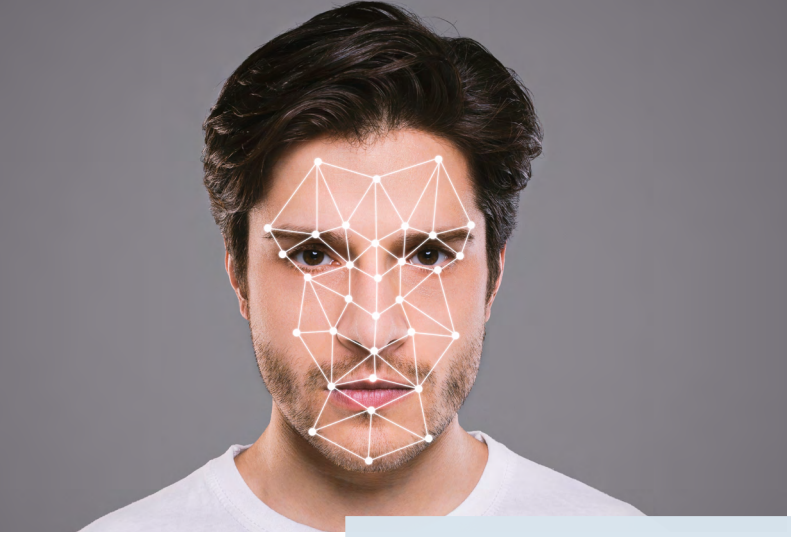
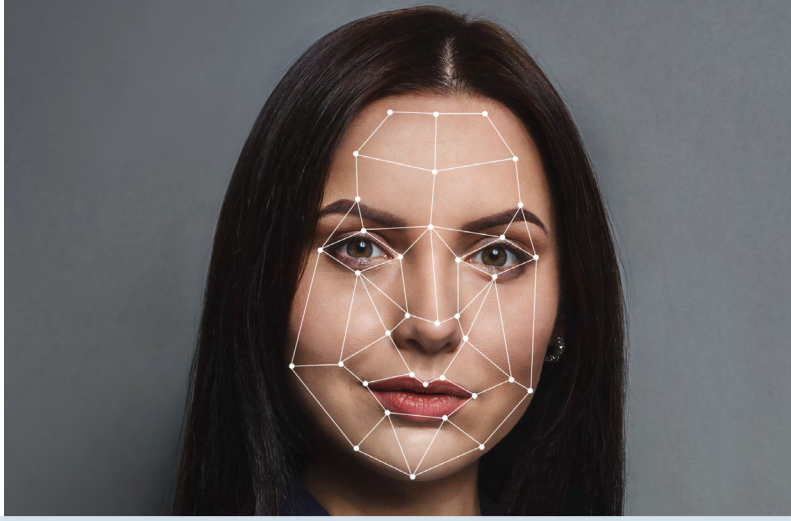
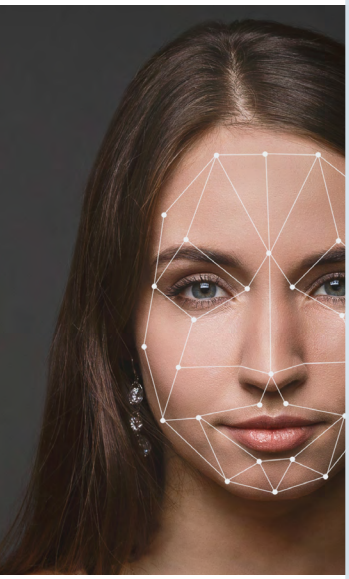
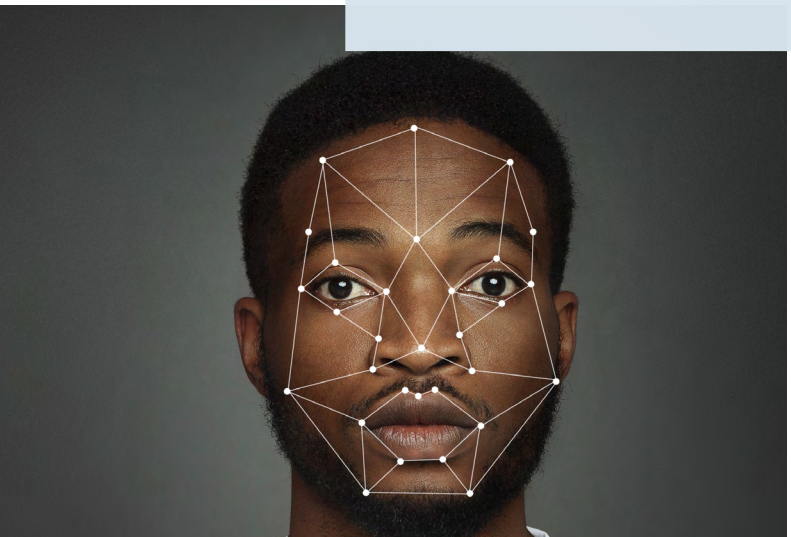
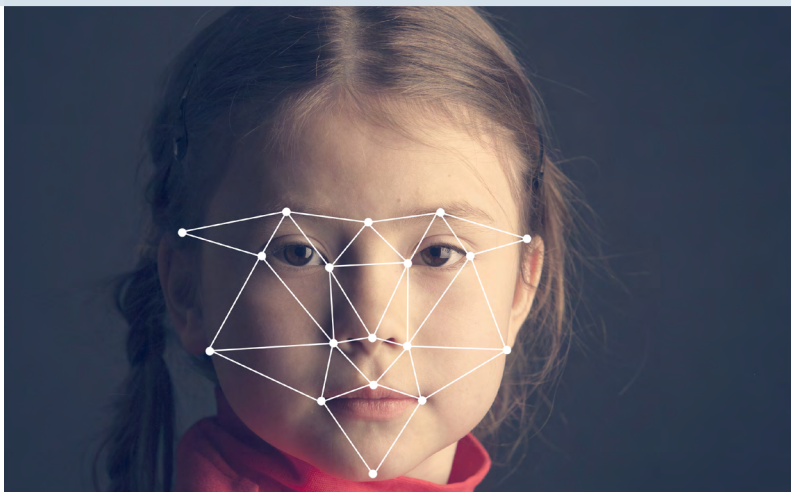





Mars 2021

Reconnaissance faciale et Droits de l'homme : Un guide pour l'investisseur

CANDRIAM
A NEW YORK LIFE INVESTMENTS COMPANY

A propos des auteurs

Benjamin Chekroun

Stewardship Analyst: Proxy Voting and Engagement

Benjamin Chekroun a rejoint Candriam en 2018 en qualité de Responsable Adjoint de la Gestion Obligations Convertibles, avant de prendre ses fonctions actuelles en 2020. Il avait auparavant travaillé au sein d'ABN AMRO Investment Solutions depuis mars 2014, où il était responsable de la stratégie obligations convertibles. Durant sa carrière, il a passé quatre années à Hong Kong, une à New York et treize à Londres en tant que trader sur les obligations convertibles. Benjamin est titulaire d'un Masters en commerce international.

Sophie Deleuze

Lead ESG Analyst, Stewardship

Sophie Deleuze a rejoint l'équipe de Recherche ESG de Candriam en 2005. Après plus de 10 années d'expérience en analyse ESG, elle s'est spécialisée dans la démarche d'engagement, de vote et de Stewardship et coordonne notre engagement avec les équipes d'analyse ESG et l'ensemble des équipes de gestion de portefeuille. Avant d'intégrer Candriam, Sophie a été analyste ESG pendant 4 ans, chez BMJ CoreRatings puis chez Arese. Sophie Deleuze est titulaire d'un diplôme d'ingénieur en Traitement de l'Eau et d'un Masters en Politique Environnementale Publique.

Quentin Stevenart

ESG Analyst

Quentin a rejoint l'équipe ESG de Candriam en 2016. Il est chargé de l'analyse ESG du secteur de la technologie de l'information et des aspects liés à la gouvernance dans différents secteurs. Par ailleurs, il coordonne la recherche de Candriam dans le domaine de l'Economie Circulaire. Quentin est titulaire d'un Masters en Management de Louvain School of Management et d'un Masters et Bachelors en Ingénierie Commerciale de l'Université Catholique de Leuven.

Sommaire

« S'il est indéniable que cette technologie est prometteuse et pourrait se révéler être une force au service du bien, la manière dont la reconnaissance faciale est conçue et utilisée aujourd'hui comporte des risques et créé des incidences sociales pour les individus qui appellent à une intervention des investisseurs sur cette problématique. Par conséquent, nous saluons les efforts, la réflexion et le leadership des investisseurs, qui en amont de la réglementation, cherchent à élargir le périmètre ESG traditionnel et à comprendre comment, où et quand la reconnaissance facile peut être employée de manière appropriée, et par qui ».

