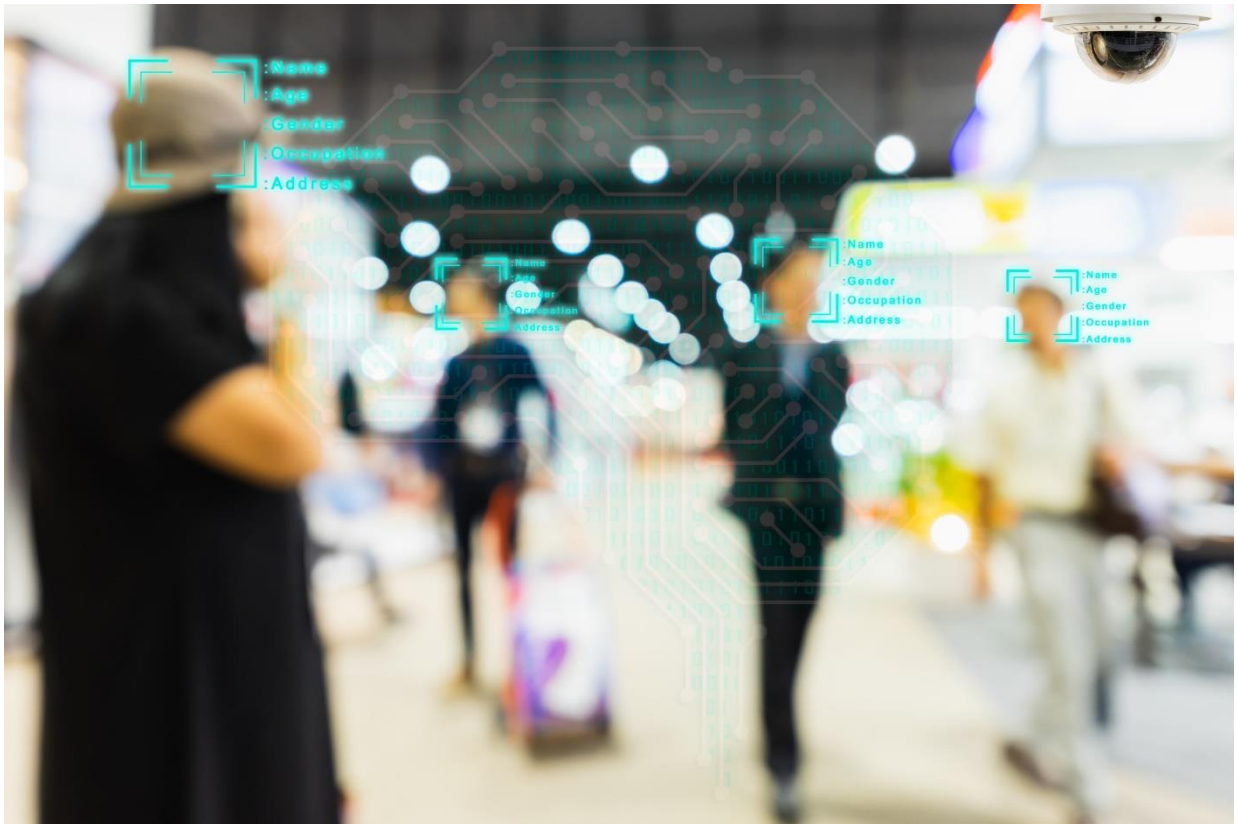
Reconnaissance faciale : entre exigence de contrôle et respect de la vie privée

Quels outils, quels enjeux, quelles garanties ?



Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ)

30ème session nationale « Sécurité et Justice » 2018 - 2019

Groupe de diagnostic stratégique (GDS) n°8

Les membres du GDS 8 remercient sincèrement l'ensemble des personnes rencontrées dans le cadre de l'élaboration du rapport, pour le temps nous ayant été accordé, et la richesse des échanges.

