NOTE DU CREOGN

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

Numéro 43 – Septembre 2019

Colonel Dominique SCHOENHER

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

@scharfsinn86 pour AdobeStock

RECONNAISSANCE FACIALE ET CONTRÔLES PRÉVENTIFS SUR LA VOIE PUBLIQUE, L'ENJEU DE L'ACCEPTABILITÉ

Le CREOGN avait déjà abordé cette question début 2016[1], une éternité en temps technologique. Les solutions techniques présentaient alors un taux de fiabilité très discutable et les usages grand public restaient marginaux.
Aujourd'hui, la technologie de reconnaissance faciale s'est banalisée dans les usages commerciaux et elle gagne chaque jour en maturité dans la fonction « sécurité publique ». Elle est déjà déployée et ouvertement assumée en tant que moyen de surveillance à l'échelle d'un pays aussi vaste que la Chine. Toutefois, comme tout emploi d'une technologie dans une optique sécuritaire, les polémiques prospèrent quant à ses dérives potentielles, son efficacité réelle et son degré d'atteintes aux libertés individuelles. En effet, si la population française consent à recourir à la reconnaissance faciale dans son quotidien de consommateur, pratique contribuant à la désensibiliser selon certains sociologues[2], elle n'est pas prête à en accepter l'exploitation par les forces de l'ordre à n'importe quelle condition. La société française, traumatisée par le Régime de Vichy et son système d'enregistrement d'identité, conserve dans son ADN collectif des marqueurs de rejet du fichage étatique. Par ailleurs, il faut reconnaître que le visage n'est pas une donnée biométrique comme les autres. Au cœur de nos interactions sociales, c'est notre carte de visite permanente dans le monde physique[3], le moyen essentiel de l'expression de nos émotions, bien plus sincère que le langage.
Afin de dépasser les postures purement idéologiques, le recours à la reconnaissance faciale par les forces de l'ordre mérite de relever d'un choix de société éclairé s'appuyant sur des garanties techniques et sur un droit consolidé permettant l'expérimentation scientifique.

I) Du Graal policier à la dystopie, un choix politique et sociétal

Si tant est qu'elle atteigne un niveau de fiabilité acceptable, la plus-value policière de cette technologie ne fait aucun doute. Elle vient consacrer la démarche d'anthropométrie judiciaire entamée il y a 150 ans pour identifier les fauteurs de troubles qui, auparavant, étaient marqués au fer rouge pour les plus dangereux. L'intérêt de cette technologie est d'exécuter systématiquement et automatiquement les actes de base des forces de l'ordre que sont l'identification, le suivi et la recherche d'individus en rendant ce contrôle invisible. Sous réserve d'algorithmes exempts de biais, elle pourrait mettre fin à des années de polémiques sur le contrôle au faciès puisque le contrôle

1 Note n° 18 du CREOGN, avril 2016. https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Numerisation-du-visage-opportunites-et-limites-de-la-reconnaissance-faciale

2 Asma Mhalla (Maître de conférences à Sciences Po) : « Nous manquons de réflexion éthique sur l'IA et la reconnaissance faciale », « L'empire du signal, ou les dangers d'un contrôle social par les corps ».

3 Selon les pratiques, ce constat peut être étendu au monde virtuel (mode des selfies, tag de reconnaissance des personnes sur les photos et même émoticônes) mais certains préfèrent y adopter d'autres visages (avatars).

d'identité serait permanent et général[4]. De même, elle permettrait une réactivité accrue pour les recherches de personnes vulnérables ou la traque de délinquants en fuite. Elle serait également de nature à instaurer un auto-contrôle limitant les incivilités (respect du code de la route, déjections animales, dépôts d'ordure) sur le modèle du crédit social chinois[5].

Autant de promesses d'efficience qui ne doivent pas masquer les potentielles dérives totalitaires au sein d'un État qui voudrait l'exploiter pour assurer un contrôle social permanent sur sa population et une répression à l'encontre des individus ou groupes de population qu'il jugerait dissidents. L'histoire nous a montré qu'aucun pays n'est à l'abri d'une dérive autoritaire. Quand bien même la France le serait-elle, un autre danger pourrait venir de l'espionnage constant exercé par une puissance étrangère si la technologie n'était pas maîtrisée dans tous ses composants[6]. Ce potentiel néfaste, renforcé par la convergence des technologies et la multiplication des objets connectés dans notre environnement comme autant de sources de nouveaux flux vidéos pouvant alimenter les systèmes de reconnaissance faciale, va rendre caduque la notion d'anonymat dans l'espace public. Faute de régulation, la prédiction du prospectiviste américain Howard Rheingold se réalisera[7].

