENSE

1. INTRODUCTION

Techniquement, la reconnaissance faciale est un sous ensemble d'un domaine de l'intelligence artificielle[1] : « la vision par ordinateur ».
Ce domaine a pour objectif de créer des « algorithmes » pour extraire de l'information venant d'images comme identifier des objets (avec des mots clés, des tags), détecter des objets avec leur position dans l'image, détecter des marques, catégoriser des images, décrire des images, détecter des visages, détecter des célébrités ou des éléments géographiques, détecter les jeux de couleurs, détecter du texte, détecter des images inappropriées. Mais également analyser des visages (genre, émotions, ou port d'accessoires, …) et identifier des visages : la reconnaissance faciale. C'est sur ces derniers points que porte le contenu de ce rapport.

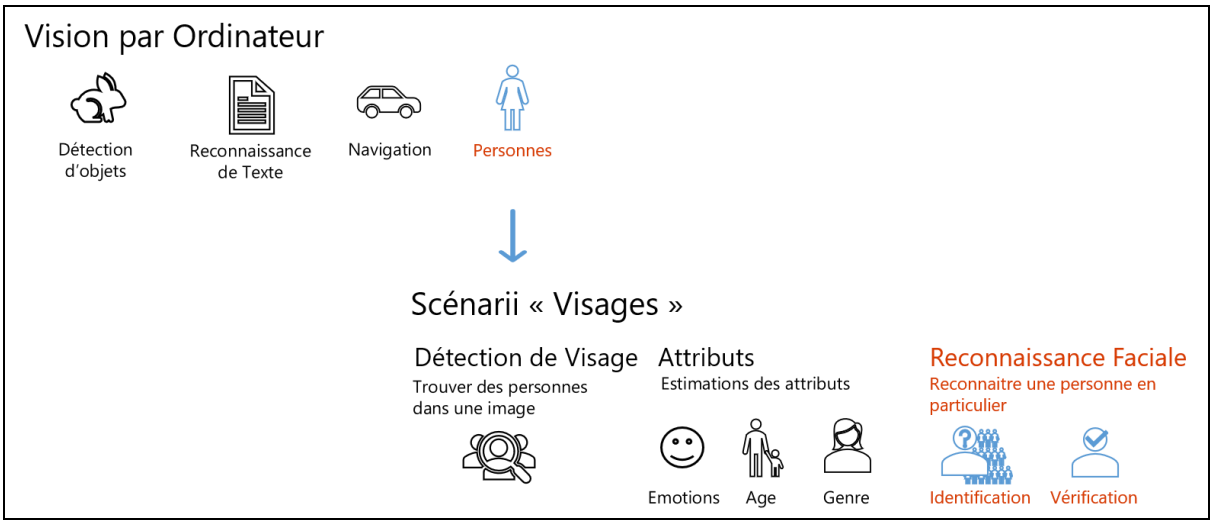

Figure 1 : Vision par ordinateur

2. FONCTIONNEMENT GÉNÉRAL

Pour réaliser les scénarii ci-dessus, il est très difficile de développer un algorithme déterministe[2], qui demanderait à un développeur une gestion quasi infinie des possibilités apportées par le volume et la variété d'images sur lesquels établir son algorithme. Et même s'il y arrivait avec une image, son algorithme ne serait pas adapté à d'autres images. Et puis selon vous, comment doit-on coder le fait de détecter un visage sur une photo ? Quelles sont les combinaisons de pixels qui font qu'on peut déduire qu'il y a ou non un visage sur une image ?
La solution à ce problème est d'utiliser des principes d'intelligence artificielle, des algorithmes basés sur le *Deep Learning*, sur les réseaux de neurones profonds (*Deep Neural Network*).

[1] Le terme « intelligence artificielle » est à la mode et nombre d'entreprises du service numérique mettent en avant leurs activités « d'intelligence artificielle ».
Or si l'on regarde en détail, la majorité développe des solutions de « Business Intelligence» ou font de la « science de la donnée » (sans algorithmes de prédiction). Il est d'ailleurs difficile d'avoir aujourd'hui une cartographie des acteurs de l'intelligence artificielle, de leur champ d'application et d'intervention, de leur valeur éthique autour de l'intelligence artificielle, etc…

[2] Les mêmes qui sont utilisés pour des applications de gestion par exemple, avec une utilisation des instructions conditionnelles, les « si » et avec des boucles, les « tant que » par exemple, etc.

L'idée ici n'est pas de rentrer dans le détail du fonctionnement de *Deep Learning* mais uniquement d'éclaircir certains points.
Premièrement, la différence que l'on peut noter par rapport à notre algorithme « déterministe », c'est que les algorithmes, les techniques d'intelligence artificielle sont « probabilistes ». On dit qu'ils sont « stochastiques »[3].

C'est un point important ; on ne peut jamais demander à un algorithme d'intelligence artificielle d'avoir une réponse fiable à 100%. Le contraire serait totalement utopique.

Deuxièmement, pour apporter une réponse la plus précise possible, l'algorithme doit apprendre à apporter la bonne réponse. Par exemple, « apprendre à détecter un visage sur une photo ». « Apprendre », cela signifie ici que c'est le réseau de neurones qui va construire le « modèle »[4] pour détecter un visage. Pour cela, on va lui donner des informations en entrées : des images et la réponse. Par exemple 10 millions de photos avec la réponse : « Oui, il y a un visage » et également des photos sans visage.

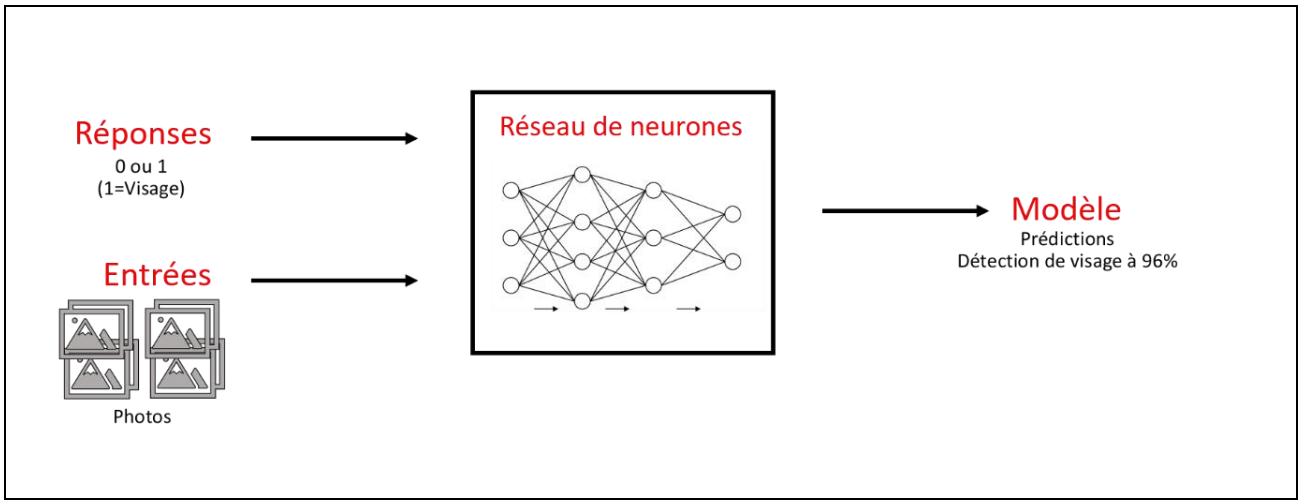

Figure 2 : Apprentissage d'un réseau de neurones

Ainsi, le réseau de neurones va apprendre (d'où le terme de *Deep Learning*) comment détecter un visage sur une photo en se basant sur des données dites d'entrainement. Ce processus, la création du modèle, peut durer quelques heures comme quelques jours, semaines, voire quelques mois. (Cela dépend du nombre d'images dans le jeu d'entrainement, de la complexité de ce qu'on lui demande et du niveau minimum de fiabilité que l'on souhaite).

On répète ce processus pour les autres cas d'usage (analyser des visages : émotions, âge, genre, etc..).

Une fois l'entrainement terminé, une fois le modèle créé donc, nous pouvons le mettre à disposition pour des développeurs qui peuvent intégrer la fonctionnalité dans une application (web, mobile, caméra ou autre). Il s'agit d'un cycle itératif.

[3] C'est-à-dire que le résultat sera une probabilité d'exactitude de la réponse. L'objectif étant de se rapprocher de 100%. « Je suis sûr à 87% que sur cette image il y a un visage et sûr à 67% qu'il sourit. »
[4] Le modèle sera l'algorithme finalisé qui répondra à la solution avec un certain niveau de précision.

