# LA RECONNAISSANCE FACIALE

La reconnaissance faciale est sans doute l'une des applications de vision par ordinateur fondées sur l'intelligence artificielle les plus polémiques mais aussi les plus répandues. C'est une forme de technologie biométrique : un processus qui permet de reconnaître une personne par une caractéristique physique ou de comportement. Il existe d'autres exemples de cette technologie tels que la reconnaissance des empreintes digitales ou de l'iris, la reconnaissance vocale et l'identification par la façon de marcher. La reconnaissance faciale comprend deux phases : premièrement, les informations biométriques de l'image sont utilisées pour créer un modèle du visage, qui est ensuite comparé à une base de données d'images.[1]

La reconnaissance faciale a deux fonctions : authentifier et identifier une personne. Dans le premier cas, le système compare le modèle biométrique d'un visage à une image d'une personne précise afin de vérifier qu'il s'agit bien de la même personne. Dans le deuxième cas, le modèle est comparé à une banque d'images afin d'identifier une personne parmi d'autres. Une troisième fonction est très polémique, il s'agit de la catégorisation : classer les gens en diverses catégories selon leurs caractéristiques individuelles, telles que le sexe, l'âge et l'origine ethnique[2] La technologie de la reconnaissance faciale en direct concerne la comparaison en temps réel entre des images enregistrées et celles figurant dans les banques d'images.

[1] Reconnaissance faciale : pour un débat à la hauteur des enjeux. CNIL; 2019. Disponible à: https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf

[2] Facial recognition technology: Fundamental rights considerations in the context of law enforcement. European Agency for Fundamental Rights (FRA); 2019. Disponible : https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf

## LA RECONNAISSANCE FACIALE DANS LA VIE QUOTIDIENNE

La reconnaissance faciale est une fonctionnalité de logiciel qui peut être intégrée dans toute une gamme de technologies actuelles et connectée à d'autres fonctionnalités. Certains smartphones utilisent la reconnaissance faciale comme une mesure de sécurité : seul.e le/la propriétaire peut déverrouiller le téléphone. Si l'utilisateur est d'accord, les plateformes des réseaux sociaux comme Facebook créent un modèle de son visage à partir des photos taguées et l'utilisent pour le reconnaître dans des photos ou vidéos.

Les gouvernements peuvent utiliser cette technologie pour améliorer l'accès aux services publics en ligne. Quand un utilisateur s'inscrit à l'application mobile ALICEM du gouvernement français, celle-ci authentifie les papiers d'identité de la personne avec un logiciel de reconnaissance faciale. Une fois ce processus terminé, l'utilisateur peut accéder aux services publics avec l'application. En Europe, la plus grande partie des expérimentations avec la technologie de reconnaissance faciale a lieu dans le domaine des transports. L'Italie a utilisé la technologie pour mesurer les flux de passagers à l'aéroport Fiumicino de Rome, et plusieurs aéroports français, y compris Charles de Gaulle, ont installé le système automatique de vérification des passeports Parafe (Passage automatisé rapide aux frontières extérieures).

## LA RECONNAISSANCE FACIALE DANS LE DOMAINE DE LA SÉCURITÉ URBAINE ET SON IMPACT SUR LE SENTIMENT DE SÉCURITÉ

Dans le domaine de la sécurité urbaine, les logiciels de reconnaissance faciale peuvent être utilisés pour la prévention, la détection et l'enquête sur les crimes et délits. Parmi les exemples d'applications figurent la recherche de personnes disparues, notamment les enfants et les personnes âgées, et l'identification et la traque de criminels. Un autre exemple est l'utilisation de la reconnaissance faciale pour repérer les cas d'usurpation d'identité.

Plusieurs villes européennes ont expérimenté la reconnaissance faciale dans les espaces publics. Pendant le carnaval de Nice 2019, la mairie et la police municipale l'ont ainsi testée dans l'une des zones où se déroule le carnaval. La police métropolitaine de Londres a mené des opérations pilotes un peu partout dans la ville, notamment pendant le carnaval de Notting Hill.