La reconnaissance faciale ne peut être « désinventée », elle a déjà prospéré dans les usages privés et commerciaux. Toutefois, les retentissantes interdictions d'emploi par les municipalités de San Francisco, Somerville et Oakland aux États-Unis, envisagées par certains États comme la Californie et que souhaiterait étendre à l'échelle fédérale le candidat à la présidentielle Bernie Sanders, ont eu le mérite d'animer le débat[8].
Or, ce débat ne peut se construire actuellement en France, la population et ses représentants n'étant que trop insuffisamment informés des enjeux de la reconnaissance faciale. Même si les articles de presse, généralement manichéens, se multiplient, il existe peu d'études ou de sondages français sur l'acceptabilité des technologies biométriques. Une étude du centre de recherche pour l'étude et l'observation des conditions de vie de 2013 montrait une validation des usages à des fins sécuritaires mais rejetait les usages commerciaux (une situation totalement inversée dans la réalité actuelle) et érigeait le consentement individuel préalable en condition *sine qua non*. Un sondage IPSOS de la même année mentionnait que 72 % des sondés étaient favorables à la vidéoprotection assortie de reconnaissance faciale (65 % chez les 15-24 ans). Un sondage ODOXA de juin 2017 faisait monter ce taux à 85 % pour la détection de fichés S lors de grands événements[9].
Bien que rares, ces sondages convergent sur trois points. Les jeunes et les minorités se sentent intuitivement plus menacés par les déviances de la reconnaissance faciale. Celle-ci ne reçoit un soutien massif que lorsqu'elle vise à réduire un risque grave et bien défini dans le temps et l'espace. Le consentement préalable du citoyen, et pas seulement son information, apparaît comme une condition à son usage légitime et légal[10] sur la voie publique.

Au-delà de ces constats statistiques, quels seraient les facteurs de nature à entraîner l'adhésion de la population française et à la convaincre de l'innocuité d'un tel outil dans les mains de l'État ?

4 Sous réserve de changement de la jurisprudence du Conseil constitutionnel qui établit que « la pratique de contrôles d'identité généralisés et discrétionnaires serait incompatible avec le respect de la liberté individuelle », décision n° 93-323 DC du 5 août 1993.

5 La Chine a mis en place un système de notation du comportement de sa population aboutissant à des mesures stigmatisantes (restrictions du droit de voyager ou d'obtenir un crédit) pour près de 23 millions d'individus jugés à faible crédit social.

6 Les débats autour des équipements HUAWEI pour le déploiement de la 5G en donnent une illustration, il en serait de même pour les algorithmes mis en œuvre.

7 Observant les effets politiques, sociaux et économiques des technologies émergentes, il concluait en 2005 « la vie privée telle qu'on la définit n'existera plus ».

8 Le *National Institute of Standards and Technology* alimente les décideurs en rapports réguliers sur les performances des algorithmes d'identification. Les policiers américains accédant à une base photographique couvrant la majorité de la population, le potentiel de la reconnaissance faciale y est davantage ressenti.

9 Un sondage anglais datant de mai 2019 sur les expérimentations de la police de Londres indiquait qu'à peine 57 % étaient en faveur de l'usage de la reconnaissance faciale de voie publique. Ce pourcentage montait à 83 lorsque la finalité était la recherche de criminels *(serious offenders).* L'acceptabilité des jeunes et des minorités reste là aussi inférieure à la moyenne de la population sondée.

10 Ce principe, conforme à la réglementation européenne (règlement général sur la protection des données), a été respecté lors de l'expérimentation au Carnaval de Nice en février 2019. Au Royaume-Uni, plusieurs procès contre la police sont en cours en raison de l'absence de consentement explicite des passants soumis au dispositif de reconnaissance.

II) Le pré-requis : une technologie fiable et sûre

La fiabilité est la première source de confiance dans la technologie. Le cas de la voiture autonome nous montre que le seuil d'acceptation social de l'erreur est très faible pour les processus animés par l'intelligence artificielle[11], a fortiori pour ceux ayant des implications sur les libertés individuelles.
Le taux d'erreur doit être garanti à un niveau acceptable, quelles que soient les conditions d'emploi (luminosité changeante, en mouvement...)[12]. La qualité du logiciel de reconnaissance faciale repose sur son algorithme et la manière dont il a été « entraîné ». L'analyse des résultats des systèmes actuels a montré que le taux d'erreur était systématiquement plus important pour les personnes de couleur et pour la gent féminine parce que les hommes blancs étaient surreprésentés dans l'échantillon d'apprentissage[13]. Le fonctionnement de l'algorithme doit donc être transparent et les conditions de son apprentissage scrupuleusement contrôlées avec une base de référence répondant à des critères qualitatifs vérifiables.