Membres du Groupe de diagnostic stratégique n°8

Présidente : **Sharone FRANCO,** *Avocat au Barreau de Paris*
Vice-Présidente : **Florence FOURETS,** *Directrice chargée de Projets Régaliens, CNIL*

Bernard BONNET, *International Travel Security Manager, Direction Sûreté, AIRBUS*
Lionel DARASSE, *Chargé d'affaire protection physique, Direction qualité sécurité contrôle gouvernemental, CEA*
Joseph DUPRE LA TOUR, *Colonel, Chef d'état-major de la brigade de sapeurs-pompiers de Paris*
Christian LARROQUE, *Ingénieur hors classe, Chef du bureau Armées, SIMMT*
Thierry MANCIOT, *Head of cybersecurity industrial, SANOFI – AVENTIS GROUP*
Catherine MARTEL, *Ingénieur en chef de PTS, Chef de division chimie, INPS/LPS59*
Robert PELLEGRIN, *Capitaine de vaisseau, Chef du bureau « sécurité-protection » de l'état-major de la Marine*
Loïc POUCEL, *Délégué à l'accueil et à la sécurité des personnes et des biens, Radio France*
Philippe RAULT, *Directeur adjoint de la protection des populations de Seine-Saint-Denis*

Sommaire

Introduction

L'état-civil pouvant facilement être falsifié, le recours à des techniques permettant de certifier l'identité d'une personne de manière irréfragable est ancien. Ainsi, la photographie, véritable système de reconnaissance d'une personne à partir de ses caractéristiques physiques, a été largement diffusée et très vite utilisée pour limiter les risques d'usurpation d'identité. Sous l'influence d'Alphonse Bertillon, les fichiers de police et l'identification de potentiels auteurs d'infractions sont aujourd'hui souvent fondés sur des mesures corporelles, allant du signalement anthropométrique à l'enregistrement de données biométriques dans des fichiers tels que le FAED (fichier automatisé des empreintes digitales) ou le FNAEG (fichier national automatisé des empreintes génétiques). L'usage de ces bases de données dans le cadre d'une enquête vise ainsi à confondre un coupable, indépendamment de son identité déclarée.

On observera par ailleurs que la protection de la vie privée et le corpus de règles y afférent ont été conceptualisés et adoptés au niveau national, européen et international[1], très souvent en réaction aux progrès techniques. La vie privée suppose toutefois l'existence d'une sphère privée garantie par l'Etat. Si tel est le cas par exemple pour les domiciles des personnes, à l'exception de circonstances, expressément prévues par le législateur qui peuvent nécessiter leur mise sous surveillance[2], cela peut paraître de moins en moins vrai pour le domaine public, avec le développement considérable de la vidéoprotection[3]. Utilisé pour la première fois durant la seconde guerre mondiale à des fins de sûreté, l'objectif général de cette visualisation à distance d'un espace géographique est aujourd'hui, plus largement, dans le domaine civil, de contribuer à la sécurité des biens et des personnes. L'enregistrement permanent de l'image de visages auquel cette technologie conduit permet de localiser en temps réel les personnes, et de tracer leurs déplacements. L'ajout d'un dispositif de reconnaissance faciale, identifiant ces mêmes personnes dès lors que des données biométriques peuvent être comparées à celles déjà enregistrées dans des fichiers, participe, selon d'aucuns, à l'instauration d'une société de surveillance ; ce d'autant que la loi du 11 octobre 2010 interdit la dissimulation du visage dans l'espace public, et qu'aux termes de la loi du 10 avril 2019, il s'agit désormais d'un délit[4]. La crainte de ne pouvoir y échapper est souvent renforcée par la mise

[1] Cf. art. 9 du code civil, aux termes duquel chacun a droit au respect de sa vie privée ; art. 8 de la Convention européenne des droits de l'homme (CEDH), qui, s'inspirant de la Déclaration universelle des droits de l'Homme, proclame le droit de toute personne au respect de sa vie privée, mais organise un régime de restrictions si celles-ci sont « prévues par la loi » et constituent une mesure qui, dans une société démocratique, est notamment nécessaire à la sécurité nationale, à la sûreté publique, à la défense de l'ordre et à la prévention des infractions pénales ; art. 7 de la Charte des droits fondamentaux selon lequel toute personne a droit au respect de sa vie privée.