Le projet européen Cutting Crime Impact (CCI) concentre une partie de sa recherche sur la mesure et la réduction du sentiment d'insécurité et la prévention de la délinquance par l'aménagement urbain (Crime Prevention through Urban Design and Planning, CP-UDP). Une des difficultés tient au fait que si l'on cherche à satisfaire un groupe de population en particulier, on risque d'en exclure un autre. Les technologies de surveillance fondées sur l'intelligence artificielle peuvent satisfaire une partie du public et améliorer le sentiment de sécurité, mais une autre partie du public peuvent considérer qu'il s'agit d'une surveillance non sollicitée dans certains espaces publics, ou qu'elle porte atteinte aux libertés individuelles. La recherche a aussi montré qu'un niveau plus élevé de surveillance peut avoir les mêmes effets que des murs ou des fils barbelés, qui en fait accroissent le sentiment d'insécurité.[3]

La présence de caméras de surveillance et savoir qu'elles sont équipées d'un logiciel de reconnaissance faciale peuvent donc avoir un impact sur le sentiment de sécurité des habitants et même la manière dont ils utilisent ou se comportent dans les espaces publics. Certains peuvent hésiter à utiliser des espaces publics qu'ils savent être sous surveillance. Cela peut avoir un effet négatif sur la liberté d'expression et de réunion. De plus, un usage limité d'un espace public peut avoir un impact économique sur tout un quartier.

[3] Davey and Wootton (2019), PIM Toolkit 4: Report on feelings of insecurity - Concepts and models adapted from Davey, C.L., & Wootton, A.B. (2014) "Crime and the Urban Environment: The Implications for Wellbeing", in Wellbeing. A Complete Reference Guide (Eds) Burton, R., Davies-Cooper,R. and Cooper, C. Wiley-Blackwell: Chichester (UK)

## IMPLICATIONS LÉGALES, SOCIALES ET ÉTHIQUES

La technologie de reconnaissance faciale suscite la controverse pour diverses raisons. On cite généralement son impact sur le droit à la vie privée, à la protection des données et à la non-discrimination mais elle soulève aussi des questions quant au respect d'autres droits fondamentaux. Il faut donc prendre en compte ceux-ci à toutes les étapes du processus de développement, d'utilisation et d'évaluation de cette technologie.

### *1. Les droits fondamentaux*

Le premier droit fondamental à prendre en compte, c'est la dignité humaine, qui est le fondement des autres droits fondamentaux protégés par la législation européenne Comme on l'a vu, le fait que certains espaces publics soient sous surveillance avec la technologie de reconnaissance faciale peut avoir un impact sur la façon dont les citoyens utilisent ces espaces. Ceci est directement lié à la liberté de réunion et d'association et à la liberté d'expression. D'autres droits fondamentaux que les collectivités doivent prendre en compte lorsqu'elles envisagent d'utiliser cette technologie sont les droits des enfants et des personnes âgées, le droit à une bonne administration et le droit à un recours effectif et à un procès équitable. Les enfants sont particulièrement vulnérables et il convient d'étudier avec beaucoup de soin les questions de nécessité et de proportionnalité lorsqu'on envisage d'utiliser leurs données biométriques, dont les photos du visage.

Les caractéristiques faciales des enfants évoluent à mesure qu'ils grandissent, ce qui augmente le risque des erreurs d'identification. Cela s'applique aussi aux personnes âgées, dont l'apparence faciale change avec l'âge et pourrait avoir un effet sur la précision de la reconnaissance faciale. En 2019, l'agence suédoise de la protection des données a donné sa première amende en réponse à une école qui avait utilisé la reconnaissance faciale pour vérifier la présence des élèves en cours . Le recours à cette technologie dans ce cas était une violation du Règlement général sur la protection des données (RGPD).