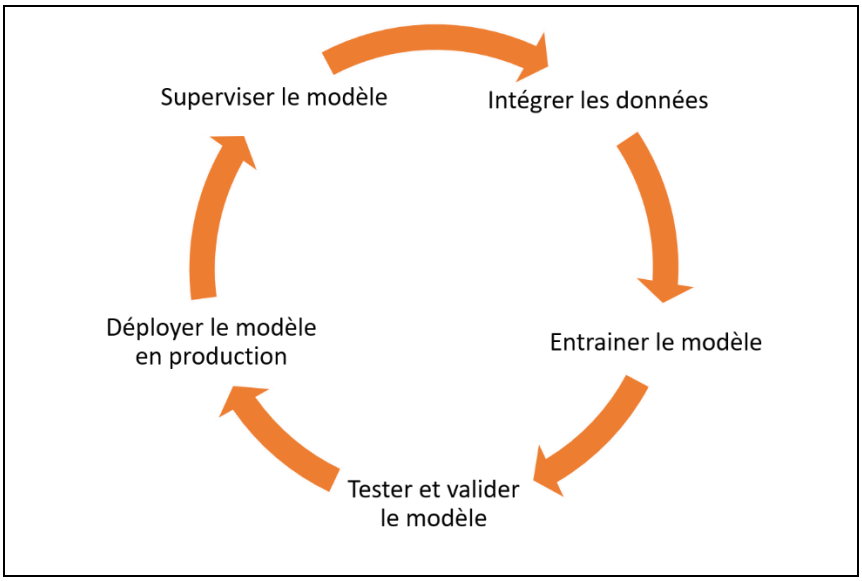

Figure 3 : Cycle itératif de développement d'un modèle intelligence artificielle

Pour chaque version du modèle, on peut y intégrer de nouvelles photos, utiliser une autre architecture de réseaux de neurones. Cela influencera le résultat en ayant pour objectif d'améliorer le pourcentage de fiabilité et de minimiser les biais.

3. PROFILS TECHNIQUES NÉCESSAIRES

On peut décomposer le savoir-faire de la création d'algorithmes de détection de visage, d'analyse des visages ou de reconnaissance faciale en 3 types de profils : les chercheurs en intelligence artificielle, les *data scientists* et les développeurs.

Les chercheurs en intelligence artificielle vont déterminer l'architecture des réseaux de neurones et le comportement des neurones qui fonctionnent le mieux pour un usage spécifique.[5]
Le d*ata scientist* va intégrer les données (les photos et les réponses) et utiliser ces architectures pour créer le programme qui va générer le modèle. Puis il va déployer le modèle.
Les développeurs vont utiliser le modèle créé pour intégrer la fonctionnalité dans leur application.

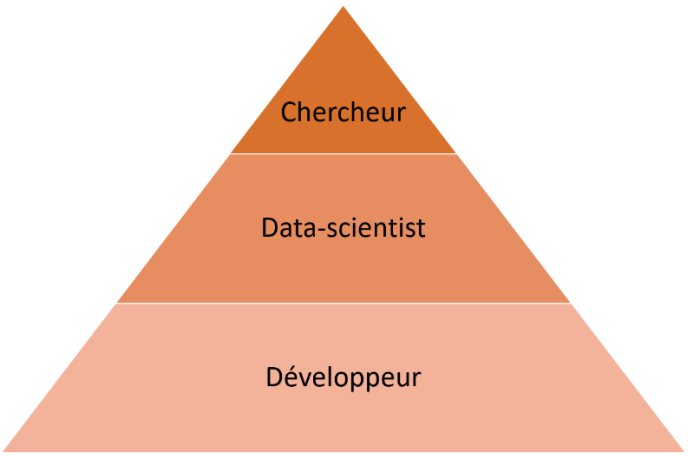

Figure 4 : Pyramide qui représente aussi la quantité de profils.

Même si ces trois profils sont complémentaires, il n'est pas nécessaire de les employer dans la même entreprise ou dans la même collectivité.

[5] On retrouve le « bestiaire » des architectures de réseaux de neurones ici : http://www.asimovinstitute.org/neural-network-zoo/

La majorité des chercheurs en intelligence artificielle sont dans des laboratoires universitaires ou dans de grands groupes privés comme les GAFA(MI) (aux États-Unis) ou les BATX (en Chine). Leurs *data scientists* mettent leurs modèles à disposition des développeurs du monde entier (gratuitement ou non).

Il existe donc deux possibilités, construire son propre modèle ou utiliser des modèles déjà entrainés.

4. CONSTRUIRE SON MODÈLE

Pour construire son propre modèle, par exemple pour détecter un visage sur une photo (c'est la base pour pouvoir ensuite faire de la reconnaissance faciale), il faut :

- un jeu de données : des photos de visages et les réponses (les labels) ;
- des ordinateurs puissants pour entrainer son modèle ;
- des ordinateurs pour déployer le modèle pour qu'il soit utilisé.

4.1 Jeux de données

On peut trouver des jeux de données sur beaucoup des plateformes et vous trouverez sur « face-rec » (http://face-rec.org/databases/) une liste de jeux de données spécifiquement pour la reconnaissance faciale. Ces jeux de données contiennent des photos et des labels (les réponses) pour entrainer l'algorithme de *Deep Learning*. Il faut dans ce cas gérer ces données, c'est-à-dire gérer leur cycle de vie : récupérer les données, les stocker, les auditer, les sécuriser, etc, en respectant le RGPD.

4.2 Entrainement

Pour entrainer un modèle d'intelligence artificielle on utilise des machines puissantes qui sont composées d'éléments techniques spécifiques (carte graphique GPU et des processeurs de nouvelles générations comme les FPGA ou TPU[6]).
On peut bien entendu acheter ce type de machines ou les louer chez un fournisseur de Cloud public comme Amazon Web Service, IBM ou Microsoft (pour les FPGA) et Google (pour les TPU).
Pour simplifier la création des modèles, on utilise des bibliothèques (souvent *OpenSource*) tels que OpenCV, Tensorflow, CNTK et bien d'autres[7].

4.3 Déploiement

On peut déployer le modèle sur une application Web, dans une application mobile (iOS ou Android) ou sur des objets connectés tels des caméras ou des drones.

Dans tous les cas, construire soi-même son modèle représente un savoir-faire non négligeable et fait appel au métier de *data scientist.*

5. UTILISER DES MODÈLES ENTRAINÉS

Si l'on n'a pas les données ou les compétences pour créer son propre modèle, il y a tout de même une solution pour utiliser la reconnaissance faciale (et tout autre modèle sur les visages). Certaines entreprises mettent à disposition leurs modèles entrainés sous forme de Web API, accessibles à toutes les développeuses et tous les développeurs. C'est le cas de certains des GAFAMI[8] comme Amazon Web Service (https://aws.amazon.com/fr/rekognition/) et Microsoft (https://azure.microsoft.com/en-us/services/cognitive-services/face/) ou également la société Kairos (https://www.kairos.com).

Voici un exemple d'utilisation d'une de ces APIs avec une application « Microsoft Kiosk ».

[6] FPGA : https://fr.wikipedia.org/wiki/Circuit_logique_programmable et TPU https://fr.wikipedia.org/wiki/Tensor_Processing_Unit
[7] Quelques projets « *OpenSource* » utilisant ces bibliothèques : https://awesomeopensource.com/projects/face-detection
[8] Google, Apple, Facebook, Amazon, Microsoft, IBM