[2] Cf. par ex. la loi du 24 juillet 2015 relative au renseignement, qui encadre les techniques de captation d'images ou de paroles au sein de lieux privés.

[3] Le terme de vidéoprotection a été substitué à celui de vidéosurveillance aux termes de la loi *"d'orientation et de programmation pour la performance de la sécurité intérieure"* (LOPPSI II) du 14 mars 2011.

[4] Cf. art. 431-9-1 « Est puni d'un an d'emprisonnement et de 15 000 € d'amende le fait pour une personne, au sein ou aux abords immédiats d'une manifestation sur la voie publique, au cours ou à l'issue de laquelle des troubles

en œuvre de technologies, telles que l'intelligence artificielle (IA), parfaitement opaques pour la plupart d'entre nous, et le fait qu'elles puissent être opérationnelles à notre insu.

Pour autant, force est de constater que la démocratisation de ces dispositifs technologiques, en particulier dans le secteur commercial, en raison de leurs coûts de moins en moins élevés et de l'appropriation qui a pu en être faite par certains d'entre nous compte tenu de leur facilité d'utilisation et du gain de temps qu'ils procurent (par exemple pour accéder à son smartphone ou ouvrir un compte bancaire en ligne), contribue à leur intégration dans une société numérique. Mais ces cas d'usage restent à la main des personnes qui en font le choix.

Qu'en est-il de l'implantation de dispositifs de reconnaissance faciale à des fins de sécurisation de sites ou établissements sensibles, ou de la voie publique dans son ensemble, auxquels ne pourraient se soustraire les personnes souhaitant y accéder ?

Souhaite-t-on vivre dans une société où son visage est constamment filmé pour être comparé à ceux figurant dans des fichiers de police, quel que soit le motif de cet enregistrement ? Si l'anonymat est considéré par certains comme une condition nécessaire de la liberté d'aller et venir, consacrée en tant que liberté fondamentale tant par la Cour de cassation que par le Conseil d'Etat, et de la préservation de la vie privée, sommes-nous prêts à accepter de cesser d'être anonymes dans l'espace public, au moins dans certaines circonstances, et faire ainsi prévaloir la sécurité sur la vie privée ? Sommes-nous prêts à souscrire à la mise en place d'un « Big Brother orwellien » ?

La lettre adressée le 15 janvier 2019 à Google, Amazon et Microsoft par 85 ONG consacrées aux droits humains et à la défense des libertés publiques, leur demandant de ne pas vendre de logiciels de reconnaissance faciale aux gouvernements au vu du risque qu'ils constituent aujourd'hui pour des migrants ou des minorités religieuses, et demain pour les générations futures qui se rendraient par exemple à certaines manifestations[5], et les réponses qu'elle a suscitées de la part de responsables de ces société sont, à certains égards, éclairantes[6]. Il en est de même pour le cas de la ville de San Francisco, dont le Conseil municipal, au mois de mai 2019, a récemment interdit certaines utilisations de technologies de reconnaissance faciale par les agents municipaux et la police[7].

A l'heure actuelle, de plus en plus de responsables politiques se prononcent, dans un contexte fortement influencé par la menace terroriste, en faveur de la mise en œuvre de dispositifs de

---

à l'ordre public sont commis ou risquent d'être commis, de dissimuler volontairement tout ou partie de son visage sans motif légitime. »

[5] *« Cette technologie offre aux gouvernements la capacité inédite de traquer qui nous sommes, où nous allons, ce que nous faisons et qui nous fréquentons. (…)*
« Dans un monde de surveillance fondé sur la reconnaissance faciale, les gens craindront d'être repérés et ciblés par le gouvernement s'ils participent à une manifestation, se rassemblent hors des lieux de culte, ou simplement vivent leur vie. »

[6] Ainsi, si les responsables de Google et Microsoft qui se sont exprimés à ce sujet semblent s'être montrés sensibles à cette alerte, ceux d'Amazon ont déclaré qu'il ne leur appartenait pas d'établir les règles de vie en société.