---

### *2. La collection des données et la non-discrimination*

Bien que la précision de la technologie de reconnaissance faciale se soit améliorée au fil des années grâce aux développements de la capacité informatique et l'intelligence artificielle ainsi qu'à une quantité croissante de données, des risques d'erreurs d'identification persistent. Ainsi, diverses études ont montré que le taux d'erreurs varie en fonction du genre et de la couleur de peau.[4] Il n'est pas difficile en soi de reconnaître les genres et les origines ethniques ne sont pas en elles-mêmes plus difficiles à reconnaître, mais les systèmes n'ont souvent pas d'ensembles de données à partir desquels ils peuvent apprendre.

Un autre problème est lié au manque d'études de recherche sur le fonctionnement de la reconnaissance avec les personnes handicapées. De tels résultats vont à l'encontre de l'idée courante selon laquelle la technologie est neutre ou objective et rendent d'autant plus pressante la nécessité de prendre en compte le droit fondamental à la non-discrimination. Il est donc très important d'intégrer des mesures pour éviter la reproduction des biais et les erreurs d'identification lors de l'étape du développement de la technologie.

[4] The Best Algorithms Struggle to Recognize Black Faces Equally, Tom Simonite. Wired, 2019 - https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/

---

### *3. Les origines des données et du logiciel*

Dans la mesure où les données utilisées pour alimenter et former le logiciel de reconnaissance faciale sont essentielles pour sa qualité, il est important de comprendre d'où elles viennent, qui les a collectées et pour quelle raison. On peut utiliser des données secondaires et dans ce cas, il faut prendre en compte le fait que l'objectif de la collecte est différent de celui poursuivi dans l'usage qui nous occupe. Selon le type d'algorithme d'intelligence artificielle utilisé, il peut être plus facile ou plus difficile de vérifier d'où viennent les données et comment l'algorithme a informé ses décisions. Un algorithme basé sur des règles est formé par un règlement désigné par des personnes, ce qui rend plus faciles la vérification et l'évaluation. Si l'algorithme se base sur l'apprentissage en profondeur, il nécessite de plus grandes quantités de données et il génère des résultats basés sur des probabilités. Cela rend le processus plus difficile et donc moins transparent.

---

### *4. La vie privée et la protection des données*

Bien que plusieurs villes et régions européennes s'intéressent à l'utilisation des systèmes de reconnaissance faciale, la question demeure de savoir si elles ont l'expertise et les ressources pour éviter des conséquences éventuellement discriminatoires. Toutes les collectivités locales n'ont pas la capacité de développer en interne un logiciel et de former leur police à travailler avec elles. Cela peut réduire la transparence et avoir un impact négatif sur le droit à une bonne administration, qui comprend le droit d'un individu à accéder à son dossier et à consulter les preuves sur la base desquelles une mesure a été prise contre lui. (FRA, 2019).
De plus, les collectivités locales doivent aussi pouvoir protéger les données contre les actes malveillants. En cas de faille, les données des personnes dont le visage a été enregistré dans les bases de données pourraient être utilisées à mauvais escient. De plus, les collectivités doivent être en mesure d'identifier les cas où l'algorithme a été trompé. Par exemple, les systèmes de reconnaissance faciale peuvent être trompés par de fausses images, un processus dit spoofing par lequel des criminels utilisent la photo de quelqu'un pour accéder à ses données personnelles.

## PRATIQUES LOCALES

### Ville de Nice (FR)

En 2019, la ville de Nice a décidé de tester la reconnaissance faciale en direct pendant son 135ème carnaval annuel et d'évaluer le bon fonctionnement, ou non, de cette technologie. Les objectifs étaient de contribuer à la sécurisation de l'espace public et de soutenir la recherche scientifique pour promouvoir l'avancement technologique.

