Note numéro 18
Avril 2016

# Note du CREOGN

Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale

## Numérisation du visage : opportunités et limites de la reconnaissance faciale

Un article du Figaro du 17 mars 2016[1] relatait l'arrestation en flagrant délit d'un cambrioleur, pris au piège d'un système de reconnaissance faciale. Le propriétaire de l'appartement parisien avait installé un dispositif qui permet de reconnaître les occupants des lieux. Informé en cas de non reconnaissance, le propriétaire avait accès aux images en temps réel et pouvait alerter les forces de sécurité de la présence de l'intrus.

La reconnaissance faciale est le traitement automatique d'images numériques qui contiennent le visage de personnes. C'est une technologie biométrique. Le principe est simple : un capteur « saisit » un visage, le transforme en données numériques pour ensuite le comparer à une base de données, ces deux dernières opérations étant réalisées par un algorithme.

L'utilisation de l'image d'un visage dans la reconnaissance, la comparaison voire l'identification d'individus est d'actualité non seulement dans le domaine de la sécurité, particulièrement sous tension depuis quelques mois, mais également dans la vie quotidienne. L'expression de ce besoin se manifeste d'ailleurs par des applications des téléphones portables ou tablettes. Ainsi, Facebook a développé *Deepface* et *Moments* et Google propose *Name Tag*. La conjonction des besoins de contrôles et des capacités croissantes du numérique dans le domaine de l'imagerie ouvre de nouvelles perspectives en la matière.

Qu'il s'agisse de sécurité publique ou de la vie quotidienne, la thématique est sensible. L'image d'une personne, et plus particulièrement celle du visage, touche en effet à l'intime bien plus peut-être qu'un code barre identifiant un ADN. Sa reproduction, sa détention par un tiers, sa comparaison ne peuvent se faire sans une acceptation de la société. Dès 2012, l'Union européenne formulait des recommandations sur l'emploi de cette technologie[2], notamment en matière de protection des données à caractère personnel. Pour autant, nos modes de vie actuels mettent en lumière un paradoxe : les médias sociaux (Facebook, Twitter, Snapschat, Instagram, LinkedIn, etc.) débordent d'images mises à disposition volontairement et peu ou pas protégées. Le visage est d'ailleurs devenu un enjeu numérique au point que le « *Hype cycle* » de Gartner a identifié la reconnaissance faciale comme une technologie digne d'intérêt.

### I – Le visage, une opportunité dans un monde devenu numérique

Il ne faut pas se leurrer : l'un des premiers usages prometteurs du visage est son utilisation numérique à des fins commerciales. Ainsi, un capteur reconnaît un visage pour le catégoriser afin de déterminer s'il s'agit d'un homme, d'une femme ou d'un enfant. Le but est d'offrir à un client une offre de produits alors qu'il évolue dans un espace commercial. L'entreprise TESCO[3] a déployé dans certaines de ses stations-services du Royaume-Uni le système Amscreen, développé par l'entreprise française Quividi, qui est déclenché dès lors que le client, dans une file d'attente, regarde l'écran dédié à une publicité ciblée. Pour aller plus loin dans l'utilisation du visage **à des fins de *marketing***, il n'a pas échappé à certains la possibilité de constituer une base de données de visages de clients associée à leurs achats habituels afin de les accueillir personnellement dans les meilleures conditions : il s'agit de les orienter vers les produits qu'ils ont l'habitude de consommer ou de leur proposer des produits similaires. Les essais menés montrent cependant que l'utilisation du visage dans ce cadre n'est pas facilement acceptée par le client.

1 http://www.lefigaro.fr/actualite-france/2016/03/17/01016-20160317ARTFIG00095-un-cambrioleur-surpris-en-flagrant-delit-par-une-camera-a-reconnaissance-faciale.php

2 Avis 2012-02 du 22 mars 2012 de l'Union Européenne sur *la reconnaissance faciale dans le cadre des services mobiles et en ligne* , Groupe de travail « article 29 » sur la protection des données.