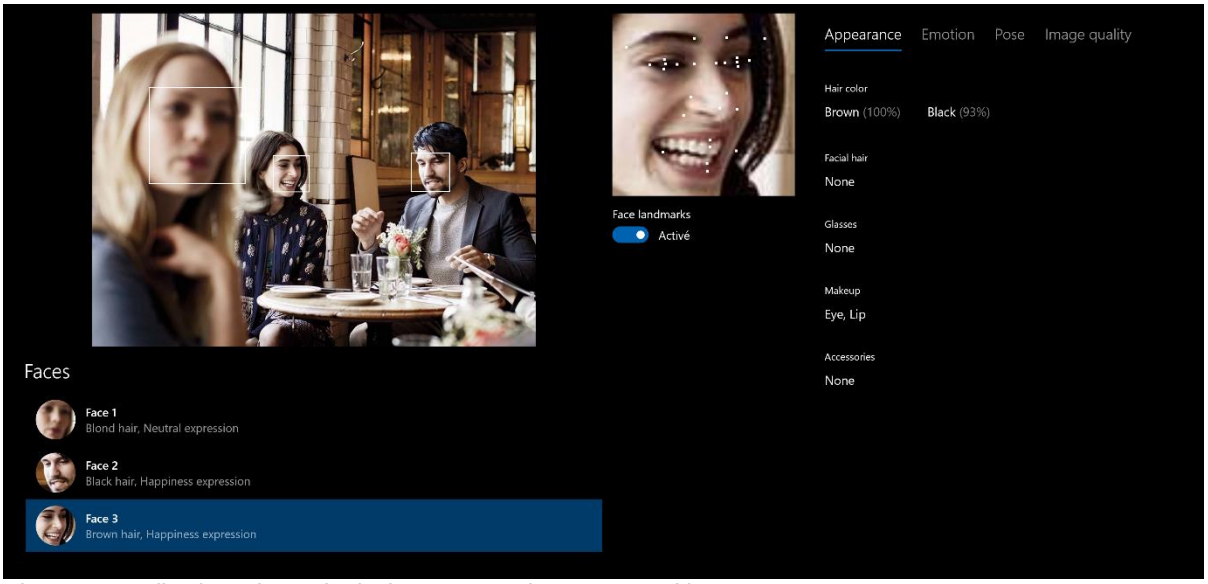

Figure 5 : Application Microsoft Kiosk pour tester les APIs cognitives

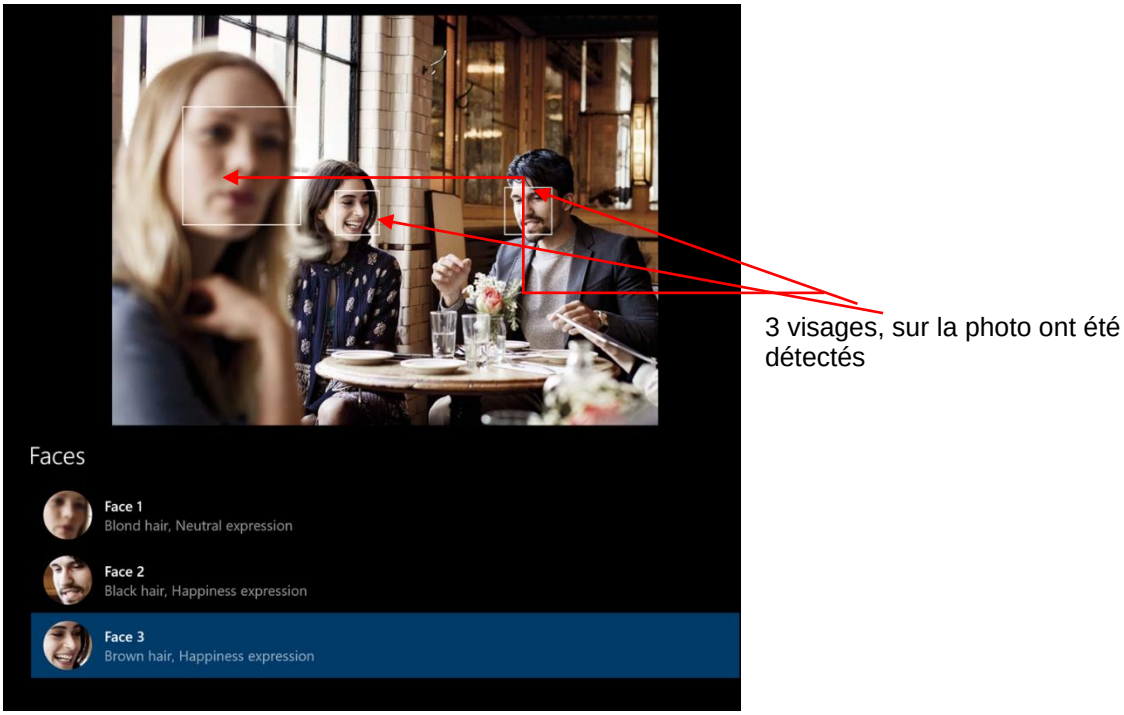

Figure 6 : Détection de visages

5.1 Apparence

- 27 points déterminent le visage, la position des yeux, du nez, de la bouche.
- La couleur des cheveux
- Si des cheveux sont devant le visage
- Les accessoires comme les lunettes
- Le maquillage des lèvres et des yeux par exemple.

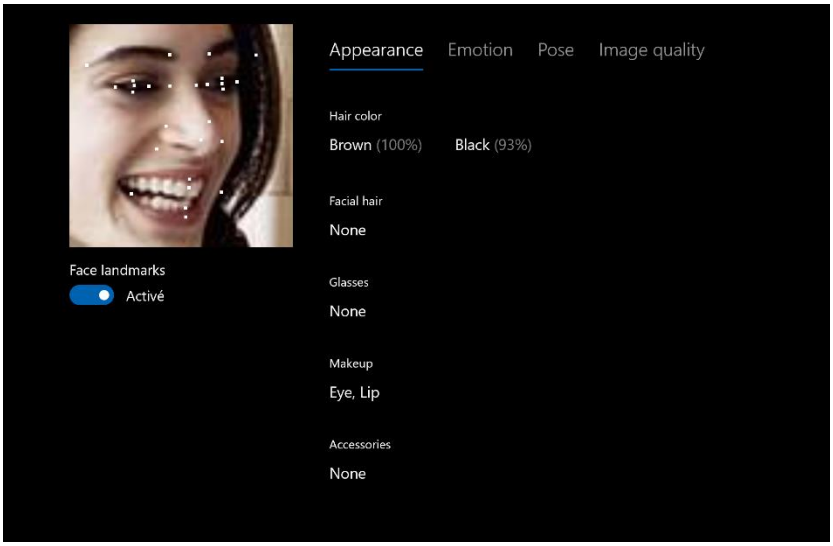

Figure 7 : Analyse de l'apparence

5.2 Émotions

8 émotions peuvent être détectées : la joie (ici 100%), la colère, le mépris, le dégout, la peur, la tristesse, la surprise ou la neutralité

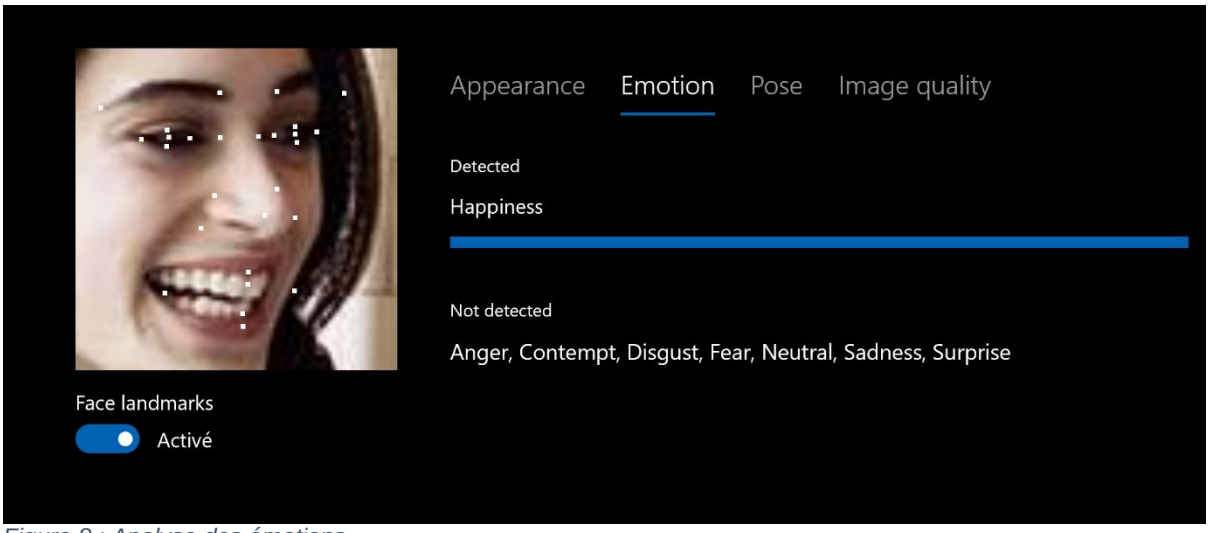

Figure 8 : Analyse des émotions

5.3 Position

La position de la tête :