- Katherine Ng, Responsable de la Recherche Universitaire,
Principes pour l'Investissement Responsable des Nations Unies

En bref

La gestion responsable ne se limite pas à réagir aux risques et aux enjeux qui nous préoccupent aujourd'hui. Elle implique de réfléchir au-delà des bilans carbones et du changement climatique et de s'interroger sur les risques et les opportunités de demain.

La technologie nous offre des avantages exceptionnels – et des investissements qui le sont tout autant. La technologie a permis à de nombreux professionnels de continuer à travailler de chez eux durant la pandémie. Le Président Joe Biden a mené une grande partie de sa campagne électorale de son sous-sol. Et pourtant, nous devons être conscients que toutes les nouvelles technologies peuvent engendrer des conséquences involontaires.

La Technologie de Reconnaissance Faciale (TRF) permet d'optimiser l'efficacité et la sécurité. Elle nous sert à déverrouiller des smartphones haut de gamme et de transiter dans les aéroports. Elle a également des incidences en matière de droits humains. La technologie est en cours de développement depuis plusieurs décennies, mais ce n'est qu'aujourd'hui qu'elle est déployée à une échelle aussi large.

Un sondage réalisé par Candriam en 2021 a permis de récolter les réponses d'environ 300 investisseurs. Sur cet échantillon, 30% estiment que la Technologie de Reconnaissance Faciale est un outil pratique et utile. Près de 70% a émis des réserves : 31% a estimé que la TRF n'est pas fiable et pour 38% des participants, les considérations éthiques doivent rattraper le retard pris par rapport à la technologie.

Parmi ces dernières figurent l'absence de consentement et le manque de réglementation. Les incidents liés à des erreurs d'identification, dont certaines ont entraîné de fausses arrestations, sont de plus en plus fréquents, surtout pour les citoyens qui ne sont pas de race blanche. En mai 2019, la ville américaine de San Francisco – berceau de la Reconnaissance Faciale – a interdit son utilisation par les forces de l'ordre. Peu de temps après, certains géants de la tech ont annoncé un moratoire d'un an sur la vente de produits de Reconnaissance Faciale.

Afin de comprendre les problématiques de droits de l'homme qui se profilent, il est donc important que les investisseurs et les autres parties prenantes s'engagent dès aujourd'hui.

Cette étude n'aurait pas été possible sans l'aide précieuse des organisations et des personnes suivantes. Nous les remercions pour le temps qu'elles nous ont accordé, la qualité de leurs explications et leur patience :
- *Clare Garvie, The Center on Privacy & Technology at Georgetown Law*
- *Nabylah Abo Dehman, the United Nations Principles for Responsible Investments*
- *Anita Dorett, The Investor Alliance for Human Rights*
- *Isedua Oribhador, AccessNow*
- *Michael Conner, Open MIC*

La Technologie

Comment fonctionne-t-elle ?

La Reconnaissance Faciale fait partie de la famille de la reconnaissance biométrique. Il s'agit d'un processus visant à **identifier** ou à vérifier **l'identité** d'une personne grâce à une photographie ou une vidéo de son visage. Elle capte, analyse et compare les schémas visuels sur la base des caractéristiques faciales de la personne. Certains systèmes utilisent désormais des images tri-dimensionnelles pour encore plus de précision.

La technologie de Reconnaissance Faciale comporte trois étapes :

- **La détection du visage** est un processus essentiel qui détecte et localise les visages humains dans les images et les vidéos.

- **La capture du visage** transforme une information analogue – un visage – en une série d'informations numériques, soit des données, qui représentent les traits faciaux de la personne. Des dizaines de caractéristiques faciales sont ainsi mesurées : écartement des yeux, des arêtes du nez, des commissures des lèvres, des oreilles, du menton etc.

- **L'authentification** vérifie que deux visages correspondent bien à la même personne.

L'algorithme livre un résultat associé à une probabilité donnée sous un format statistique : « *Authentification positive – Monsieur X – probabilité de 97,36%* ».

Une brève histoire de la Reconnaissance Faciale

Les origines de la Reconnaissance Faciale remontent aux années soixante. Woody Bledsoe, un évêque mormon et co-fondateur de la Panoramic Research à Palo Alto, avait développé une méthode permettant de saisir manuellement les traits du visage d'une personne dans un ordinateur. Si cette technique est peu efficace selon les normes actuelles, elle a néanmoins démontré que le visage constitue une série de données biométriques valide. La précision des systèmes de reconnaissance s'est améliorée au cours des années 70, car les chercheurs y ont intégré des marqueurs supplémentaires. Les vrais progrès ont eu lieu dans les années 80 et 90 avec l'arrivée de nouvelles méthodes permettant de localiser un visage dans une image et d'en extraire les caractéristiques, rendant possible la Reconnaissance Faciale entièrement automatisée. En 1996, le Programme FERET aux États-Unis a marqué la première construction d'une base de données faciales. En 2001, le Super Bowl a été l'occasion pour les forces de l'ordre de tester en masse la Reconnaissance Faciale – 19 criminels recherchés par la police ont été identifiés dans la foule. Les plus grandes avancées ont eu lieu en 2010, et après, lorsque les réseaux de neurones artificiels ont enrichi la technologie. En 2011, la technologie de Reconnaissance Faciale a aidé à confirmer l'identité d'Oussama ben Laden lorsqu'il a été tué dans un raid aérien américain. Facebook a déployé les identifications (tagging) dans les photos et en 2014, son programme DeepFace a été le premier à obtenir des performances quasi-humaines dans la reconnaissance des visages. En 2017, l'iPhone X a été le premier smartphone accessible au grand public à proposer le déverrouillage par reconnaissance faciale, la première diffusion de masse de cette technologie. En mai 2019, San Francisco est devenue la première grande ville américaine à interdire le recours à la Reconnaissance Faciale par les services des forces de l'ordre. L'été suivant, le patron d'IBM s'est engagé à ne plus proposer IBM FR ou ses logiciels d'analyse afin de respecter les « Principes de Confiance et de Transparence » de l'entreprise ; IMB a été suivie par les géants de la technologie, dont Amazon, Facebook et Microsoft, qui ont décidé d'un moratoire d'un an sur la vente de leurs produits.

La réalisation de ces étapes nécessite, en amont, la mise à disposition et l'utilisation de certaines données et technologies.

- Un système de Reconnaissance Faciale apprend à reconnaître les schémas visuels du visage en utilisant une **base de données « d'entraînement »** contenant un grand nombre d'images. Cette base de données doit être large, complexe et hétérogène pour obtenir des résultats plus précis.

- La technologie de Reconnaissance Faciale associe le recours à l'**Intelligence Artificielle** (le système est capable d'apprendre en analysant les données), la **Machine Learning** (le système peut élargir sa capacité à traiter et utiliser l'information sans intervention humaine en apprenant de ses expériences passées) et le **Deep Learning** (une nouvelle technique capable de réaliser de la Machine Learning et qui s'inspire du fonctionnement des réseaux de neurones dans le cerveau humain).

Applications

En règle générale, la technologie de Reconnaissance Visuelle réalise une ou plusieurs tâches combinées :

Identification

« Qui êtes-vous ? »

Authentification

« Etes-vous bien celui que vous prétendez être ? »

Catégorisation

« A quel(le) groupe /catégorie appartenez-vous ? »

Si les systèmes de Reconnaissance Faciale sont principalement utilisés pour la sécurité et le maintien de l'ordre, ils sont également employés dans le domaine de la médecine et du marketing. La liste des applications s'allonge rapidement.

- **Maintien de l'ordre** – permet de localiser les personnes suspectées d'activités criminelles ou terroristes, de trouver une personne disparue, de contrôler les accès ou les foules.
- **Sécurité** – pour déverrouiller une porte/téléphone/système, valider une transaction, contrôler les passagers dans un aéroport.
- **Ecoles** – pour la protection, le suivi de l'assiduité, de l'attention.
- **Médecine** – pour poser des diagnostics sur un nombre restreint de maladies (mais potentiellement en hausse), pour évaluer la gestion de la douleur.
- **Réseaux sociaux** – pour identifier les personnes dans des photos.
- **Marketing** – pour proposer des publicités 'intelligentes'.
- **Interaction Humain-Machine** – des Humains Digitaux Autonomes vont bientôt interagir avec les êtres humains et adapter leur réponse en fonction de la Reconnaissance Faciale.[1]

Les avantages

Ce n'est pas en examinant nos empreintes digitales ou en analysant les détails des iris de nos yeux que nous reconnaissons les autres, mais en regardant leurs visages.

La Reconnaissance Faciale est considérée comme **la méthode de mesure biométrique la plus naturelle**, car aucune interaction physique n'est nécessaire par l'utilisateur final.