3 http://www.telegraph.co.uk/technology/news/10435521/Facial-recognition-inevitable-but-will-shoppers-approve.html

Ce n'est pas tant l'utilisation de l'image qui le gêne que sa liberté de déplacement et de choix. Le visage est aussi **un moyen d'authentification fort.** Il pourrait dépasser le fameux code PIN (*Personal Identification Number*). Son utilisation est envisageable pour sécuriser des moyens de paiement ou mieux contrôler les accès à des lieux sécurisés (limitation à des invités). Le système *Ped Cam* (*Pin Entry Device Camera*)[4] de l'entreprise Worldpay illustre ce système encore en expérimentation. En plus du code PIN, le terminal de paiement est équipé d'une caméra qui compare le visage du client avec la photo qui est détenue dans un centre sécurisé. Le système met à jour de façon automatique la photo du client. De même, Master Card a annoncé en juillet 2015 initier le développement d'un nouveau **mode de paiement** en utilisant la photo de l'acheteur que ce dernier transmet par *selfie*. On peut également citer l'exemple de la société Socure qui développe l'outil *Percieve* dont le principe est de sécuriser les paiements par reconnaissance faciale et qui dans le même temps consulte les comptes médias sociaux de ses clients pour plus de sécurité. Amazon travaille aussi sur un projet de paiement sécurisé par reconnaissance faciale. Enfin, on peut imaginer l'utilisation de capteurs vidéo pour autoriser après reconnaissance faciale l'accès d'une personne à un véhicule pour le conduire[5].

Ces systèmes sont peu attentatoires à la vie privée, on parle de biométrie douce. Le point critique est la protection des bases et les flux de données à caractère personnel. En fait, dans la plupart des cas, les données sont traitées directement avec l'appareil. Dans les autres cas, la consultation est réalisée dans un *cloud*, les données sont transformées en algorithme qui est lui-même crypté. D'un point de vue acceptabilité, peu de voix s'élèvent contre ces systèmes de reconnaissance que l'on peut croiser au quotidien.

## II – Le visage numérisé, une technologie qu'éprouve et développe la sécurité.

En matière de sécurité, le visage numérisé est une opportunité très forte pour travailler sur la recherche et l'identification de personnes. Le contexte de la sécurité s'inscrit dans le mouvement d'accélération qu'impose le numérique. Les usages relèvent soit d'une **phase d'anticipation** ou de préparation d'événements, soit d'une **phase d'investigation.** Dans cette dernière, il s'agit de **comparer** l'image captée avec une base de données pour repérer une personne qui fait l'objet d'un intérêt particulier parce que mise en cause, victime ou témoin. Dans une phase préventive et en temps réel, le but est de révéler un indicateur, que l'on pourra appeler signal faible, prenant la forme de comportements anormaux afin **de préparer la survenue d'un trouble ou désordre** qui nécessite une réaction.

**La reconnaissance faciale est déjà utilisée par certaines forces de sécurité**. Lors des opérations menées en Afghanistan, les forces américaines ont déployé les outils (*Handheld Interagency Identity Detection Equipment*) indispensables à la création de bases de données biométriques, incluant le visage, aux fins de comparaison et d'identification. Au **Canada**, la police de Calgary était la première force de police à faire usage de cette technologie. **Aux États-Unis**, le Federal Bureau of Investigation dispose de l'outil *Next Generation Identification Program*[6] qui utilise les fichiers nationaux et les médias sociaux pour construire une base de données de plus de 52 millions de personnes. Les polices de Chicago, New York, Seattle, San Diego ou Dayton Beach ont investi dans ces moyens techniques proposés par Neoface ou Reveal de Nec pour des montants allant jusqu'à 5,4 millions de $. La police d'Hawaï[7] a mis en œuvre *Morphoface Investigate* qui contient près de 450 000 visages. Intégrée dans des programmes de sécurité qui visent principalement à lutter contre le phénomène des gangs, la reconnaissance faciale devient un outil d'une stratégie de sécurité. Fin 2015 et pour un budget de 18,5 millions de $, le **gouvernement australien** a lancé le programme *Capability* pour lutter contre le terrorisme et la délinquance transfrontalière en s'appuyant au moins sur les fichiers nationaux. Après avoir fait l'objet de nombreux débats, ce programme devrait être opérationnel au cours de l'année 2016. Les **forces de police judiciaire allemandes**, quant à elles, utilisent depuis 2007 l'application de reconnaissance faciale *Face-VACS/DB Scan* de l'entreprise Cognitec.