- l'inclinaison de la tête
- l'angle du menton
- la rotation du visage

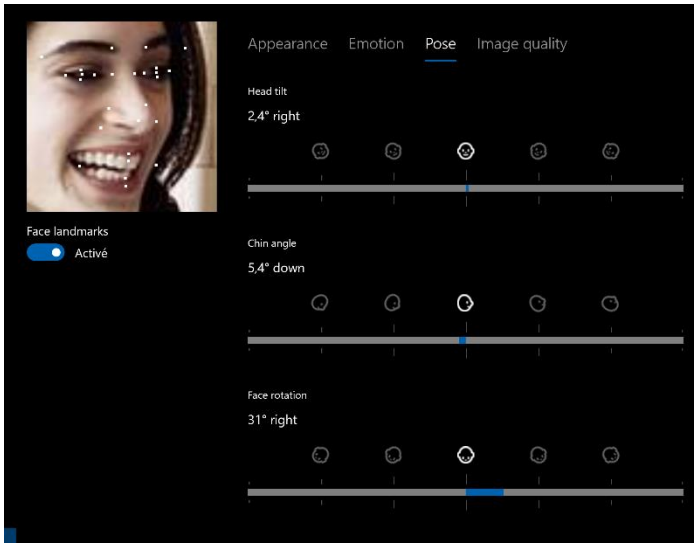

Figure 9 : Analyse de la position de la tête

5.4 Qualité

La qualité de l'image :

- l'exposition
- le flou
- le bruit
- l'occlusion

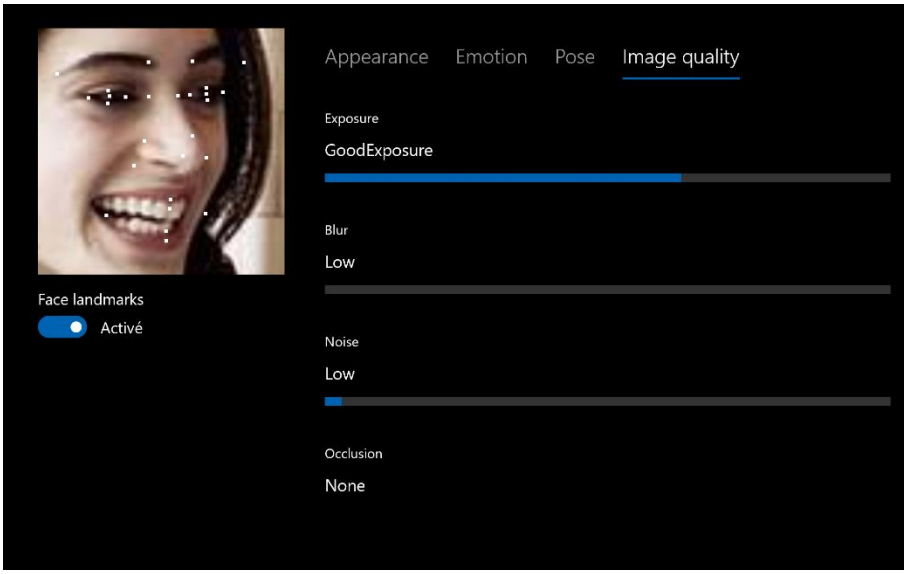

Figure 10 : Analyse de la qualité de l'image en entrée

Ici, il n'y aucun entrainement à faire pour le développeur, juste à envoyer une image pour obtenir tous ces détails. C'est très simple d'utilisation et peut s'intégrer dans n'importe quelle application : application Web, application mobile, caméras, drones, etc.

6. IDENTIFICATION

Nous avons vu comment les algorithmes permettent aujourd'hui de récupérer beaucoup d'informations sur les visages d'une photo ou d'une vidéo. Pour faire de l'identification il suffit de comparer un visage trouvé sur une photo avec des images dans une base de données.

Une étape intermédiaire doit alors avoir lieu. Celle d'entrainer un modèle avec des photos de visages et leur nom (ou identifiant). Une photo peut suffire pour ensuite faire de l'identification. Évidemment, plusieurs photos vont permettent une meilleure identification (surtout avec des angles de prises de vue différents).

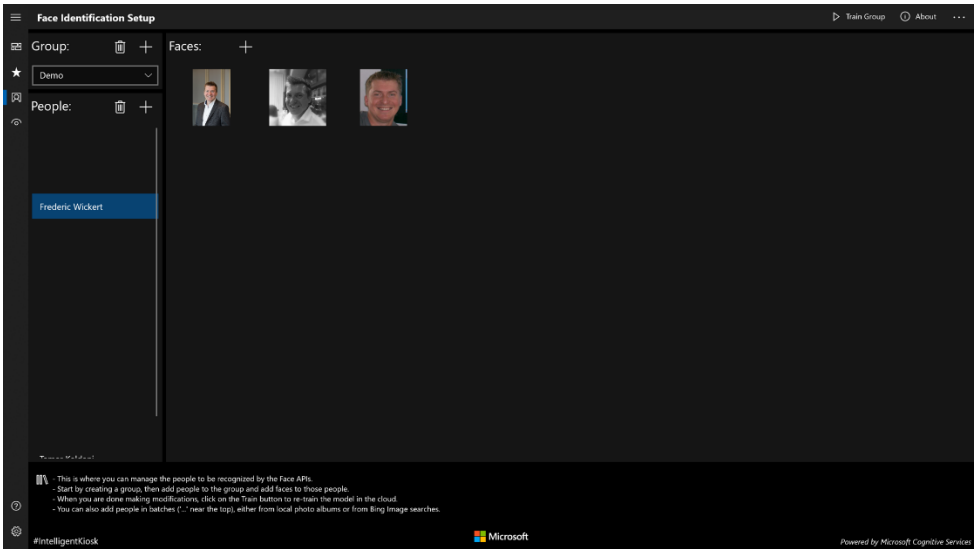

Figure 11 : 3 visages ici pour entrainer la reconnaissance de cette personne

Une fois les visages et les réponses renseignés, l'entrainement va prendre quelques secondes. Ensuite l'identification est possible.

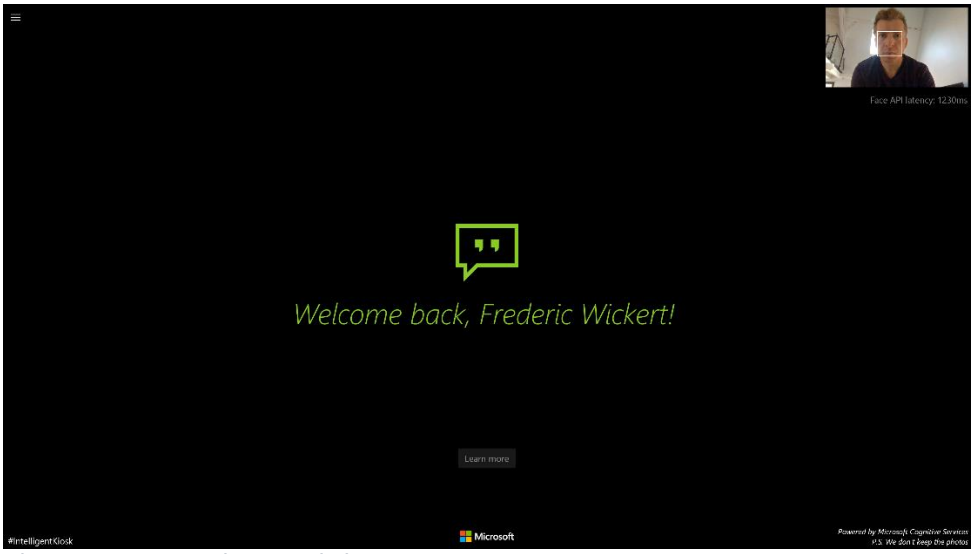

Figure 12 : Reconnaissance de la personne

Un pourcentage de fiabilité de l'identification est également récupéré. Ce qui permet d'être plus strict sur le niveau d'exigence attendu de l'identification. Dans la figure 13, on peut constater une fiabilité de reconnaissance faciale de 93% (ainsi que l'âge et l'émotion).