Quarante volontaires ont accepté que leur photo soit incluse dans une base de données avec laquelle leur image serait comparée. Portée par l'entreprise monégasque Confidentia, cette expérimentation utilisait le logiciel israélien Anyvision, qui est capable de prendre en compte le vieillissement et donc de reconnaître quelqu'un jusqu'à 20 ans après la date de la photo.

Trois scénarios ont été mis en place lors du carnaval niçois : l'accès contrôlé par l'identification faciale à la porte d'entrée, la détection d'une personne d'intérêt dans la foule, et repérer une personne d'intérêt à son passage à l'entrée. La participation à ce projet pilote était volontaire et les visiteurs pouvaient choisir de se rendre ou non dans les zones sous caméra de surveillance. Quelque 5 000 personnes au total ont participé à l'expérience sur trois jours.

## Police métropolitaine de Londres (UK)[5]

Entre 2016 et 2019, la police métropolitaine de Londres ( Metropolitan Police Service, MPS) a effectué 10 tests de Reconnaissance faciale en direct (Live Facial Recognition, LFR) en fonction de différents scénarios et en utilisant des listes de personnes suspectes différentes, dans toute la ville. Le but de ces essais était « d'évaluer la valeur, la viabilité et les difficultés (y compris les difficultés technologiques, légales, éthiques et de gouvernance) » de la technologie.[6] Le logiciel de reconnaissance faciale a été intégré aux caméras. Celles-ci pouvaient donner l'alerte, à charge pour les agents de police d'évaluer et de juger la situation.

La base de données que la MPS a utilisée comprenait une liste de 2 041 suspects accompagnée de leurs images faciales. Pendant les trois ans qu'a duré l'expérience, la LFR a été utilisée au total pendant 69 heures. Le système a dégagé quelque 180 000 possibilités de reconnaissance (des visages apparus dans les vidéos), et la police a contacté 27 individus et en a arrêté 9 en réponse aux alertes du système.

L'efficacité du système de LFR dépend beaucoup du nombre d'individus enregistrés dans la liste des personnes à surveiller. L'allongement de la liste des personnes à surveiller a semble-t-il contribué à ce qu'un plus grand nombre d'identifications et d'arrestations aient lieu lors de la deuxième phase de l'opération pilote. Comparée à la tactique de « chasse à l'homme » où les délinquants sont repérés grâce au déploiement de policiers en plusieurs endroits pendant une longue période de temps, la LFR nécessite moins de ressources et peut améliorer l'efficacité opérationnelle. En ce qui concerne la localisation des caméras, le système s'est avéré plus efficace dans les zones où les flux de circulation des personnes étaient sous contrôle. Les tests ont montré que le taux de faux positifs était négligeable en ce qui concerne l'origine ethnique, mais qu'il était en revanche important en ce qui concerne le genre. Ainsi, pour les femmes, il y a eu un moindre taux aussi bien de faux positifs que de vrais positifs.

[5] Pour une description détaillée de l'expérience, voir : https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf
[6] Ibid, page 3.

### QUELS DÉFIS POUR LES VILLES?

Au niveau opérationnel, les collectivités peuvent avoir des difficultés à cause de la complexité et de la nouveauté de cette technologie. Sans une formation appropriée, il est difficile de comprendre comment elle fonctionne et comment l'utiliser efficacement. Si l'on ne prend pas en considération l'impact de la reconnaissance faciale sur les droits fondamentaux et donc sur la la légitimité de son usage, cela peut engendrer des situations de discrimination.

Etant donné la complexité de la technologie et le fait qu'elle peut être largement utilisée, il est essentiel de réfléchir aux moyens de protéger les droits et libertés fondamentaux tout en répondant aux besoins de sécurité. Comment préserver l'anonymat dans l'espace public ? Quelles formes de surveillance sont-elles acceptables sans pour autant effrayer le public et renforcer le sentiment d'insécurité ?