4 http://www.dailymail.co.uk/sciencetech/article-3254831/Combatting-fraud-FACE-Shops-soon-use-facial-recognition-pay-check-card-hasn-t-stolen.html

5 http://www.numerama.com/magazine/32613-safran-veut-mettre-sa-reconnaissance-faciale-dans-les-voitures.html

6 https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/initiatives/next-generation-identification-program

7 http://in.reuters.com/article/idUSnMKWB6rZ4a+1e4+MKW20150128

**En Inde**, la ville de Surat a combiné l'application NeoFace Reveal de Nec avec son système de vidéo-surveillance pour procéder en temps réel à la reconnaissance faciale. Dans le même but, la ville de **Buenos Aires** a modernisé ses moyens de vidéo-surveillance pour améliorer l'éclairage des rues afin d'obtenir une qualité d'image supérieure et faciliter ainsi le travail de reconnaissance faciale. Dans certains aéroports européens (**Belgique**[8] et Allemagne), des systèmes de reconnaissance faciale ont été mis en place. Dans le sas du dispositif appelé *e-gate*, un capteur prend une photo du voyageur qui est comparée aux documents d'identité. Aéroports de Paris a testé fin de 2015 un autre système. Il s'agissait de s'assurer que la personne qui entrait dans le sas était la même qui en sortait, en comparant deux photos saisies par deux capteurs dans et après le sas sans qu'il y ait la mise en place ou la consultation d'une base de données.

**Le monde de la recherche est très investi dans la reconnaissance faciale.** Ainsi, le **projet européen** Secur-ed (*SECured URban transportation-European Demonstration*)[9] aborde la reconnaissance faciale au même titre que la détection d'intrusion, la surveillance de foule ou le suivi de personnes dans les transports collectifs. Des chercheurs de l'université de **Hong-Kong** proposent des solutions pour pallier les contraintes de prises de vue[10]. Des projets comme Methodeo (Méthodologie d'évaluation des algorithmes d'exploitation des enregistrements de la vidéoprotection) de Thales ou Physionomie (Rapprochement physionomique à des fins d'investigation) de Morpho se concentrent sur l'exploitation des images de visages et sur les qualités des algorithmes d'exploitation des données dans la phase judiciaire. En **Allemagne**, le projet GES-3D (*Multi-Biometrische Gesichtserkennung*)[11] souligne l'intérêt de cette technologie en abordant la notion de 3ème dimension pour la reconnaissance faciale. On peut également citer une application comme LISA (Logiciel d'Identification de Suspects par Analogie) de l'entreprise Spikenet Technology qui identifie des caractéristiques propres à des individus (parties du visage ou du corps). Avec l'appui de l'entreprise Morpho, **Interpol s'implique dans la reconnaissance faciale**[12] et l'intègre désormais dans ses domaines d'expertise forensique. En 2015, cette agence créait un groupe de travail (*Facial Expert Working Group*) avec pour objectif de déterminer des normes de qualité, de format et de transmission des images pour alimenter une base de données dès 2016 et d'être en capacité de l'exploiter en temps réel sur le terrain lors d'opérations.

## III- Le visage numérisé : quelles limites pour la sécurité ?

Les différentes expériences et les outils développés ne doivent pas cacher certaines contraintes. La première de celles-ci est la qualité des images. Les différentes conditions de prise de vue, les performances des capteurs et l'absence de normes rendent compliquée l'exploitation des images. Le taux d'erreur des applications peut atteindre 20 %. Par ailleurs, **cette technologie n'est pas nécessairement acceptée par la société**. Ainsi, la police de Boston a mis un terme à l'utilisation de ce procédé à l'instar de celle d'Oakland du fait de réactions citoyennes vives. La mise en place de la reconnaissance faciale s'était faite sans information du public. D'autres cas, comme celui de la police de San Diego, mettent en évidence un déploiement du dispositif à marche forcée. Les policiers, sans contrôle, numérisent d'office le visage de toute personne contrôlée dans la rue pour constituer la base de données. **Au Royaume-Uni**, ce sont des unités de police qui, sans cadre juridique stabilisé, ont alimenté une base de données *(Police National Database*) de photos de milliers d'individus prises lors des opérations anthropométriques de garde à vue. L'autorité administrative indépendante britannique en charge des questions de biométrie relevait la problématique des outils et applications qui n'avaient fait l'objet d'aucun test de fiabilité et d'efficacité. La technologie de la reconnaissance faciale n'est peut être pas la panacée et ne peut se développer sans préparation et acceptation de la société. Les tentatives de mise en place sans information du public sont en effet vouées à l'échec. **Le citoyen reste attaché à sa vie privée** et au droit à l'anonymat quand bien même la menace est forte.