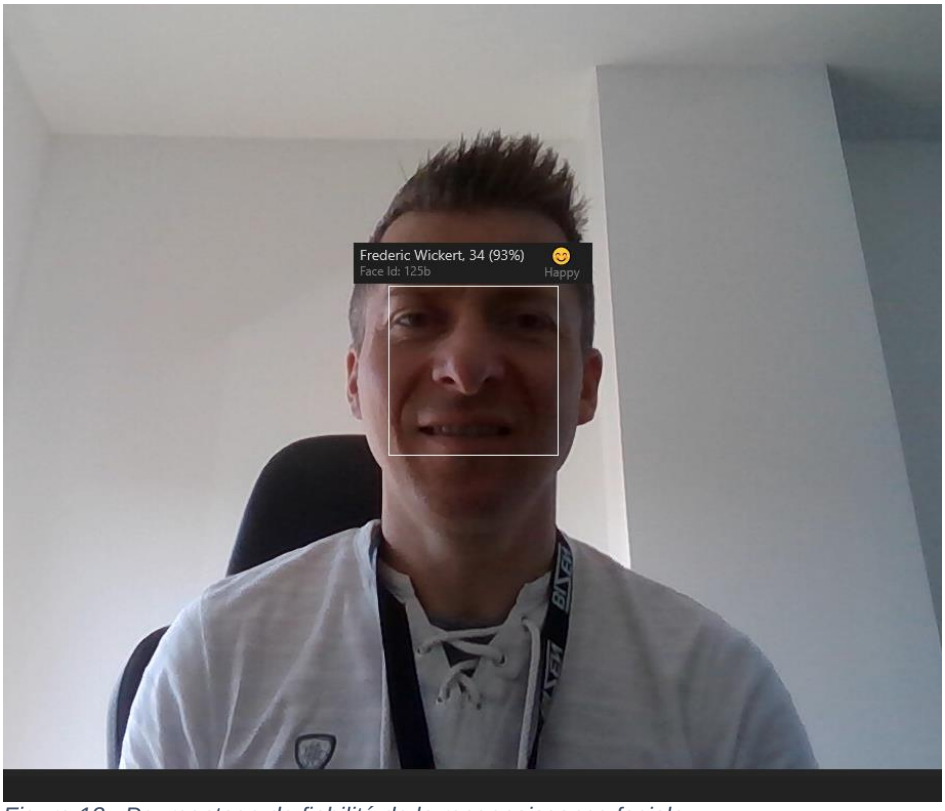

Figure 13 : Pourcentage de fiabilité de la reconnaissance faciale

7. CAMÉRA

La qualité de l'identification dépend de la photo en entrée. Dans ce scénario, la photo en entrée est générée par une caméra et envoyée au service d'identification. De ce fait, la qualité de la caméra joue un rôle essentiel.
Les caméras classiques sont aujourd'hui de bonne qualité mais ne font pas la différence entre un vrai visage et une photo sur papier ou sur smartphone. Il est du coup facile de se faire passer pour quelqu'un d'autre.
Pour résoudre ce problème, il faut utiliser des caméras Infra rouge. Elles permettent une meilleure qualité même avec un faible éclairage et ne captent pas les visages issus de photos.

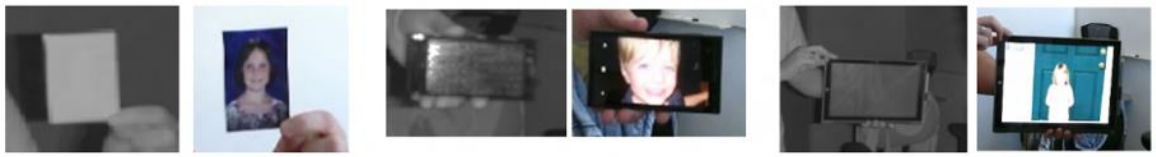

Figure 14 : Une caméra infrarouge ne capte pas des photos de visages

« Apple FaceID » et « Windows Hello » utilisent des caméras Infrarouge.

8. BIAIS

Il est probable qu'un algorithme ne détecte pas de visage, se trompe sur le genre, l'émotion ou d'autres analyses faussées par des biais « cognitifs ».

Les biais que l'on peut retrouver dans la détection de visage et dans l'identification viennent :

- des photos d'entrainement :
    - pas assez de photos ;
    - pas correctement « taguées » avec les bonnes réponses : l'encadrement du visage pas au bon endroit, une erreur de genre est possible humainement aussi ;
    - pour l'identification, une photo trop ancienne biaise les algorithmes.
- de la qualité de la photo envoyer pour détection
- d'une mauvaise caméra.

9. CAS D'USAGES

Les cas d'usages sont multiples mais ne sont pas tous éthiques. Voici une liste de quelques cas d'usages :

- permettre à un non-voyant via une prise de photo et un retour auditif de récupérer un certain nombre d'informations sur les personnes en face de lui (genre, âge, émotions). Exemple : Seeing AI : https://www.microsoft.com/en-us/ai/seeing-ai
- retrouver des enfants disparus : https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms
- un algorithme de simulation de vieillissement permettrait de reconnaitre des enfants disparus aujourd'hui adulte. Exemple : FaceApp : https://www.faceapp.com/
- reconnaitre une maladie génétique rare : https://www.genome.gov/news/news-release/Facial-recognition-software-helps-diagnose-rare-genetic-disease
- identifier des patients perdus dans un hôpital
- détecter des intrus
- surveiller les émotions d'individus
- déterminer l'orientation sexuelle à partir des traits du visages : étude https://psyarxiv.com/hv28a/
- déterminer si une personne va commettre un crime en fonction des traits de son visage
- détecter les émotions pendant un film, un jeu vidéo, un spectacle.

Et nous pouvons imaginer bien d'autres scénarii.

ASPECTS JURIDIQUES

Par Sandra AZRIA, avocate

Introduction

Rien n'est plus personnel que son propre corps. Au XVIII[e] siècle, le philosophe utilitariste Jeremy Bentham imagine une architecture carcérale, le panoptique, dans lequel les geôliers, installés dans une tour centrale, sont en mesure de surveiller tous les faits et gestes des prisonniers sans être visibles eux-mêmes. Les détenus, qui ne peuvent savoir s'ils sont observés ou non, se trouvent contraints à une permanente docilité. Pour Bentham, on peut étendre le principe aux usines, aux écoles ou aux hôpitaux. Michel Foucault, deux cents ans plus tard, considère dans *Surveiller et punir* que *«* cette visibilité organisée entièrement autour d'un regard dominateur et surveillant *»* est au cœur de ce qu'il nomme le modèle disciplinaire moderne.

I – ÉTAT DES LIEUX

La technologie - imparfaite mais qui s'améliore rapidement - est basée sur des algorithmes qui apprennent à reconnaître les visages humains et les centaines de façons dont chacun d'entre eux est unique.

Pour bien faire cela, les algorithmes doivent être alimentés de centaines de milliers d'images de visages divers. De plus en plus, ces photos proviennent d'Internet, où elles sont balayées par des millions de machines à l'insu de ceux qui les ont publiées, classées par âge, sexe, couleur de peau et des dizaines d'autres paramètres, et partagées avec les chercheurs des universités et des entreprises.

Pour beaucoup d'entre nous, la reconnaissance faciale est passée rapidement du statut de nouveauté technologique à celui de réalité incontournable de notre quotidien, des millions de personnes étant prêtes à accepter au minimum que leur visage soit scanné par un logiciel d'aéroport, pour effectuer un achat[9] ou par les serveurs de Facebook.

En Russie, la Banque Centrale déploie depuis 2017 un programme biométrique visant à recueillir visages, voix, scan d'iris et empreintes digitales dans tout le pays[10]. En Inde, la reconnaissance faciale est désormais utilisée comme moyen d'authentification de l'AADHAAR (système d'identification de la population ayant déjà permis d'identifier plus de 960 millions de personnes).[11]

Une étude réalisée en 2016 par l'Université de Georgetown a révélé qu'un adulte américain sur deux, soit 117 millions de personnes, se trouve dans les bases de données de reconnaissance faciale et que peu de règles régissent l'accès à ces systèmes[12].

En tout état de cause, il ne fait aucun doute que la technologie de reconnaissance faciale peut être un outil puissant.

1) Un usage de plus en plus répandu

Les usages les plus courants à date concernent :

> **Sécurité** : la délivrance de documents d'identité, le contrôle aux frontières, le contrôle policier ou encore les enquêtes relatives à des infractions pénales (la reconnaissance faciale aurait ainsi permis d'identifier le suspect dans la mort de cinq employés de la *Gazette de la capitale* à Annapolis le 28 juin 2018[13]).