[7] https://www.lemonde.fr/economie/article/2019/05/15/san-francisco-interdit-la-reconnaissance-faciale_5462287_3234.html

reconnaissance faciale sur l'espace public pour renforcer la sécurité du territoire national et sauvegarder l'ordre public en améliorant les modalités de recherche de personnes ayant commis de graves infractions, voire en prévenant la commission de telles infractions (à l'image du scénario du film *Minority Report*).

On le voit, l'émergence de cette nouvelle technologie, d'ores et déjà adoptée et mise en œuvre par certains Etats au nom d'une sécurité qui serait ainsi renforcée, mais aussi fortement contestée au vu de son fonctionnement, fondé sur des données biométriques, et des risques que son déploiement ferait peser sur les libertés fondamentales, illustre à sa manière l'antagonisme classique qui existerait entre sécurité et libertés. Pour autant, il est vraisemblable qu'un subtil équilibre entre l'apport que peut être celui de la reconnaissance faciale dans un contexte de forte exigence de contrôle, et le respect de la vie privée puisse être trouvé. Aussi, après avoir dressé un état des lieux du développement de cette technologie, tant d'un point de vue technique que juridique, français comme international (**I**), il est fait état dans le présent rapport des différents enjeux qu'elle soulève, au nombre desquels figure sans aucun doute la question de la souveraineté nationale incarnée par le rôle que peuvent jouer les industriels français en la matière (**II**).

Les préconisations formulées au terme de ce rapport traduisent la volonté de respecter, et préserver, la vie privée des personnes, et s'inscrivent dans une démarche où le potentiel recours à la reconnaissance faciale se veut pragmatique, et volontairement gradué.

I. ETAT DES LIEUX

A. Que faut-il comprendre de l'expression reconnaissance faciale ?

La reconnaissance faciale, objet du présent rapport, est un procédé informatisé biométrique qui compare, à partir des traits du visage, deux ou plusieurs images prises à des lieux et/ou des moments différents. Cette technique permet notamment de satisfaire plusieurs objectifs :

Authentifier une personne par ce biais consiste à comparer une de ses caractéristiques physiques (en l'occurrence son visage) avec celle enregistrée préalablement (enrôlement) et censée la caractériser. L'authentification permet de répondre à la question « Est-ce bien Monsieur X ? » et donc de confirmer, par exemple, que le porteur d'un titre d'accès est bien celui qu'il prétend être. On parle de système « 1 pour 1 ».

Identifier une personne nécessite de comparer la même caractéristique avec une base de données de personnes connues. L'identification permet de répondre à la question « Qui est cette personne ? » et donc de confirmer, par exemple, que le porteur d'un titre d'accès est bien légitime à accéder au site, puisqu'il figure dans la base de données des « autorisés ». On parle de système « 1 pour N ».

Ré-identifier une personne vise à retrouver quelqu'un préalablement observé. La ré-identification permet de répondre à la question « Ai-je déjà vu cette personne ? » et de confirmer, par exemple, qu'elle a cheminé par différents points du site. Cette action est engagée à la suite d'une première identification formelle (1 pour N) ou à partir de caractéristiques non morphologiques (par ex. un sac ou un vêtement d'une couleur donnée).

Rechercher une personne suppose une action de surveillance permanente d'une foule de personnes inconnues, afin de vérifier si y figure une personne dont on dispose des caractéristiques biométriques de son visage. La recherche permet de répondre à la question « Est-ce que Monsieur X est présent ? ». On parle de système « N pour M ».

Ces grandes catégories d'exploitation d'un dispositif de reconnaissance faciale sont mises en œuvre selon les cas sur des points de passage obligé ou en surveillance plus générale de zone, en milieu public ou privé, en intérieur ou extérieur, en temps réel ou différé et sur une période de temps limitée (à la suite d'un événement) ou en continu.