D'autres signatures du corps humains existent, comme les empreintes digitales, l'analyse des iris, la reconnaissance vocale, la digitalisation des veines de la paume des mains ou les mesures comportementales, mais elles sont plus difficiles et lourdes à mettre en place. La reconnaissance faciale est **simple d'accès, rapide, automatique et fluide**.

Les systèmes de reconnaissance faciale sont capables de traiter de très grandes quantités d'images. Par exemple, la police britannique utilise un système proposé par la société japonaise NEC appelée NeoFace, qui peut scanner et identifier jusqu'à 300 visages par seconde.

Des erreurs, oui ... ...et pourtant les systèmes de Reconnaissance Faciale sont difficiles à leurrer.

Des défenseurs des droits de l'homme se sont servis des réseaux sociaux pour montrer que certaines combinaisons de coiffures ou de maquillage peuvent se révéler efficaces pour déjouer les systèmes de Reconnaissance Faciale.

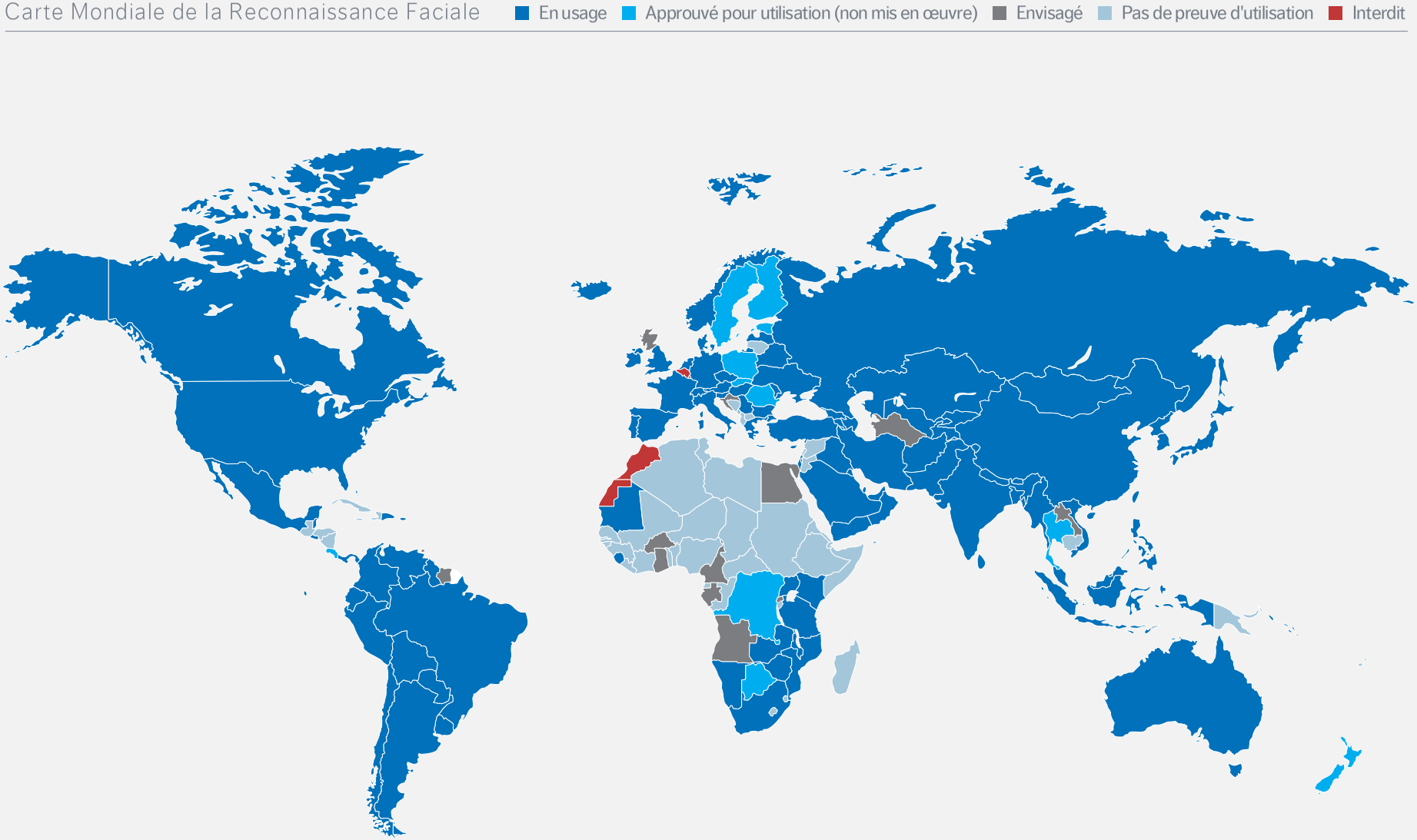
Mais en réalité, peu de personnes souhaitent se promener comme ceci :

Reconnaissance Faciale – une présence mondiale

La technologie est utilisée dans quasiment tous les pays du monde, avec quelques exceptions. La Belgique en fait notamment partie.

Figure 1 :

Carte Mondiale de la Reconnaissance Faciale

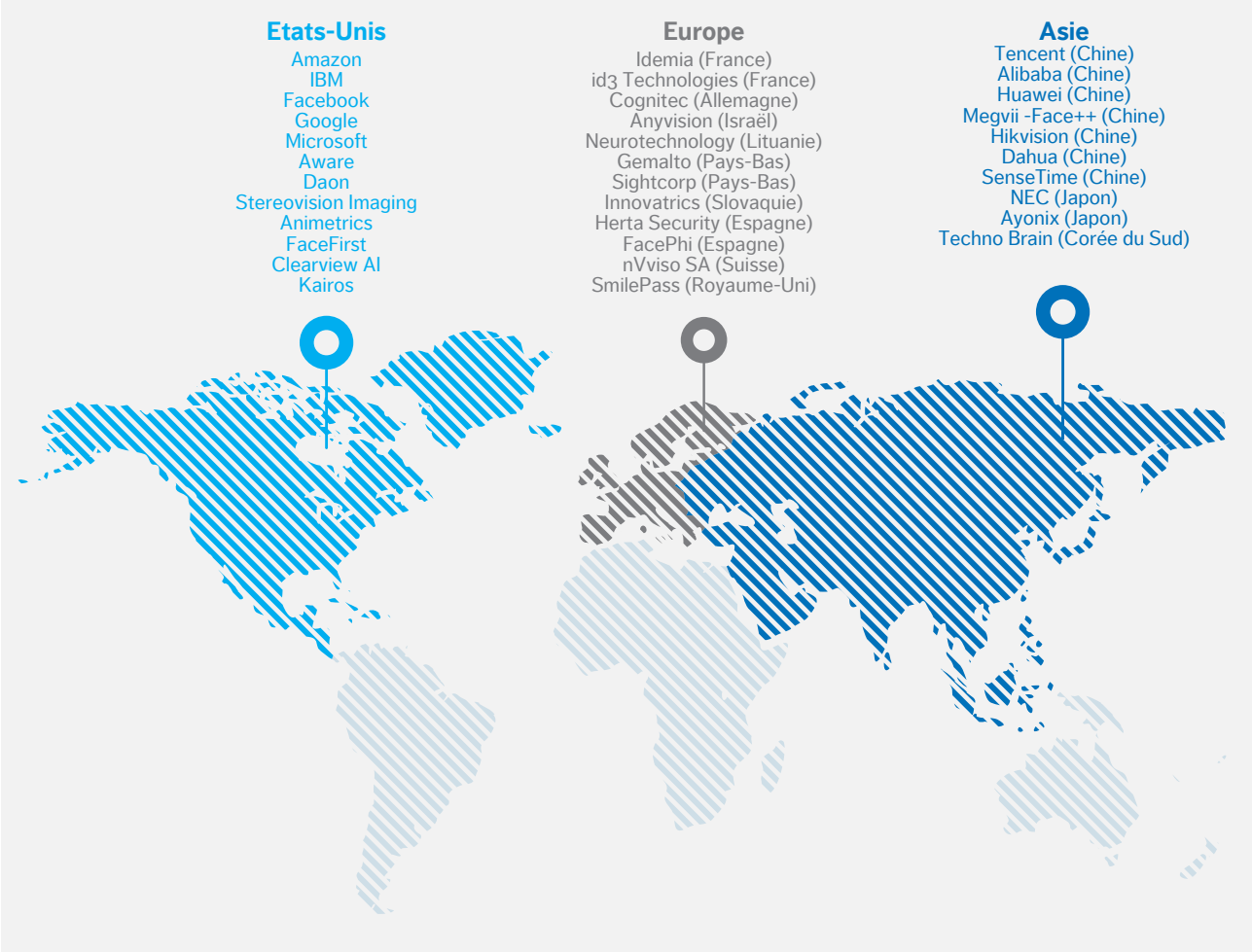


Sources : visualcapitalist.com, mai 2020; Candriam

Taille du marché et principaux acteurs

Selon une étude réalisée en 2018 par Allied Market Research[2], le marché de la reconnaissance faciale devrait atteindre 9,6 milliards de dollars d'ici 2022, ce qui correspond à **un taux de croissance proche de 25 %**. Tout bien considéré, il reste néanmoins un marché de niche. Il semble que quelques géants de la tech comme Amazon proposent ces systèmes gratuitement dans le cadre **d'abonnements à des services plus lucratifs**.