[9] https://www.reuters.com/article/us-alibaba-payments-facialrecognition/just-smile-in-kfc-china-store-diners-have-new-way-to-pay-idUSKCN1BC4EL
[10] https://financialobserver.eu/cse-and-cis/russian-banks-to-use-biometric-data/
[11] https://timesofindia.indiatimes.com/india/face-recognition-to-be-must-for-all-aadhaar-authentications/articleshow/65522828.cms
[12] https://www.law.georgetown.edu/news/half-of-all-american-adults-are-in-a-police-face-recognition-database-new-report-finds/
[13] https://www.theatlantic.com/technology/archive/2018/06/capital-gazette-shooting-face-recognition/564185/

Selon une étude de 2018[14], 77 % des aéroports et 71 % des compagnies aériennes ont prévu d'investir dans les technologies d'identification biométrique dans les trois ans. Et 59 % des aéroports et 63 % des compagnies prévoient notamment de recourir à des portes d'embarquement à reconnaissance faciale.

Le pionnier mondial de ces nouvelles technologies est une entreprise européenne, basée à Genève : la Société internationale de télécommunication aéronautique, plus connue sous le sigle SITAL. A Roissy-CDG et à Lyon-Saint-Exupéry, la reconnaissance faciale a permis de réduire considérablement l'attente aux frontières[15], les nouveaux sas ayant la possibilité d'associer un visage à la photo figurant sur le passeport, ce qui a permis d'élargir le pourcentage de voyageurs éligibles à ce type de contrôle, même si le système reste très imparfait. « Les obstacles ne sont pas technologiques, mais administratifs », souligne la directrice de SITA. « Il faut que les gouvernements européens se mettent d'accord sur des normes communes et que les réglementations convergent ». Certains pays, comme l'Australie, ambitionnent d'automatiser 90% des contrôles passagers via la reconnaissance faciale d'ici à 2020.

Enfin, un système de reconnaissance faciale peut aider à réunir les enfants perdus ou enlevés avec leur famille et à enrayer la traite des personnes[16].

- **Santé** : le suivi de la consommation des médicaments de patients[17], la détection de maladies génétiques[18] (comme par exemple, le Syndrome de DiGeorge avec taux de réussite de 96,6%[19]) ou encore l'accompagnement de la prise en charge de la douleur[20].

- **Commerce** : les usages se développent notamment afin d'analyser le parcours client[21] au sein de boutiques mais aussi afin d'effectuer des paiements[22].

  En Australie, Coca-Cola teste la technologie depuis le début de l'année sur une cinquantaine de distributeurs de boissons capables de relayer des messages publicitaires, collecter des données commerciales et analyser les interactions de l'utilisateur via un écran digital et une caméra. Selon Coca- Cola, ces distributeurs auraient permis d'augmenter les ventes de 12% sur la période d'essai[23].

  Au Royaume- Uni, la chaîne Tesco a équipé 450 stations-services d'écrans publicitaires délivrant des messages publicitaires en temps réel selon l'âge et le sexe détectés par la caméra[24].

  Dès 2014, Ford et Intel annonçaient le projet **Mobii** (PDF), qui intègre un système de reconnaissance du conducteur, pour personnaliser l'expérience de conduite (déverrouillage, chargement de réglages personnalisés, intégration de l'agenda au GPS, alertes en cas d'endormissement).[25]

  Chaque jour, l'actualité révèle de nouvelles utilisations mais aussi de nombreux scandales qui font s'interroger sur la possibilité de protéger efficacement les Droits de l'Homme en présence d'un outil de reconnaissance faciale.

[14] https://www.sita.aero/resources/type/surveys-reports/air-transport-it-insights-2018
[15] https://www.tourmag.com/Aeroports-vers-la-fin-des-cartes-d-embarquement_a97696.html
[16] https://www.telegraph.co.uk/peoples-daily-online/science/china-facial-recognition-missing-persons/
[17] https://journal.ahima.org/2018/09/04/facial-recognition-enters-into-healthcare/
[18] https://ai-med.io/facial-recognition-and-medicine/
[19] https://www.genome.gov/news/news-release/Facial-recognition-software-helps-diagnose-rare-genetic-disease
[20] https://www.sciencedirect.com/science/article/pii/S1877050916300874
[21] https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto
[22] http://www.globaltimes.cn/content/1159070.shtml
[23] https://www.businessinsider.com.au/coca-cola-is-using-facial-recognition-technology-on-fridges-in-australia-to-sell-more-drinks-2014-5
[24] https://www.retaildetail.eu/en/news/algemeen/tesco-installing-facial-recognition-camera%E2%80%99s-advertisers
[25] https://thenewswheel.com/project-mobii-facial-recognition/

II - RISQUES POSÉS

1) Sur la vie privée

Le dernier scandale en date illustre parfaitement l'impact majeur potentiel sur la vie privée des personnes concernées. Ainsi, en août 2019, l'autorité de contrôle britannique (ICO) a ouvert une enquête afin d'analyser la mise en place d'une surveillance par reconnaissance faciale dans le quartier de King's Cross à Londres.[26] La déclaration émanant de Madame Elizabeth Denham, *Information Commissioner*, souligne « le scan des visages des gens au cours de leur vie quotidienne, afin de les identifier, est une menace potentielle à la vie privée qui devrait tous nous préoccuper. C'est particulièrement le cas si cela se fait à l'insu et sans la compréhension des gens ».

En effet, un des premiers problèmes posés par la reconnaissance faciale est que les personnes concernées ne savent pas forcément qu'elles en sont l'objet. De plus, la question du volume et de la rapidité du traitement des visages rend difficile l'application du consentement comme base légale (quand elle est applicable) à ce traitement de données personnelles et ce alors même que s'agissant de données sensibles, celui-ci devrait être explicite.

De plus, les accès à des réseaux sociaux (autorisés ou non, publics ou non) donnent accès à des milliards de photos susceptibles d'être utilisés sans consentement des personnes concernées.

Enfin, l'interopérabilité technologique pourrait avoir à long terme comme conséquence pratique l'assimilation de l'utilisation de certaines données biométriques à un identifiant unique d'application générale. Un facteur aggravant pourrait venir du fait que, contrairement au numéro d'identification qui peut être changé au cours d'une vie, un tel changement n'est évidemment pas envisageable pour les données biométriques et encore moins pour un visage.

Il faut faire preuve également d'une inquiétude particulière à l'égard de la reconnaissance d'émotions, une sous-classe de la reconnaissance faciale, qui prétend pouvoir détecter des informations telles que la personnalité, les sentiments intérieurs, la santé mentale et le niveau d'engagement d'un salarié en se fondant sur des images ou des vidéos de visages.

La perspective que la police utilise la « reconnaissance d'émotions » pour déduire ce que sera votre future activité criminelle à partir de « micro-expressions » de votre visage, est infiniment pire et nous plonge dans un futur à l'image de Minority Report.

En 2016, des étudiants de l'Université de Shanghai ont publié un compte-rendu détaillé de ce qu'ils affirmaient être une méthode de *Learning Machine* pour déterminer le potentiel délinquant des personnes en se fondant sur les seules caractéristiques du visage.[27] Leur publication a été largement critiquée comme étant une résurgence des idées physiognomoniques dans les applications de reconnaissance d'émotions.

L'idée que les systèmes d'intelligence artificielle puissent nous dire ce qu'un étudiant, un client ou un suspect ressent vraiment, ou bien le type de personne qu'ils sont intrinsèquement, se révèle être très attrayante pour les grandes entreprises autant que pour les États, bien que les justifications scientifiques de telles affirmations restent extrêmement douteuses et que l'on dispose d'une histoire bien documentée de leur usage à des fins discriminatoires.

Entre Faception, qui prétend pouvoir "détecter" si une personne est terroriste à partir de son visage[28], et HireVue, qui pratique l'enregistrement vidéo en masse de candidats en entretien d'embauche pour prédire à partir des micro-expressions de leur visage s'ils seront de bons employés ou pas[29], la faculté d'utiliser l'analyse de données de masse pour faire des corrélations conduit à faire des assertions très suspectes.

---

[26] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/

[27] « Automated Inference on Criminality using Face Images », Université Shanghai Jiao Tong, 21 novembre 2016.

[28] https://www.faception.com/

[29] https://www.hirevue.com/blog/7-things-you-need-to-know-about-game-based-cognitive-assessments

Dans la même logique, les autorités chinoises de la province de Jilin veulent faire la traque à l'alcool au volant. Comme les forces de l'ordre l'ont annoncé, cette province du nord-est de la Chine va expérimenter une technologie pour reconnaître si un conducteur est alcoolisé ou non.

Ils se sont appuyés sur plusieurs traits faciaux afin de déterminer si un automobiliste a consommé de l'alcool. L'intelligence artificielle étudiera si des rougeurs apparaissant sur le visage du conducteur, si sa respiration est haletante, s'il baille ou a quelques hoquets[30]. À la suite d'une identification suspecte, les informations seront envoyées aux agents en patrouille et intercepteront le conducteur afin d'effectuer des tests approfondis.