D'autres technologies, non étudiées dans le présent rapport mais pourtant souvent associées à la reconnaissance faciale, utilisent également la comparaison d'images à des fins de sécurité. Il s'agit principalement de dispositifs permettant de :

- rechercher des objets abandonnés (colis suspect),
- identifier des objets (recherche d'un objet dans des banques vidéo),
- analyser des changements de scènes (sécurisation de trajets ou de lieux),

- détecter des intrusions (définition de zone interdites, « vidéo sensor »),
- lire automatiquement des plaques d'immatriculation (LAPI),
- analyser des comportements (contre sens de circulation, mouvements de foules, ..),
- analyser des expressions ou des émotions exprimées par les visages.

B. Comment fonctionne la technologie ?

1- L'architecture d'un dispositif de reconnaissance faciale

Tous les dispositifs de reconnaissance faciale reposent sur une action de comparaison avec un attribut présenté par une base de données ou un support physique détenu par la personne, et sont généralement construits autour de 5 modules :

- Un système **d'acquisition** collecte l'échantillon d'une image à partir d'un dispositif matériel (caméra, appareil photo, ordinateur …) ;
- Un **procédé de traitement** d'image convertit les données d'échantillon en canevas biométriques uniques, propres à chaque personne. Ce traitement peut être simple si l'image est prise de face par un appareil de bonne qualité, ou bien très complexe, s'il faut isoler une personne dans une foule, corriger les données d'environnement (éclairage …) et « redresser » la photographie, ou bien « vieillir » une image ancienne, ou encore dé-pixelliser une image trop zoomée, etc.
- Une **unité de stockage** des données caractéristiques biométriques sur un support informatique (base de données, puce électronique sur un passeport, code barre sur une carte d'enregistrement de vol, …). Un mécanisme de codage / chiffrement peut être appliqué avant le stockage, rendant les données non lisibles. D'autres données numériques (identité de la personne, données administratives, métadonnées) peuvent être associées à ce stockage.
- Un **dispositif de traitement par comparaison** entre les canevas biométriques, recueillis à des endroits et des moments différents, selon le processus retenu (cf. schéma infra). Ce dispositif donne lieu à un score de correspondance (exprimé en pourcentage de certitude).
- Un **système de décision** s'appuie sur les résultats de la comparaison et des critères de décision (seuil par exemple). Le résultat est de type « Oui/Non » pour une vérification et une liste de candidats possibles dans le cadre d'une identification par score.

Le **processus d'enrôlement** concerne les 3 premières phases précitées et permet ainsi d'enregistrer les caractéristiques biométriques faciales d'une personne ainsi que ses données d'identification.

Actuellement mises en œuvre sur des systèmes dédiés, les implémentations de reconnaissance faciale pourraient se déployer à l'avenir sur des environnements plus distribués et mutualisés, notamment dans le Cloud dans un souci de réduction de coût et d'amélioration des performances. Par ailleurs, les

constructeurs commencent à proposer d'embarquer la technologie de traitement d'images directement dans les caméras et non de façon déportée sur un système informatique.

2- Des standards de référence

Fort de l'expérience relative aux empreintes digitales, les premiers travaux engagés dans le domaine de la reconnaissance faciale ont visé à établir des standards permettant de fiabiliser les résultats d'analyse, faciliter les inter-comparaisons et tenter d'établir les éléments de preuve numérique.

Ainsi, au fur et à mesure du déploiement de cette technologie, plusieurs règles (non formalisées) ont vu le jour chez les industriels du secteur :

- construction des canevas numériques par enregistrement d'un nombre déterminé de points caractéristiques du visage ;
- définition de standards qualitatifs pour les opérations d'enrôlement (visage : 120 X 120 px – espace inter yeux : 80 px), pour les images prélevées (visage : 100 X 100 px – espace inter yeux : 50 px) et pour la résolution minimale des caméras : visage (833 px/m) espace inter yeux (416 px/m) ;
- positionnement des caméras et définition d'angle maximal de déviation verticale (<15°), etc.