Figure 2 :
Les acteurs du marché



Source : Candriam

Risques et controverses

Au cours des dix dernières années, l'émergence de la technologie de Reconnaissance Faciale à des fins de surveillance de la population a suscité de fortes craintes pour la société, notamment sur le respect des droits de l'homme.

Une technologie invasive

La surveillance par Reconnaissance Faciale **touche un grand nombre d'entre nous** dans nos vies quotidiennes et bien souvent **sans que nous en soyons informés**. Elle permet une surveillance à très grande échelle, qui porte atteinte à nos droits.

Certes, des millions de personnes utilisent volontairement et apprécient cette technologie. De nombreux utilisateurs d'iPhone haut de gamme utilisent « Face ID » pour déverrouiller leurs smartphones. Des millions de personnes se sont inscrites au système automatisé de contrôle des frontières biométrique, comme « l'ePassport » du Royaume-Uni.

A travers le monde, les services de maintien de l'ordre déploient d'ores et déjà la Reconnaissance Faciale à très grande échelle. **Il est estimé qu'un milliard de caméras de surveillance seront opérationnelles d'ici la fin de l'année 2021**[3]. La Chine est de loin le pays qui utilise le plus profusément ces systèmes, avec 600 millions de caméras installées aujourd'hui – soit une caméra pour 2,3 habitants. La Chine est suivie de près par les États-Unis, où il est estimé que 140 millions de caméras ont été installées - une pour 2,4 habitants. La plupart sont des systèmes numériques, dont les données peuvent être exploitées par les outils de Reconnaissance Faciale.

Aujourd'hui, les habitants de Détroit, Londres, Monaco, Moscou, Beijing... vaquent à leurs occupations sans savoir que leurs visages sont scannés par des outils de reconnaissance faciale contrôlés par la police.

Des problèmes de fiabilité

En janvier 2020, Robert Williams, un résident de Détroit, a été arrêté par la police pour avoir commis des vols en magasin après avoir été faussement identifié par la reconnaissance faciale.

En 2018, un test réalisé sur la technologie d'Amazon, *Rekognition* - qui a pris comme échantillon les membres du Congrès des États-Unis - a faussement identifié 28 membres comme ayant été arrêtés par la police pour diverses infractions par le passé[4]. Ce test a également mis en évidence le biais racial de la technologie, car les membres du Congrès d'origine afro-américaine ont fait l'objet de plus de fausses correspondances avec les criminels de la base de données, et ce de manière disproportionnée. L'une de ces personnes était John Lewis, récipiendaire de la Médaille de la Liberté décernée par le Président, et aujourd'hui décédé.

Même les systèmes affichant les meilleurs taux de fiabilité aujourd'hui peuvent susciter des interrogations. Imaginez les forces de l'ordre d'une petite ville qui utiliserait une technologie de Reconnaissance Faciale avec un taux de fiabilité de 99,9% et où 100 000 personnes sont filmées tous les jours par des caméras de vidéosurveillance. Acceptons-nous que 100 individus soient faussement identifiés tous les jours ?

Depuis 2016, après quatre années de déploiement, la surveillance par Reconnaissance Faciale de la Metropolitan Police de Londres a été inefficace à 93,59 %. En 2020, lors de deux des trois déploiements, la Met a admis un taux d'échec de 100 % - c'est-à-dire qu'elle n'a pas identifié une seule personne[5]. Le rapport indépendant mandaté par la Metropolitan Police a également conclu que leur surveillance par Reconnaissance Faciale était foncièrement inexacte. Cette analyse a porté sur six des tests réalisés par la police et a conclu que le taux de fiabilité de la Met ne s'élevait qu'à 19 % et donc que les résultats sont faux 81 % du temps[6].

Pourquoi la Reconnaissance Faciale, une technologie destinée à améliorer l'efficacité et la sécurité de notre vie quotidienne, constitue également une menace pour les droits de l'homme ?

Isedua Oribhador, Analyste Politique, États-Unis, chez AccessNow : *« Si la technologie de reconnaissance faciale a été vantée comme un moyen de renforcer l'efficacité et la sécurité, nous avons déjà pu constater qu'elle est également source de risques avérés. Entre les biais raciaux et de genre qui sont intrinsèques à ces systèmes et les risques d'atteinte à la vie privée inhérents à la collecte de ces données personnelles, sans compter le potentiel de surveillance de masse des citoyens, la technologie de reconnaissance faciale constitue une réelle menace pour de nombreux droits fondamentaux. Il est impératif d'examiner ces risques et de tracer des limites strictes autour de certaines zones, dès lors que la technologie est incompatible avec le respect des droits humains. »* [7]

« Les forces de l'ordre chinoises se sont servies d'un système de Reconnaissance Faciale secret, de grande envergure, pour identifier, tracer et contrôler les 11 millions de Ouïghours, une minorité de confession principalement musulmane. »

Focus pays – La Chine

La loi de 2017 sur le renseignement en Chine impose aux organisations et aux citoyens de « soutenir, assister et coopérer avec les services de renseignement de l'Etat ». Concrètement, toutes les entreprises de logiciels ou de hardware en Chine sont sommées de transmettre leurs données à Beijing si les autorités estiment être confrontées à un problème de sécurité nationale.

Plus de 200 millions de caméras de surveillance étaient en fonctionnement en 2018 ; selon les estimations, elles sont plus de 600 millions en 2020. Parmi le top 10 des villes qui disposent du plus grand nombre de caméras par habitant, Chongqing, Shenzhen, Shanghai, Tianjin et Jinan se classent en tête. Les tours de Reconnaissance Faciale dans les villes chinoises sont symptomatiques de cette tendance. La technologie de Reconnaissance Faciale s'étend désormais aux agents de police, qui portent des lunettes de soleil 'intelligentes' capables de scanner les visages et d'alerter en cas de correspondances.

Le système de surveillance civile de la Chine est aujourd'hui lié au « Système de Crédit Social », qui note un individu en fonction de son comportement. Avec ce système, qui a vu le jour en 2013, les citoyens reçoivent des récompenses ou des punitions selon leurs scores.

La police chinoise travaille avec des entreprises développant des logiciels d'intelligence artificielle comme Yitu, Megvii, SenseTime et CloudWalk. Les fabricants d'équipements (hardware) comme Dahua et Hikvision peuvent également recevoir des commandes importantes de la part du gouvernement. Toutes ces entreprises ont été placées sur la liste noire du gouvernement américain en raison de leur implication dans la répression des Ouïghours.

Néanmoins, les ambitions de la Chine dans le domaine de l'IA et de de la technologie de RF restent très élevées. Le pays a pour objectif de se classer parmi les leaders mondiaux de l'IA d'ici 2030. En tant qu'Etat, la Chine est clairement le plus grand investisseur dans les technologies de surveillance de pointe, d'IA et de RF.

La répression des Ouïghours

Dans la région du Xinjiang, les autorités chinoises ont utilisé des technologies de reconnaissance faciale à des fins de profilage et de surveillance. Les forces de l'ordre chinoises se sont servies d'un système de Reconnaissance Faciale secret, de grande envergure, pour identifier, tracer et contrôler les 11 millions de Ouïghours, une minorité de confession principalement musulmane. La police chinoise a installé des scanners de RF à l'entrée de plusieurs mosquées de la région. Xinjiang a ainsi servi de zone de test à grande échelle pour ces entreprises, qui ont pu déployer leurs différentes fonctionnalités sans subir les contraintes habituelles.

Biais racial / de genre et vol de données

Lors des premières expériences réalisées dans le domaine de la Reconnaissance Faciale, la technologie n'a pas été capable de reconnaître les personnes d'origine afro-américaine ou asiatique. Pire, Google a été contraint de s'excuser en 2015 lorsque sa nouvelle application de l'époque, *Google Photos*, avait identifié certaines personnes de couleur noire comme étant des « gorilles ».

Une étude réalisée en 2018 par le Media Mab de MIT a révélé que certains logiciels de Reconnaissance Faciale pouvaient identifier un homme blanc avec une précision quasi-parfaite, mais échouaient de manière spectaculaire à identifier des femmes à la peau plus foncée.