S'il existe peu de données sur les faux négatifs (non-détection d'une cible), le taux de faux positifs (détection d'une cible qui n'en est pas une) fait l'objet de controverses pour les mêmes essais. Ainsi, pour ses expérimentations en 2019, la police de Londres le mesure à moins de 1/1000 (une erreur pour 1 000 visages scannés) et les chercheurs le fixent à plus de 80 % (pourcentage des personnes arrêtées à tort suite à une détection par le système)[14].
Enfin, pour que le dispositif soit pertinent, son efficacité doit se maintenir même en cas de tentative de dissimuler son visage (casquette, lunette, masque, postiche, foulard, parapluie). Dans le cas contraire, la cible utilisera ces contre-mesures pour leurrer le système comme lors des manifestations à Hong-Kong. Se posera alors la question d'interdire et de verbaliser la dissimulation du visage sur la voie publique, ce qui se révèle difficilement applicable.

Le système d'information doit être protégé dans son fonctionnement contre les menaces internes, comme c'est le cas pour tous les traitements de données policiers, en imposant une traçabilité permanente des actions des opérateurs afin d'éviter les mésusages et les détournements de finalité.
Au regard des menaces externes, il constitue une cible de choix pour les hackers aux motivations libertaires ou plus bassement matérielles mais aussi pour les services de renseignement d'un État tiers à des fins d'espionnage. Son architecture et son infrastructure doivent être non seulement parfaitement sécurisées mais aussi résilientes. La surveillance des paramètres de fonctionnement doit être constante pour détecter toute anomalie résultant d'un piratage. L'avantage en la matière reste à l'attaquant.
Les données biométriques étant par essence sensibles, il faut en assurer la protection contre le vol, en garantir l'intégrité contre les modifications ou destructions ainsi que la disponibilité en temps utile pour le bon fonctionnement du système.

Ce pré-requis ne peut être atteint que dans un environnement juridique consolidé, qu'il s'agisse de l'expérimentation ou de la mise en œuvre opérationnelle sur la voie publique.

III) La nécessité : un cadre juridique consolidé avec un contrôle éthique et scientifique

La Commission nationale de l'informatique et des libertés (CNIL) est régulièrement sollicitée pour arbitrer la légitimité des usages de cette technologie. Sur le fondement du Règlement général sur la protection des données (RGPD) et de la directive européenne « police-justice »[15], elle étudie au cas par cas les causes d'exception à l'interdiction de principe de traitement des données biométriques[16].

11 Ce phénomène est également amplifié par la surmédiatisation de ces accidents présentant le double attrait du fait divers et de la nouveauté technologique.
12 En conditions parfaitement contrôlées (dispositif PARAFE en zone aéroportuaire), il est inférieur à 0,5 %.
13 http://www.lefigaro.fr/secteur/high-tech/amazon-somme-de-ne-plus-vendre-sa-technologie-de-reconnaissance-faciale-a-la-police-20190404
14 https://information.tv5monde.com/info/reconnaissance-faciale-nouvelles-polemiques-apres-l-echec-cuisant-de-la-police-de-londres
15 Directive n° 2016/680 du 27 avril 2016.
16 Le 17 juillet 2019, la Quadrature du Net a annoncé avoir déposé un recours auprès du Conseil d'État pour faire annuler le décret autorisant la création de l'application « Alicem » (Authentification en ligne certifiée sur mobile). S'appuyant sur l'avis rendu par la CNIL, l'association dénonce le recours forcé à la reconnaissance faciale dans le processus de cette application. Elle juge cette approche non conforme au principe de consentement libre prévu par le RGPD et considère qu'elle contribue à la banalisation de cette

Consciente de la multiplication des cas d'usage, elle en appelle depuis septembre 2018 « à la tenue d'un débat démocratique...[et] demande au Législateur de se saisir de ces questions »[17]. Elle a été rejointe sur ce point par le ministre de l'Intérieur le 21 juin 2019[18] et les parlementaires au cours de l'été[19]. Le travail législatif pourrait utilement être précédé d'une réflexion collégiale et scientifique servant d'orientation au débat public, à l'exemple de ce qui se fait en bioéthique[20]. Le respect du principe de stricte proportionnalité établi de longue date en droit administratif concernant les atteintes aux libertés individuelles (vie privée, anonymat, liberté de mouvement…) constituera le fondement de cette réflexion.