Enfin, au-delà de ces nombreux risques, à terme, c'est notre anonymat qui risque de disparaître en mettant à disposition du grand public de tels outils. Reconnaître n'importe quelle personne que l'on croise dans la rue sera bientôt une réalité avec des applications du type « NameTag » ou « Facezam ». Même si celles-ci se sont révélés être des supercheries, l'accélération du développement technologique les rendra sans doute rapidement d'actualité. L'idée était qu'en les utilisant sur un smartphone ou des [lunettes connectées] Google Glass, il suffisait de prendre une photo de quelqu'un pour découvrir leurs profils virtuels sur les réseaux sociaux et donc leur identité, adresse, membres de leur famille, profession, goûts, etc. [31]

En revanche, être reconnu à l'entrée d'un commerce par un système de reconnaissance faciale qui utilise vos photos Facebook, est désormais possible. Le concept semble effrayant, même s'il a été imaginé pour récompenser la fidélité des clients. L'idée a germé au sein d'une jeune agence de publicité, basée à Nashville aux États-Unis. L'agence Redpepper est en train de tester une caméra faisant le lien entre vos photos sur Facebook et un système de reconnaissance faciale, le but étant d'offrir des réductions aux clients de petits commerces[32].

Pour sa première utilisation, la caméra baptisée Facedeals a été installée à l'entrée d'un bar. Lorsqu'un client approche, cette caméra connectée en wifi analyse sa cible pour retrouver son compte Facebook. Lorsque le client a été identifié, Facedeals calcule, en fonction de ses « j'aime» et de son comportement sur le réseau social, des offres et des réductions spéciales. Le client reçoit enfin son coupon de réduction sur son téléphone portable.

Même en étant particulièrement vigilant sur notre propre utilisation de nos photos sur les réseaux sociaux, cette technologie est tellement puissante que notre anonymat restera menacé. Une anecdote qui pourrait sembler charmante est ainsi arrivée à Monsieur Fred B. En 2014, il reçut un courriel de Facebook l'informant qu'il avait détecté son visage sur un certain nombre de photos et lui demandant s'il aimerait y être tagué. Lorsqu'il a cliqué sur le lien, il s'est amusé à trouver onze photos en noir et blanc correspondant au visage de sa mère à l'université. Il avait été identifié par erreur via l'algorithme DeepFace du réseau social.

Selon Monsieur David Tunnell, directeur de la technologie chez NXT-ID, spécialisé dans la reconnaissance faciale tridimensionnelle, « on peut utiliser la reconnaissance faciale pour identifier l'origine ethnique, la région d'origine et l'appartenance familiale d'une personne. Avec de bonnes données provenant de mes parents, de mes frères et sœurs ou de mes cousins, il dit qu'il serait peut-être possible de m'identifier même si le système n'avait pas d'images réelles de moi pour travailler »[33].

2) Risques liés à la fiabilité

Malgré le développement inouï de cette technologie, de nombreuses interrogations persistent sur sa fiabilité et les nombreux risques provoqués par une erreur potentielle.

L'utilisation d'un système basé sur des données biométriques repose inévitablement sur des probabilités d'ordre statistique. Il n'existe pas de système infaillible. S'il existe un degré suffisant de probabilité, la personne concernée sera « reconnue » par le système.

[30] http://www.xinhuanet.com/english/2019-03/07/c_137875388.htm
[31] https://www.entrepreneur.com/article/290742 « people can't stalk your profile through face recognition apps - Yet »
[32] https://www.adweek.com/digital/redpepper-facedeals/
[33] https://www.theverge.com/2014/9/10/6126027/facebook-is-convinced-this-man-is-his-mother-deep-face

Les systèmes biométriques sont donc intrinsèquement faillibles. Le risque d'une fausse reconnaissance ou d'une fausse non reconnaissance peut avoir de fâcheuses conséquences pour la personne concernée.

Par exemple, si elle est « reconnue » à tort comme apparaissant sur une liste de criminels ou délinquants recherchés, la conséquence pratique pourrait être qu'elle aura à démontrer son innocence. Le taux de fausse reconnaissance et de faux rejets dépend de plusieurs propriétés du système, comme sa qualité et sa fiabilité, le processus d'enrôlement etc. Les taux peuvent être ajustés de manière à obtenir le niveau de sécurité requis pour la finalité du système. Les efforts visant à prévenir des résultats erronés devraient être proportionnels à la finalité du système.

L'ACLU, l'Union américaine pour les libertés civiles, a ainsi demandé qu'Amazon cesse de commercialiser son système Rekognition. Un test avait en effet montré les défaillances de celui-ci : la technologie avait identifié par erreur 28 membres du Congrès américains comme des criminels purgeant actuellement une peine de prison et en proportion beaucoup plus de personnes noires ou de couleur[34].

Au Royaume-Uni, une étude indépendante réalisée par l'Université d'Essex concluait que quand la police de Londres a commencé à tester son système de reconnaissance faciale, dans 98 % des cas lorsque le système d'intelligence artificielle lançait des alertes d'identification de suspects, il s'agissait de faux positifs. De quoi susciter des craintes au sein de la population. Aujourd'hui, ce taux d'erreur serait encore de 81% ce qui semble ahurissant au vu des conséquences néfastes possibles pour les personnes concernées.[35]

3) Sur la sécurité des données

Les conséquences d'une violation des données de reconnaissance faciale sont toutefois potentiellement plus graves et plus durables que celles portant sur d'autres données personnelles, car il est beaucoup plus difficile pour une personne de changer son visage que son numéro de carte de crédit.

Ainsi, l'actualité regorge d'exemples de défaillances techniques majeures en matière de sécurité.

Ainsi, la fonction de reconnaissance faciale du Galaxy S10 reste manifestement aussi faible que sur les précédentes générations. En effet, il semblerait qu'il soit possible de le débloquer en utilisant une simple photographie ou une vidéo de son propriétaire.[36]

Lewis Hilsenteger, alias Unbox Therapy sur YouTube, en a fait la démonstration. En diffusant une vidéo devant le capteur du smartphone, il a ainsi pu en débloquer l'accès, abusant le système de reconnaissance faciale.

Un journaliste italien de SmartWorld.it avait quant à lui déverrouillé un Galaxy S10 en n'utilisant rien d'autre qu'une photo - a priori nettement plus simple à obtenir pour un hacker. Sur ce sujet, Samsung et ses Galaxy S ne sont toutefois pas des cas isolés.

Une étude réalisée l'an dernier par une association néerlandaise avait révélé que les fonctions de déverrouillage par reconnaissance faciale de 42 des 110 smartphones testés pouvaient être détournées grâce à une simple photo.[37]

4) Sur la liberté d'expression et la liberté de religion

Les critiques les plus virulentes de la reconnaissance faciale sont bien évidemment liées à ces atteintes les plus graves, et notamment celles liées à la liberté d'expression ou la liberté de religion.

Ainsi, les militants des libertés civiles craignent de plus en plus que les forces de l'ordre ne déploient la reconnaissance faciale en "temps réel" au moyen de drones, de caméras corporelles et de caméras sur le tableau de bord de leurs véhicules.

[34] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-
[35] https://www.technologyreview.com/f/613922/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time/
[36] https://www.zdnet.com/article/samsung-galaxy-s10-facial-recognition-fooled-by-a-video-of-the-phone-owner/
[37] https://www.zdnet.com/article/facial-recognition-doesnt-work-as-intended-on-42-of-110-tested-smartphones/

”La véritable préoccupation, c'est que la police en patrouille identifie à volonté les Américains respectueux des lois à l'aide de caméras corporelles”, a déclaré Matthew Feeney, spécialiste des technologies émergentes à l'Institut Cato.[38]

Une situation encore bien plus inquiétante est celle de la province de Xinjiang (qui abrite une importante communauté musulmane d’origine ouïgour) en Chine.

Chaque citoyen de plus de 12 ans doit faire scanner son visage en 3D pour faciliter le travail de ces caméras. Cette surveillance de masse - officiellement destinée à prévenir les actes terroristes - permet de repérer tous les comportements définis par les autorités comme « extrémistes » : s'éloigner de plus de 300 mètres de son domicile, se rendre trop souvent à la mosquée ou même faire le plein plusieurs fois par semaine.[39] « Ceux qui se font prendre risquent de se faire envoyer dans un camp de rééducation », dit Maya Wang. Un million d'Ouïgours y seraient déjà internés.[40]

5) Sur la liberté de mouvement

De nombreux experts soulignent également les effets paralysants potentiels sur les libertés d'expression, d'action et d'association et d'autres droits civils causés par la perte de l'anonymat dans le suivi public et perpétuel par les systèmes de reconnaissance faciale.