Clearview AI a déclaré travailler pour plus de 2 400 services de forces de l'ordre aux États-Unis. Son Président, Hoan Ton-That, est connu pour ses liens avec les mouvements politiques d'extrême droite. Clearview a récupéré des milliards de photos sur Facebook, YouTube et Venmo pour construire sa base de données[8]. Le Président et Fondateur de Banjo, Damien Patton, a quitté ses fonctions après avoir été accusé d'entretenir des liens avec le Ku Klux Klan. A l'époque, Banjo avait signé un contrat de service de Reconnaissance Faciale de 20 millions de dollars avec l'Etat de l'Utah.

Les géants de la tech comme Amazon, Microsoft et la société mère de Google, Alphabet, ont tous été attaqués en justice pour l'utilisation de photos, sans le consentement de la personne, dans le cadre du développement et de la formation de leur technologie de Reconnaissance Faciale. Ainsi, Facebook a été contraint de verser une amende de 650 millions de dollars au titre de l'article sur la confidentialité des données de l'État de l'Illinois[9]. Les documents fuités par Edward Snowden ont révélé que l'Agence Nationale de la Sécurité américaine avait recueilli des millions d'images faciales. Ces fuites suggèrent que les photos qui ont été collectées à partir de messages électroniques, de sms, des réseaux sociaux et de chats vidéo[10].

Des utilisations frauduleuses pour profits illicites

Des enquêteurs en Russie ont découvert que l'accès au CCTV (Closed-Circuit TeleVision) en live stream de Moscou avait été mis en vente sur le Dark Net par des officiers de police vraisemblablement corrompus. Le centre-ville de Moscou est doté d'un réseau dense de 175 000 caméras de vidéosurveillance, dont la plupart sont équipées de technologie de Reconnaissance Faciale. Comme le système est basé sur le Cloud, les fonctionnaires peu scrupuleux ont pu simplement vendre leurs identifiants de connexion – pour un montant de seulement 470 dollars - offrant ainsi un accès au live stream ainsi qu'aux enregistrements des cinq jours précédents.

Au-delà de la CCTV – la surveillance de masse via les ordinateurs, les smartphones, les drones...

Quasiment tous les nouveaux smartphones, ordinateurs ou tablettes vendus aujourd'hui sont équipés d'au moins une caméra digitale. Or chacune de ces caméras peut alimenter un système de Reconnaissance Faciale.

Un autre domaine qui suscite des inquiétudes est le déploiement de la technologie des caméras militaires sur les drones, comme l'ARGUS-IS, qui peut permettre aux gouvernements d'enregistrer en continu des zones allant jusqu'à 10 miles^2 ou 26 km^2, soit la moitié de la surface de Manhattan. Ces systèmes sont suffisamment puissants pour scanner les visages de tous les individus présents dans ce rayon, à tout moment[11].

Les enjeux

L'absence de consentement

L'absence de consentement est au cœur du problème. Aucune entreprise ou agence, aucun État ou gouvernement n'a demandé le consentement des citoyens. Dans la plupart des juridictions, lorsque ces derniers présentent une photo d'identité à l'administration pour obtenir un passeport, une carte d'identité ou un permis de conduire, ils ne consentent - à aucun moment - à ce que leur photo soit utilisée à des fins de Reconnaissance Faciale. Les autres formes d'identification biométrique impliquent le consentement de la personne concernée. Il y a peu de chances que les membres du public scannés par la Reconnaissance Faciale soient conscients d'avoir fait l'objet d'une authentification d'identité et ils n'ont pas la possibilité de donner leur accord ou de la refuser.

En Europe, la directive générale sur la protection des données (GDPR) introduite en 2016 est très claire sur le fait que les données biométriques obtenues par la technologie de Reconnaissance Faciale sont des données personnelles. Elles tombent dans le champ de la protection de données et nécessitent donc le consentement de la personne, si ces données sont ensuite utilisées par un individu, une entreprise, un organisme. Et pourtant, les forces de l'ordre dans des pays de l'UE comme le Royaume-Uni, la France, l'Italie et la Grèce utilisent déjà cette technologie.

Absence de fondement juridique

Dans la plupart des pays, aucune base juridique n'autorise la police à utiliser la surveillance en live par Reconnaissance Faciale. La Reconnaissance Faciale empiète sur les lois fondamentales garantissant la liberté, comme le Premier Amendement de la Constitution américaine ou le Human Rights Act au Royaume-Uni.

Clare Garvie, de Georgetown Law's Center on Privacy & Technology, explique à Candriam que : *« Le recours à la reconnaissance faciale par la police aux États-Unis reste largement non-règlementée, malgré les efforts de certains États et associations locales pour interdire entièrement son usage et le fait qu'elle ait entraîné l'arrestation d'au moins trois hommes innocents. Compte tenu des risques qu'elle fait peser sur les droits constitutionnels à la vie privée, à la liberté d'expression, aux procès justes et à l'égalité de la protection des lois, le recours à la reconnaissance faciale nécessite un moratoire, à moins que des mesures de règlementation fortes ne soient imposées pour protéger ces droits ».*

Un manque de supervision

Dans la plupart des pays, comme aux États-Unis ou en Europe, une supervision appropriée et impartiale visant à contrôler l'utilisation de technologies de surveillance par les entreprises privées et les services des forces de l'ordre semble faire largement défaut.

Une intrusion disproportionnée

De multiples tests réalisés au Royaume-Uni ont permis de déterminer le taux de réussite suivant : un criminel a été identifié tous les 300 000 visages scannés. Le Commissaire en charge des caméras de surveillance a conclu que le déploiement a été extrêmement disproportionné, notant que « compte tenu de l'échelle et du volume de traitement associé à toutes les personnes passant devant une caméra, le groupe qu'ils cherchent à identifier est extrêmement petit ».

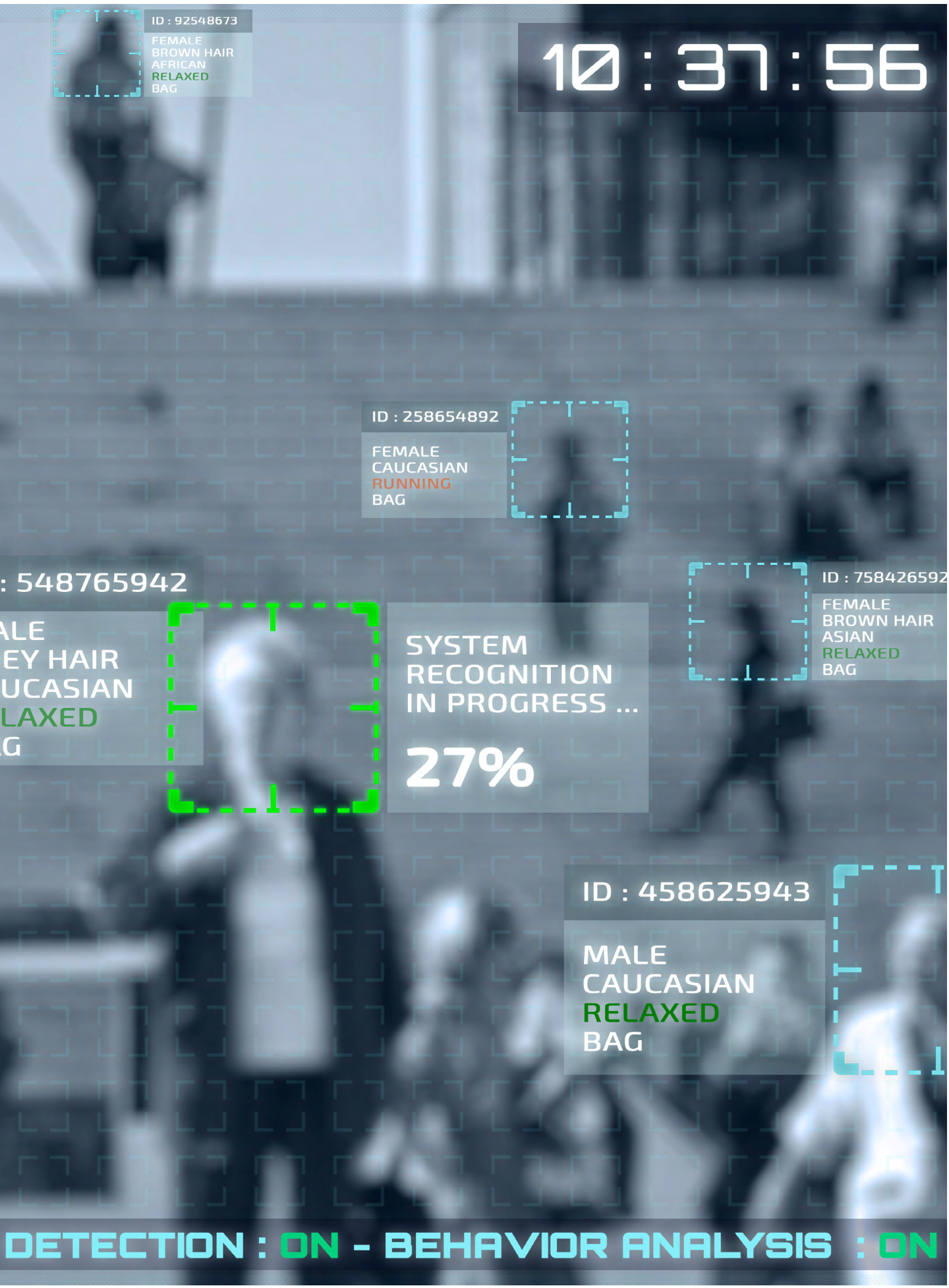
Le droit à l'anonymat

Une société prospère repose sur plusieurs libertés – la liberté d'expression, de mouvement, de religion, d'association – mais également sur le droit à un certain degré d'anonymat. Or le droit de nous déplacer dans des lieux publics en toute anonymité n'est plus garanti à ce jour en raison du déploiement à grande échelle des systèmes de Reconnaissance Faciale.