Au plan international, la vacuité du cadre juridique autour de cette technologie est semblable, avec des degrés de contentieux différents selon l'attachement des populations à leurs libertés individuelles. Il est ainsi à noter que le Royaume-Uni, pays européen en pointe dans le déploiement de la reconnaissance faciale, est confronté à plusieurs procès contestant la base légale de son usage sur la voie publique.
Dans l'optique d'une consolidation du marché des technologies de sécurité, les entreprises du secteur sont elles-mêmes en demande de régulation et parfois prennent des initiatives infra-réglementaires. *Microsoft* et *Google* ont décidé de respecter des principes de responsabilité dans le développement des technologies à base d'intelligence artificielle (IA) et suggèrent à leurs concurrents de faire de même[21].

Il ne faut toutefois pas que la peur ou le principe de précaution empêchent l'expérimentation qui seule permet de se rendre compte des biais mais aussi des apports d'une innovation. Sous réserve de la mise en place d'un pilotage stratégique évitant la dispersion des initiatives, elle conditionnera l'élaboration d'une régulation équilibrée. En toute transparence, ces tests en situation réelle doivent être évalués scientifiquement et leurs résultats publiquement partagés[22]. Dans un cadre juridique suffisamment souple, ils permettraient aux industriels français de développer des solutions souveraines et sans doute d'autres approches basées également sur la vidéoprotection mais ressenties comme moins intrusives. Ainsi, la société chinoise WATRIX expérimente un logiciel de reconnaissance de la démarche qui permettrait d'identifier une personne de dos ou dissimulant son visage[23]. La caution scientifique, le contrôle vigilant du juge et de l'autorité administrative indépendante sont autant d'éléments clefs pour rassurer la population. Si, par ailleurs, elle y perçoit un gain objectif en sécurité et surtout une réduction de contraintes[24] (la fameuse expérience usager améliorée), la technologie sera acceptée.

Pour conclure, on ne peut que constater que les systèmes politiques, juridiques et sociaux ne sont pas prêts pour gérer cette technologie comme toutes celles résultant des NBIC[25]. La reconnaissance faciale en tant qu'outil d'administration des populations s'inscrit nécessairement dans un projet politique. Au sein d'une démocratie, il est impératif que le débat public en fixe les limites fonctionnelles, les cas d'usage acceptables, au regard des dérives possibles et pas seulement des bénéfices attendus. La recherche ne doit donc pas se limiter à l'aspect technique mais se densifier dans les domaines de la sociologie et de l'éthique dans le but d'en fixer les limites d'usage et d'en faciliter l'acceptation. « Il faut remettre la science au cœur de la décision publique »[26].

technologie.

17 https://www.cnil.fr/fr/la-cnil-appelle-la-tenue-dun-debat-democratique-sur-les-nouveaux-usages-des-cameras-video

18 http://www.lefigaro.fr/flash-actu/videosurveillance-castaner-veut-un-debat-sur-la-reconnaissance-faciale-20190621

19 Note n°14 de l'office parlementaire d'évaluation des choix scientifiques et technologiques.

20 Une initiative en ce sens a été lancée en juin par le Conseil national du numérique.

21 https://www.actualitesdudroit.fr/browse/affaires/immateriel/18182/reconnaissance-faciale-microsoft-devoile-six-principes-et-appelle-a-legiferer

22 Le rapport d'expérimentation très positif rédigé par la municipalité de Nice concernant le Carnaval 2019 ne présente pas les qualités « scientifiques » ni « la précision technique » attendues par la CNIL.

23 KANG, Dake, « Chinese 'gait recognition' tech IDs people by how they walk », *associated Press* sur : https://apnews.com/bf75dd1c26c947b7826d270a16e2658a

24 Comme ce fut le cas pour la coupe du monde de football en Russie avec Fan ID (visa gratuit, accès rapide au match et aux transports publics). La coupe du monde de rugby en 2023 et les JO de Paris en 2024 représentent des opportunités remarquables de convaincre la population de l'intérêt de déployer la reconnaissance faciale.

25 Nanotechnologies, Biotechnologies, Informatique et Cognotechnologies (intelligence artificielle).

26 Déclaration du 2 septembre 2019 de la ministre de l'Enseignement supérieur, de la recherche et de l'innovation.