Les préoccupations sont particulièrement vives dans le domaine de la surveillance gouvernementale. Les outils de reconnaissance faciale mis au point pour les déploiements militaires à l'étranger sont de plus en plus utilisés à des fins d'application de la loi aux États-Unis avec peu de lignes directrices et peu de surveillance publique.

Ainsi, un document publié par le Département de la sécurité intérieure américain et relayé par l’Union américaine pour les libertés civiles (ACLU) montre que la Maison Blanche a pour projet de s’équiper d’un système de reconnaissance faciale, permettant d’identifier et de suivre les déplacements d’individus potentiellement dangereux.

Encore en phase de test, le système en question présente des risques importants de dérives. Sans rien pouvoir y faire, les passants qui se promènent autour de la Maison Blanche, à Washington, pourraient bientôt voir leurs visages enregistrés et analysés par les services secrets américains[41].

Reste que les visages de plusieurs milliers de personnes - qu’elles soient activistes, touristes ou fonctionnaires - seraient ainsi, dans cette zone de Washington, scrutés sans leur consentement.

Un problème que le document évacue en une phrase assez lunaire « Les personnes qui ne souhaitent pas être filmées par les caméras impliquées dans ce projet pilote peuvent choisir d’éviter la zone » qui démontre bien la restriction sur le principe de liberté de mouvement.

En cas de succès, le système pourrait donc offrir la possibilité aux agents chargés de la sécurité du bâtiment de suivre les déplacements de ceux que le document nomme des « sujets d’intérêt ».

Sur quels critères l’étiquette « sujet d’intérêt » sera-t-elle attribuée aux différents passants ? Pour l’Union américaine pour les libertés civiles (ACLU), c’est précisément là que le bât blesse. « Nous ne savons pas exactement comment les services secrets déterminent si une personne est un “sujet d'intérêt” ou pas », s’inquiète-t-elle par la voix de l’un de ses membres, Jay Stanley, dans un article sur son site. « L’agence affirme que les personnes pourraient être identifiées de différentes manières, notamment par “des publications sur les réseaux sociaux postées sur des forums publics” ainsi que des rapports d’activités suspectes et des reportages dans les médias. Malheureusement, les agences gouvernementales qualifient depuis longtemps de “menaces” les personnes en fonction de leur race, de leur religion ou de leurs convictions politiques. L'année dernière, par exemple, un document a révélé que le FBI avait

[38] https://fee.org/articles/should-police-be-able-to-use-facial-recognition-technology/
[39] https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report
[40] https://www.lemonde.fr/asie-pacifique/article/2018/08/31/la-chine-detiendrait-un-million-d-ouigours-dans-des-camps-d-internement_5348573_3216.html
[41] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/secret-service-announces-test-face-recognition

préparé une évaluation du renseignement établissant à tort, et à partir de leur race et de leurs convictions, que les militants noirs constituaient des menaces, les qualifiant d'extrémistes de l'"identité noire". »

Dans un registre plus léger mais également significatif, Mike Downing, chef de la sécurité du groupe Oak View ayant eu l'occasion de tester le système pour un concert de Taylor Swift, a expliqué son fonctionnement à *Rolling Stone* : « Toute personne qui entrait se mettait à fixer l'écran, ce qui enclenchait le logiciel de reconnaissance faciale ».

Les visages ainsi capturés étaient envoyés dans la foulée à un poste de contrôle situé à Nashville, dans l'État du Tennessee. Ce dernier s'attelait à vérifier la correspondance des profils présents au concert avec la base de données répertoriant la centaine de harceleurs de la chanteuse, déjà identifiés. Cette exploitation de la reconnaissance faciale soulève inévitablement des questions concernant le respect de la vie.[42].

Pour le moment justifié à des fins de protection lors des représentations, ce système pourrait à l'avenir être motivé par des considérations autres que sécuritaires. Le groupe TicketMaster a en effet partagé son ambition de remplacer à terme les classiques tickets et e-billets pour un scanner facial, afin de fluidifier l'entrée aux événements. Pour ce faire, le groupe a déjà investi dans la startup Blink Identity, dont les capteurs peuvent identifier une personne marchant vite à côté en une demi-seconde[43].

6) Risques liés à une discrimination

Plusieurs études ont démontré les risques forts de discrimination liée à la couleur de peau ou le sexe en matière de reconnaissance faciale.

Ainsi, l'étude parue en juillet 2019 du *National Institute of Standards and Technology* (NIST) de *l'US Department of Commerce*[44] a révélé que les algorithmes de reconnaissance faciale faisaient erreur dix fois plus souvent concernant des personnes noires et plus particulièrement s'agissant de femmes.

La dernière source d'inquiétude est une étude publiée par le Media Lab du MIT[45], qui a révélé que Rekognition avait de moins bons résultats lorsqu'il s'agissait d'identifier le sexe d'une personne si elle était de sexe féminin ou à la peau plus foncée.

Dans les tests menés par Madame Joy Buolamwini du MIT, Rekognition n'a commis aucune erreur dans l'identification du sexe des hommes à la peau claire, mais elle a confondu les femmes avec les hommes 19 % du temps et les femmes à la peau plus foncée avec les hommes dans 31 % des cas.

Une autre étude également effectuée par Madame Buolamwini mais portant cette fois sur un outil développé par Microsoft, IBM et MEGVII faisaient des erreurs du même type.[46]

Microsoft a annoncé le mois dernier qu'il avait apporté des améliorations significatives pour la reconnaissance faciale à travers les tons de peau et les genres.

IBM, quant à elle, a déclaré qu'elle lançait une étude à grande échelle « pour améliorer la compréhension des biais dans l'analyse faciale »[47].

Enfin, on ne peut passer sous silence le fait que le service de photo-organisation de Google censure toujours les termes de recherche "gorille" et "singe" après un incident survenu en 2015, au cours duquel des algorithmes ont étiqueté des Noirs comme gorilles[48].

---

[42] https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/
[43] https://www.theverge.com/2018/5/7/17329196/ticketmaster-facial-recognition-tickets-investment-blink-identity
[44] « Ongoing Face recognition – vendor test » National Institute of Standards and Technology, 22 juillet 2019
[45] « Actionable Auditing:Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products », Association for the Advancement of Artificial Intelligence, 25 janvier 2019
[46] https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error
[47] https://www.cnbc.com/2019/01/29/ibm-releases-diverse-dataset-to-fight-facial-recognition-bias.html
[48] https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people

7) Sur l'accès et le contrôle des données

Sur ce sujet également, il est régulièrement avéré que les données personnelles liées à la reconnaissance faciale sont partagées et diffusées sans que les personnes concernées en soient même informées.

Or, même si les personnes peuvent identifier les entités commerciales qui ont recueilli des données les concernant à l'aide de systèmes de reconnaissance faciale, il pourrait être difficile ou impossible pour ces personnes de déterminer quelles données ont été recueillies à leur sujet, comment elles sont utilisées, avec qui elles ont été partagées et de demander l'accès pour corriger les erreurs ou supprimer les renseignements les concernant.

Ainsi, IBM a utilisé et partagé en janvier 2019 une galerie de près d'un million de photos prises sur le site d'hébergement de photos Flickr pour décrire l'apparence des sujets et entraîner son outil de reconnaissance faciale. IBM a largement communiqué sur cette démarche auprès des chercheurs comme une étape progressive vers la réduction des biais dans la reconnaissance faciale.[49]

Toutefois, il est rapidement apparu que ces photos avaient été partagées et diffusées sans l'autorisation ou même l'information des personnes concernées.

En réponse, IBM s'est contenté de donner l'assurance que les utilisateurs de Flickr pouvaient demander à se voir se retirer de la base de données. En pratique, il s'est avéré presque impossible de faire supprimer des photos.

En effet, IBM exigeait que les photographes envoient par courrier électronique des liens vers les photos qu'ils souhaitent supprimer, mais la société n'a pas partagé publiquement la liste des utilisateurs Flickr et des photos incluses dans l'ensemble de données. Il n'existe donc pas de moyen de déterminer à qui appartiennent les photos incluses et privent donc les personnes concernées de tout réel droit à ce sujet.

[49] https://www.theverge.com/2019/3/12/18262646/ibm-didnt-inform-people-when-it-used-their-flickr-photos-for-facial-recognition-training