Tout le monde devrait pouvoir se promener librement en tout anonymat. Il est de notre nature, en tant qu'êtres humains, de vouloir vivre sans que nos faits et gestes soient observés. Et pourtant, notre espace « non-surveillé » se réduit très rapidement. Le fait d'être identifiés, où que nous allions, par les forces de l'ordre, les entreprises ou l'État, entrave notre individualité. A terme, ceci aura un impact négatif sur nos mouvements, notre créativité, notre confiance et même sur la démocratie.

A titre d'exemple, le rapport du Panel Déontologique de la Police de Londres sur la surveillance à Reconnaissance Faciale en live a relevé que 38 % des jeunes entre 16 et 24 ans choisiraient d'éviter des événements ou des endroits où la surveillance par Reconnaissance Faciale était utilisée, à l'instar d'un grand nombre de personnes noires, asiatiques ou issues de minorités ethniques[12].


CAM 3
ID : 254876592
MALE
BROWN HAIR
CAUCASIAN
STRESSED
ID
MA
GR
CA
RE
BA
BIOMETRIC IDENTIFICATION : ON - OBJECTS


ID : 92548673
FEMALE
BROWN HAIR
AFRICAN
RELAXED
BAG
10 : 37 : 56
ID : 258654892
FEMALE
CAUCASIAN
RUNNING
BAG
: 548765942
ALE
EY HAIR
UCASIAN
LAXED
G
SYSTEM
RECOGNITION
IN PROGRESS ...
27%
ID : 758426592
FEMALE
BROWN HAIR
ASIAN
RELAXED
BAG
ID : 458625943
MALE
CAUCASIAN
RELAXED
BAG
DETECTION : ON - BEHAVIOR ANALYSIS : ON

Une petite perte de confidentialité est-elle le prix à payer pour plus de sécurité ?

Lorsque l'on leur demande ce qu'ils pensent de la Reconnaissance Faciale, les citoyens répondent majoritairement qu'ils comprennent de devoir perdre peu de confidentialité pour plus de sécurité. L'argument qui convainc est celui de la localisation rapide d'une personne soupçonnée de terrorisme ou d'un enfant qui a été enlevé.

Le secteur de la surveillance exploite le marketing de la peur. Les craintes d'une attaque terroriste, par exemple. La ville de Nice a été le théâtre d'un terrible attentat en 2016 lorsqu'un terroriste, au volant d'un en camion, a foncé dans la foule rassemblée sur le front de mer pour fêter le 14 juillet, provoquant la mort de 87 personnes. En réaction, la municipalité a équipé les forces de police locales avec des systèmes de Reconnaissance Faciale et des technologies de surveillance les plus importantes de toutes les villes de France.

En tant que citoyens responsables, nous devrions nous poser les questions suivantes :

- Voulons-nous être identifiés, en continu, par des algorithmes non-testés et potentiellement inexacts ou biaisés ?
- Voulons-nous que nos gouvernements enregistrent chacun de nos mouvements, les endroits que nous visitons et les personnes que nous rencontrons ?
- Souhaitons-nous que les forces de l'ordre soient capables d'enregistrer les noms de tous les participants à une manifestation ou célébration religieuse ?
- Acceptons-nous d'accorder à nos gouvernements des pouvoirs illimités leur permettant de surveiller ***Tout le Monde, Partout, Tout le Temps ?***

Une société de schizophrènes ?

Lorsque nous autorisons nos gouvernements et les forces de l'ordre à déployer cette technologie de surveillance pour assurer notre sécurité, nous acceptons également que pour que nous soyons tous en sécurité, il faut surveiller tout le monde en continu. Pour certains sociologues, il s'agit là d'une forme de schizophrénie.

Des différences culturelles dans l'acceptabilité d'une surveillance de l'État

Nous ne pouvons pas analyser les problématiques de droits de l'homme liées à la Reconnaissance Faciale à travers le prisme des valeurs occidentales. La perception de la vie privée et de l'intrusion est très variable selon les cultures. En Chine, la majorité des personnes estime que la surveillance de masse est un compromis normal pour assurer la sécurité. Ces dernières années, l'association d'un déploiement de masse de technologie de surveillance avec le lancement du Système de Crédit Social (voir encadré, page 13) a contribué à une baisse spectaculaire des taux de criminalité.

Une parade d'identification continue

Selon ce concept, décrit par le *Centre for Privacy and Technology* de Georgetown Law[13], personne ne prendrait volontairement part à un alignement de suspects sachant que la victime allait identifier le coupable ! La victime pourrait en effet vous sélectionner par erreur. Or les systèmes de Reconnaissance Faciale le font tous les jours, quasiment partout aux États-Unis et en Chine[14].

Le capitalisme de surveillance

Dans son livre « The Age of Surveillance Capitalism », Shoshana Zuboff définit ainsi le capitalisme de surveillance : un processus proposant des services gratuits, que des milliards de personnes utilisent sans états d'âme, et qui permettent aux fournisseurs de ces dits services de suivre le comportement de ces usagers avec un degré de détail remarquable – souvent, sans leur accord explicite. « Le capitalisme de surveillance exploite, de manière unilatérale, les expériences humaines qui lui offrent de la matière gratuite transformable en données comportementales. Les capitalistes de la surveillance réalisent des bénéfices financiers gigantesques grâce à la monétisation des données comportementales individuelles et collectives et aux prévisions sur les comportements futurs des personnes ».

La combinaison d'un état de surveillance et de sa contrepartie capitaliste signifie que la technologie digitale **sépare les citoyens, dans toutes les sociétés, en deux groupes : *ceux qui regardent* – invisibles, inconnus et sans restriction – et *ceux qui sont regardés***. Cet état de fait a deux conséquences profondes pour la démocratie, car l'asymétrie de l'information engendre des asymétries de pouvoir. Mais si la plupart des sociétés démocratiques a un certain degré de contrôle sur la surveillance de l'État, nous n'avons, à l'heure actuelle, aucun contrôle réglementaire sur sa version privatisée[15].

Engagement – Guide pratique

En tant qu'investisseur responsable, notre rôle est d'intégrer les facteurs environnementaux, sociaux et de gouvernance (ESG) à nos décisions d'investissement et de mettre en pratique notre démarche d'actionnariat actif. Notre objectif est de créer de la valeur pour nos clients sur le long terme, en générant des impacts positifs pour l'économie, l'environnement et l'ensemble de la société.

Nous sommes convaincus que l'intégration de la technologie de Reconnaissance Faciale et de toutes ses implications à notre gestion et à notre démarche d'engagement contribuera aux deux pans de cet objectif. Un nombre en progression constante d'entreprises, d'États et de régions dans lesquels nous investissons sont concernés et impliqués dans cette technologie.

Si nous n'investirions sans doute pas expressément dans un acteur pur de la Reconnaissance Faciale, tout investissement dans une entreprise qui l'utilise ou commercialise cette technologie doit s'accompagner d'un processus de « due diligence » rigoureux, visant à :

- Evaluer les risques associés,
- Partager nos éventuelles inquiétudes avec les entreprises détenues en portefeuille,
- Encourager les changements qui peuvent contribuer à atténuer les risques identifiés.

Comme nous l'avons décrit dans note chapitre consacré à la technologie et aux enjeux associés, les attentes des investisseurs peuvent être multiples, complexes et variables selon les parties prenantes. Les objectifs portent notamment sur :

Emetteurs privés

- **Engagement direct et/ou collaboratif** afin de mieux comprendre les pratiques des entreprises Elargir le recours aux meilleures pratiques en établissant un dialogue avec les entreprises, les ONG etc.