8 http://www.air-journal.fr/2015-07-12-brussels-airport-controle-aux-frontieres-avec-reconnaissance-faciale-et-forte-croissance-au-s1-5147154.html

9 http://www.secur-ed.eu/

10 http://www.cv-foundation.org/openaccess/content_iccv_2013/papers/Lu_Face_Recognition_Using_2013_ICCV_paper.pdf

11 https://www.igd.fraunhofer.de/Institut/Abteilungen/IDB/Projekte/Multi-Biometrische-Gesichtserkennung-GES-3D

12 http://www.interpol.int/fr/INTERPOL-expertise/Forensics/Facial-recognition

Depuis toujours les enquêteurs des forces de sécurité n'ont de cesse, quand ils sont à la recherche d'individus, de solliciter leur mémoire, celles de leurs pairs ou de citoyens par voie d'affichage, afin d'identifier ou de reconnaître des visages. Certains agents sont d'ailleurs dédiés au travail de reconnaissance d'individus notamment à l'occasion de rencontres sportives pour repérer les hooligans. Ce procédé est mis en valeur dans certaines unités de police britanniques. Ainsi en est-il des « *super recognizers* »[13], policiers qui ont le don de mémoriser les visages au point de les repérer et de les identifier dans une foule avec une efficacité supérieure à une application de reconnaissance faciale.

Il existe aussi d'autres limites à la reconnaissance faciale. Ainsi, la société AVG a expérimenté des lunettes, qui par l'utilisation d'ampoules led infra-rouge ou de matériau rétro-réfléchissant, atténuent considérablement la qualité de l'image captée et rendent donc inopérante la technologie[14]. Par ailleurs, dans la construction des algorithmes de comparaison, **certains biais structurels ont été mis en évidence** notamment sur l'identification de la couleur de peau ou la forme des yeux, ce qui en fait une outil potentiellement discriminatoire. La crainte de cette technologie repose aussi sur la fiabilité des lieux de stockage des documents numérisés ainsi que des conditions d'accès. On peut remplacer un code PIN ou un numéro de carte que l'on vous vole mais, à l'instar de l'usurpation d'identité, on imagine aisément la force du préjudice d'un détournement du visage numérisé. **La protection des systèmes de reconnaissance faciale est donc un enjeu majeur** du déploiement de cette technologie, et rejoint les enjeux de cybersécurité. Enfin, l'une des contraintes de cette technologie réside dans les mises à jour des photos qui pourraient se traduire par des sollicitations plus fréquentes des administrations.

Le cadre juridique est aussi et heureusement une limite. A l'échelle européenne la directive 95/46/CE sur **la protection des données s'applique aux systèmes de reconnaissance faciale**. Elle s'impose à la France où les risques d'atteinte à la vie privée et à la protection des données à caractère personnel sont de véritables enjeux de société. La technologie évolue et doit ouvrir sur des solutions juridiques qui satisfassent l'ensemble des parties prenantes (État, société, forces de sécurité). Les forces de sécurité intérieure françaises ont déjà la possibilité juridique de procéder à un processus de reconnaissance faciale (article 40-26 du code de procédure pénale pour les mis en cause, les victimes décédées ou les personnes disparues) à partir de l'application de Traitement des Antécédents Judiciaires. Considérant le haut niveau de la menace terroriste, la modernisation et la prise en compte de cette technologie pourraient intéresser les forces de sécurité intérieure pour compléter l'arsenal des techniques de renseignement actées par la loi 2015-912 du 24 juillet 2015 relative au renseignement.

La reconnaissance faciale est donc une technologie qui a atteint une certaine maturité au point d'en faire un outil non seulement de la vie quotidienne mais également une solution parmi d'autres pour améliorer la sécurité. L'enjeu est celui des normes techniques qui garantissent un niveau de qualité et d'exploitation large. C'est aussi un enjeu économique pour le développement des produits et leur exploitation. Mais l'enjeu porte surtout sur l'évolution de la norme juridique. Elle doit garantir le juste équilibre entre liberté et sécurité dans un cadre transfrontalier. Cette norme doit également anticiper les avancées de la technologie vers le « big data », l'Internet des objets voire l'intelligence artificielle. Le déploiement de cette technologie pose des questions d'éthique et de sécurité qu'il faut considérer au-delà de nos frontières. Kelly Gates, de l'université de Californie, mettait en garde dès 2011 contre les risques de cette technologie[15]. Pour autant, en matière de sécurité, la reconnaissance faciale, que ce soit dans une phase préventive ou d'enquête, reste un des éléments du faisceau d'indicateurs ou d'indices utiles à la décision. A « l'image » des *super-recognizer*, la reconnaissance faciale ne peut se passer de l'action humaine qui, seule, porte le poids de la responsabilité du choix d'intervenir ou non.

13 http://www.bbc.com/news/uk-england-34544199
14 http://www.semageek.com/une-casquette-pour-devenir-invisible-de-big-brother/
15 Kelly Gates, 2011*, Our Biometric Future, facial recognition technology and the culture of surveillance*, Paperback editions