## Éléments à prendre en compte lors du développement et de l'utilisation des technologies de reconnaissance faciale

- Mettre en place un cadre législatif et réglementaire clair : Face à la rapidité et à la vitesse auxquelles la technologie de reconnaissance faciale évolue, l'Union européenne souhaite réévaluer les cadres juridiques existants, tels que le RGPD, et promulguer de nouvelles réglementations. Dans son livre blanc sur l'intelligence artificielle, la Commission liste les aspects qu'elle compte revoir : les données sur la formation, l'archivage des dossiers et des données, les informations à fournir, la robustesse et la précision, et le contrôle par des êtres humains. Partager à l'échelle européenne des expériences locales, les problèmes rencontrés et les enseignements à tirer peut contribuer à ce que de nouvelles réglementations répondent aux besoins réels des villes et régions européennes.

- Évaluer l'impact sur les droits fondamentaux : Étant donné que les technologies de reconnaissance faciale ont un impact sur différents droits fondamentaux, il est important de les évaluer aussi bien lors de la phase de développement que pendant l'utilisation.

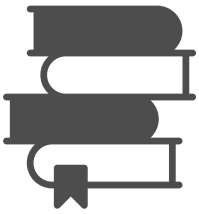
- Évaluer la nécessité et la proportionnalité : Avant d'utiliser la technologie de reconnaissance faciale, la collectivité doit avoir une bonne compréhension de son contexte local de sécurité urbaine, appuyée par des données probantes. Les informations recueillies pendant un diagnostic local de sécurité peuvent contribuer à mieux prendre en compte les principes de nécessité et de proportionnalité afin de trouver le bon équilibre entre les avantages et les risques de la technologie de reconnaissance faciale. Notamment, cela permet d'évaluer quels espaces publics doivent être équipés de cette technologie, pour quelles raisons et pour répondre à quels problèmes.

- Surveiller la mise en oeuvre de la technologie de reconnaissance faciale : Quand la police utilise un logiciel de reconnaissance faciale, il est essentiel que les agents vérifient les résultats, s'assurent qu'ils sont corrects et ensuite décident de l'action à mener. Des organes de contrôle indépendant doivent vérifier le degré de précision et l'efficacité du logiciel.

- Une bonne compréhension de la technologie : Les collectivités ont pour la plupart recours à des technologies qui sont développées à l'extérieur, ce qui rend plus difficile la bonne compréhension du logiciel de reconnaissance faciale et de son fonctionnement. Afin de s'assurer que les droits fondamentaux, tels que le droit à la non-discrimination et à la protection des données, soient intégrés non seulement lors de l'utilisation mais aussi à l'étape de développement, il convient de les prendre en compte dans la formulation des appels d'offre. (FRA, 2019)

- Une formation adaptée pour la police : Certains logiciels, dont la qualité varie, peuvent émettre de nombreuses alertes à la police. Mais le traitement des personnes suspectes dont le visage a été signalé doit répondre aux mêmes principes que pour tout autre suspect. De nouveau, il est important de bien connaître les failles et inexactitudes possibles du logiciel pour comprendre qu'une identification-machine ne veut pas dire pour autant que la personne a été correctement identifiée. Une formation appropriée des agents de police sur la façon de gérer de telles situations peut contribuer à ce que les échanges avec le public demeurent calmes et dignes.

## À LIRE



- En 2019, la Commission Nationale de l'Informatique et des Libertés (CNIL) a publié un rapport sur les éléments techniques, juridiques et éthiques de la reconnaissance faciale qu'elle recommande de prendre en compte.

- En 2019, l'Agence des droits fondamentaux de l'Union européenne (Agency for Fundamental Rights, FRA) a publié un rapport sur les droits fondamentaux à prendre en compte lors de l'utilisation de la technologie de reconnaissance faciale pour le maintien d'ordre.

- La Commission européenne a publié en 2020 un livre blanc intitulé Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance.

CCI
CUTTING CRIME IMPACT

European Forum for Urban Security