- **Intégrer les évolutions dans l'analyse ESG** des entreprises. Définir les meilleures pratiques, le progrès acceptable et les critères d'exclusion.

- **Encourager les entreprises à l'amélioration de leurs comportements**. Continuer de placer l'éthique et le respect des droits de l'homme au cœur de la gouvernance des entreprises. Mettre en place un comité indépendant consacré au risque de droits humains rattaché au Conseil d'Administration. Encourager les entreprises à choisir des clients et des fournisseurs qui respectent les valeurs qu'ils défendent.

Gouvernements

- **Inciter à la suspension du recours à la Reconnaissance Faciale par les forces de l'ordre,** tant qu'un cadre réglementaire spécifique n'a pas été instauré.

Universités

- **Encourager la dispense de cours sur l'Ethique** dans les cursus AI/ Tech.

Chez Candriam, si nous souhaitons aborder ce sujet avec les autorités européennes, nous estimons que notre levier prioritaire sera d'initier un dialogue avec les entreprises, et surtout avec celles qui figurent déjà dans nos portefeuilles.

Dans cette perspective et inspirés par nos échanges avec les spécialistes et experts de la Reconnaissance Faciale, nous avons établi une série de questions (page 25) qui ont pour objectif d'aider les investisseurs à mesurer l'implication des entreprises détenues en portefeuille dans la Reconnaissance Faciale, mais également à capter le niveau de risques associés en termes de droits de l'homme.

Open MIC travaille depuis de nombreuses années avec les actionnaires afin d'encourager les entreprises à adopter des pratiques « éthiques » dans le domaine de la reconnaissance faciale.

Les entreprises de la Big tech ont déployé beaucoup d'énergie et de ressources pour résister à ces efforts. Malgré une pression intense de la part des actionnaires – mais également de la part de multiples organisations dédiées aux droits de l'homme – les entreprises refusent, en grande partie, d'admettre qu'il existe un problème.

Comme le souligne ce rapport, quasiment tous les produits de reconnaissance faciale présents sur le marché fonctionnent sans le consentement des millions de personnes dont les visages sont scannés quotidiennement. Il a été démontré qu'un grand nombre de ces systèmes comportent des biais raciaux. Or il n'existe aucun recours ou mesure corrective pour ces personnes dont les droits ont été bafoués, ce qui est contraire aux principes directeurs relatifs aux entreprises et aux droits de l'homme des Nations Unies. En 2019, le Rapporteur Spécial de l'ONU sur la liberté d'opinion et d'expression a recommandé un « moratoire immédiat sur le périmètre mondial et le transfert des technologies de surveillance privée, tant que des mesures de protection des droits humains n'ont pas été adoptées ». Il n'existe à ce jour aucune garantie sur le respect des droits de l'homme et pourtant les ventes se poursuivent. Comme le rappelle ce rapport, le marché est même en plein essor.

Une des questions est de savoir si la perspective d'un cadre réglementaire et juridique – dans les pays de l'UE et aux États-Unis – peut inciter les entreprises à adopter de réels standards à l'échelle du secteur. Les acteurs de la filière vont sans doute exercer de la pression, par le biais de lobbies, pour diluer les contrôles de l'État sur la reconnaissance faciale. Les investisseurs doivent donc continuer à faire ce qu'ils font déjà : utiliser tous les outils qui sont à leur disposition pour inciter les entreprises à mettre en place les politiques et les pratiques qui feront bouger les lignes ; il sera intéressant de voir si un engagement collaboratif médiatisé et de grande ampleur, comme celui préconisé ici, peut inciter les entreprises à initier des dialogues plus productifs.

Michael Connor est le Président Fondateur d'Open MIC, une association à but non lucratif qui œuvre pour renforcer la responsabilité des entreprises au sein des secteurs des médias et de la technologie, principalement à travers une démarche d'engagement. En travaillant en partenariat avec les investisseurs socialement responsables, Open MIC identifie, développe et soutient les campagnes visant à promouvoir les valeurs d'ouverture, d'égalité, de respect de la vie privée et de diversité – des valeurs créatrices d'avantages à long terme pour les citoyens, les entreprises, l'économie et la santé de nos sociétés démocratiques. Open MIC travaille aujourd'hui sur des campagnes ciblant Amazon, Twitter, Google et Facebook.

Guide de l'Engagement

Niveau d'implication

- Votre entreprise fournit-elle des produits (hardware, logiciels, bases de données) liés à la technologie de reconnaissance faciale ?

- Quelle est la fonction du produit ?
  • Surveillance
  • Identification
  • Maintien de l'ordre
  • Catégorisation (ex. publicités ciblées)
  • Investigations
  • Sécurité
  • Autre (merci de préciser)

- A quels types d'utilisateurs proposez-vous une technologie de reconnaissance faciale ?
  • Gouvernements ou États
  • Ecoles
  • Services des forces de l'ordre
  • Entreprises
  • Armées

Gouvernance

- Votre entreprise a-t-elle adopté une politique destinée au public portant sur la technologie de reconnaissance faciale ? Si oui, quel a été l'impact de cet engagement sur
  1) vos relations avec vos partenaires commerciaux, sous-traitants, clients et utilisateurs finaux ? et
  2) sur vos activités de lobbying ?

- Quels risques associés à la technologie de reconnaissance faciale avez-vous identifiés et à quelle fréquence sont-ils remontés au Conseil d'Administration ?

- Votre entreprise réalise-t-elle des évaluations d'impact en matière de droits humains afin d'identifier et évaluer les risques réels et potentiels liés à vos technologies de reconnaissance faciale ? Quels risques avez-vous identifiés et quelles sont les parties prenantes impliquées dans cette évaluation ? Comment avez-vous adapté votre fonctionnement et votre stratégie ? Qui, au sein de l'entreprise (au niveau de l'entité / de la région / de la branche) est responsable de gérer l'ensemble de ces risques spécifiques et leurs impacts potentiels au quotidien ?

- Quels processus avez-vous mis en place pour définir les clients auxquels vous pouvez vendre vos produits ? Avez-vous interdit les ventes/livraisons de votre produit ou service à certains pays gouvernés par des régimes totalitaires/non démocratiques ?

Gestion des risques liés à la conception

- Comment êtes-vous organisés en interne pour identifier, prévenir et résoudre les problèmes liés à la Reconnaissance Faciale ?

Plus précisément :

- Comment votre entreprise a-t-elle construit/obtenu/acheté la base de données de photos/noms utilisée à l'entraînement ? Si vous n'avez pas construit la base de données vous-mêmes, comment votre prestataire a-t-il construit/obtenu/acheté la base de données que vous utilisez ?

- Communiquez-vous sur la fiabilité de votre technologie, et de la leur, après qu'elle ait été mesurée par un organisme d'évaluation scientifique, comme National Institute of Standards and Technology (NIST) ? Si cela n'est pas le cas, merci d'apporter des explications.

- Quelles vérifications sont réalisées en interne pour détecter les biais de l'algorithme, par exemple sur les races, les genres ou l'âge ? Qu'en est-il de votre/vos fournisseur(s) ?

- Avez-vous mis en place un mécanisme de réclamations et d'indemnisation en cas d'identification erronée pour les personnes indûment impactées par la technologie à ce niveau ?

Gestion des risques liés à l'utilisation

- Vos clients sont-ils soumis à des restrictions réglementaires dans leur utilisation de la technologie de reconnaissance faciale ? Est-ce un facteur que vous suivez ?

- Votre produit propose-t-il une technologie de reconnaissance faciale pour une analyse en temps réel, ou uniquement rétroactive ?

- Votre produit analyse-t-il les vidéos live ou uniquement les images statiques ?

- Votre produit de technologie de reconnaissance faciale propose-t-il une forme de catégorisation, par exemple par genre, par âge, raciale, mentale, ou autre ? Votre technologie de reconnaissance faciale propose-t-elle une forme d'analyse prédictive ?

- Avez-vous mis en place un mécanisme de réclamation et d'indemnisation en cas d'identification erronée pour les personnes indûment impactées par la technologie à ce niveau ?

Conclusion

Aujourd'hui, la Reconnaissance Faciale est une problématique qui manque cruellement de transparence. Son utilisation est bien accueillie par certains, controversée pour d'autres. Ses usages peuvent être détournés et l'existence de biais et d'erreurs a été prouvée.

Or sans transparence, il est impossible d'évaluer ces controverses. Des leviers plus forts seront nécessaires pour ouvrir la voie à un processus d'analyse et de dialogue. Les pouvoirs publics ont commencé à agir, au niveau national et local. Les entreprises aussi. Le débat commence à s'ouvrir et une dynamique se crée au sein de la population ; les ONG lancent des campagnes.

Maintenant, c'est au tour des investisseurs de réagir.

Notes et Références

[1] Mashable.com. *Douglas, the latest step toward realistic AI, is unsettling.* Actualisé le 22 novembre 2020. https://mashable.com/article/douglas-realistic-ai-unsettling/?europe=true, consulté le 8 février 2021.

[2] https://www.alliedmarketresearch.com/press-release/facial-recognition-market.html

[3] CNBC. *One billion surveillance cameras will be watching around the world in 2021.* 6 décembre 2019. https://www.cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html, consulté le 8 février 2021.

[4] The American Civil Liberties Union. ACLU.com. Snow, Jacob. *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots.* 26 juillet 2018. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28, consulté le 8 février 2021.

[5] Metropolitan Police. LIFR Deployments 2020. https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/latest-past-deployment-data.pdf, consulté le 8 février 2021.

[6] The Human Rights, Big Data and Technology Project. Fussey, Professor Pete and Dr. DaraghMurray. Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. Juillet 2019. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf, consulté le 8 février 2021.

[7] Isedua Oribhabor est Analyste Politique, États-Unis, pour AccessNow. Son périmètre d'analyse couvre également les droits des Entreprises et les droits de l'homme. La recherche réalisée par Isedua avec le *Leitner Center for International Law and Justice* à Fordham a éveillé son intérêt pour les Droits des Entreprises et les Droits Humains, l'encourageant à approfondir le sujet dans le cadre du secteur de la technologie. AccessNow est une organisation mondiale non-gouvernementale spécialisée dans la défense des droits de l'homme dans le domaine de la technologie. AccessNow s'intéresse principalement aux domaines suivants : respect de la vie privée, liberté d'expression, sécurité digitale, droits des entreprises et droits humains et discriminations nettes. AccessNow est une organisation internationale qui emploie 60 personnes dans 13 pays.

[8] The New York Times. Hill, Kashmir. *The Secretive Company That Might End Privacy as We Know It.* Actualisé le 31 janvier 2021. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, consulté le 8 février 2021.

[9] CNET News. Musil, Steven. *Amazon, Google, Microsoft sued over photos in facial recognition database.* 14 juillet 2020. https://www.cnet.com/news/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/, consulté le 8 février 2021.

[10] The New York Times. Risen, James and Laura Poitras. *N.S.A. Collecting Millions of Faces From Web Images.* 31 mai 2014. https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html, accessed 8 February, 2021.

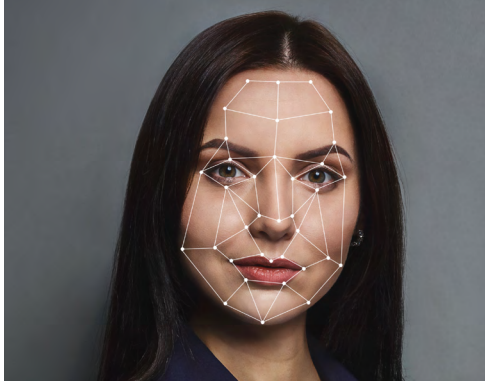
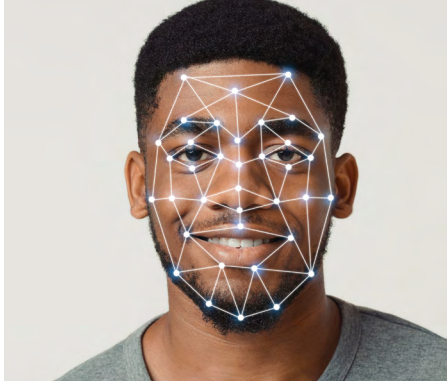
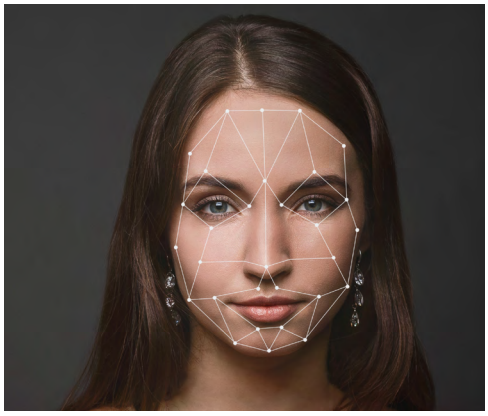
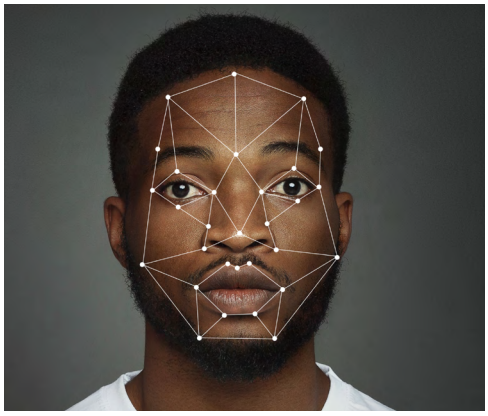
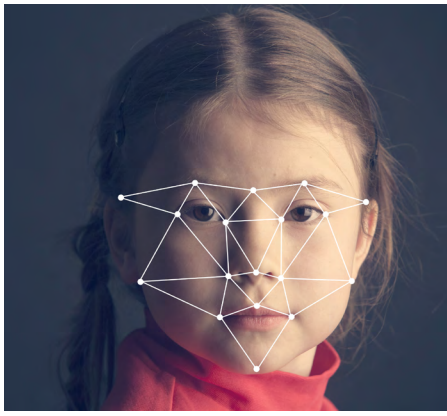
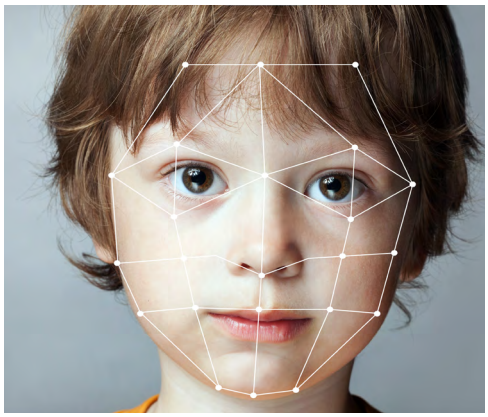
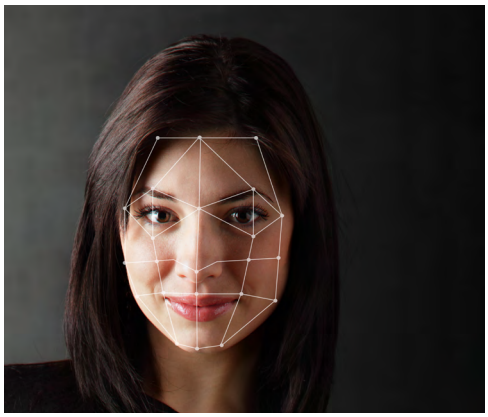
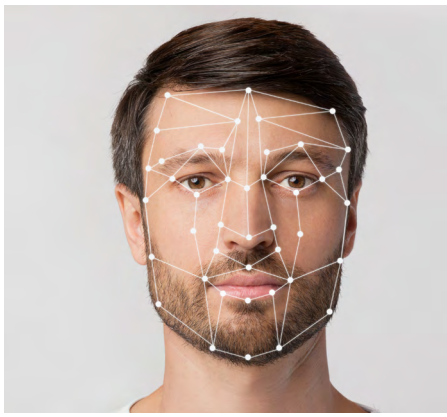
[11] University of Richmond Law Review. Laperruque, Jake. *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance.* Mars 2017. http://lawreview.richmond.edu/files/2017/03/Laperruque-513-website.pdf, consulté le 8 février 2021.

[12] http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf

[13] Georgetown Law Center on Privacy & Technology. Garvie, Clare; Alvaro Bedorya, and Jonathan Frankle. *The Perpetual Line-Up: Unregulated Police Face Recognition in America.* https://www.perpetualline-up.org/, consulté le 8 février 2021.

[14] Ce concept a également été utilisé dans le documentaire d'Arte réalisé par Sylvain Louvet : « Tous surveillés, 7 milliards de suspects ». Ce documentaire a obtenu le prix Albert Londres du meilleur documentaire en 2020.

[15] The Guardian. Naughton, John. *'The goal is to automate us': welcome to the age of surveillance capitalism.* 20 janvier 2019. https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook, consulté le 8 février 2021.

140 Mds €

d'actifs sous gestion
au 31 décembre 2020

570

experts
à votre service

25 ans

Leader dans
l'investissement responsable

CANDRIAM. INVESTING FOR TOMORROW.

WWW.CANDRIAM.COM

CANDRIAM
A NEW YORK LIFE INVESTMENTS COMPANY