Si le positionnement des caméras reste un point stratégique, leurs évolutions techniques (prise en compte du contraste, de l'exposition, etc.), l'augmentation des capacités de calculs et l'avènement des algorithmes permettent d'atteindre des performances élevées, selon les usages envisagés et ce, même dans des conditions d'exploitation difficiles (prises de vues partielles de visages,…).

Ces évolutions techniques ont progressivement mis fin aux tentatives de définition de standards qualitatifs minimums pour l'acquisition et le traitement des images, mais n'ont pas permis, à l'instar de ce qui existe pour l'empreinte digitale, de définir les conditions de la preuve numérique. Aujourd'hui encore, la reconnaissance faciale constitue un outil d'aide à la décision mais l'arbitrage formel permettant de « reconnaitre » une personne reste du ressort d'experts.

3- Le rôle de l'intelligence artificielle dans la technologie de reconnaissance faciale

La reconnaissance faciale évolue considérablement depuis quelques années, portée par les innovations technologiques. La comparaison de deux images ne repose plus désormais sur leurs seuls points caractéristiques, mais sur la confrontation de tous les éléments de l'image (pixels) à partir d'algorithmes bâtis sur des réseaux de neurones artificiels (deep learning). Cette technologie présente l'avantage de l'auto-apprentissage : la machine s'entraine à détecter des visages en examinant des milliers d'images de visage et les résultats (succès ou échec) des comparaisons.

- **Des algorithmes perfectibles**

Les algorithmes étant codés ou entrainés sur des bases prescrites par des humains, ils sont intrinsèquement marqués par des biais de leurs producteurs.

Jean-Michel Loubes, statisticien à l'université de Toulouse, considère qu'il faut donc s'interroger sur le fonctionnement de l'intelligence artificielle et la contrôler. La performance de la reconnaissance faciale nécessiterait une auscultation des entrailles d'algorithmes. Une série de test serait donc indispensable à mettre en œuvre pour vérifier les réponses d'algorithme, et s'assurer que les biais sont gérés. Une stratégie pourrait consister à introduire des exemples « tordus » dans la phase d'apprentissage, pour entraîner le système à se méfier.

Afin de démontrer les vulnérabilités des algorithmes de reconnaissance d'image, Nicolas Papernot, chercheur scientifique, et ses collègues ont cherché à altérer des images de panneaux de signalisation pour transformer des « stops » en « céder le passage », sans que ce changement soit perceptible aux humains.

Enfin, il reste difficile d'expliquer comment la machine obtient ses résultats. Dans ce contexte, un fonctionnement totalement autonome ne semble pas envisageable : cela reviendrait à donner le pouvoir décisionnel à un système de type « boite noire » sans aucune garantie d'objectivité. Ce point conduit le sociologue Jean-Gabriel Ganascia à affirmer que le pouvoir décisionnel doit rester à l'humain.

- **Principales contraintes en termes de besoins d'échantillons**

Pour développer les algorithmes de reconnaissance faciale, les laboratoires de recherche et développement (R&D) ont besoin de gigantesques bases de données « contextualisées » (des centaines de milliers de données), i.e. des images plaçant les personnes dans le contexte de la recherche à mener et les données d'enrôlement associées pour réaliser les correspondances (« hits »). Ces données sont donc « l'or noir » des algorithmes d'auto-apprentissage.

Or, en Europe, ces données sont qualifiées de « données sensibles à caractère personnel ». Leur regroupement et leur exploitation relèvent de règles contraignantes selon les finalités. Les bases de données du NIST[8] ne sont pas disponibles pour la R&D (recherche et développement), mais uniquement dans le cadre de « benchmarks » collaboratifs. Les laboratoires utilisent donc des bases de données publiques - « data-set » académiques ou bibliothèques de visages de personnalités (acteurs, célébrités ...) - qu'ils trient ou enrichissent pour répondre au mieux aux cas d'usage des algorithmes développés.

C. Quelles utilisations de la reconnaissance faciale à ce jour ?

Les cas dans lesquels des technologies de reconnaissance faciale sont utilisées sont très variés : en dehors du cadre « sécuritaire » (et militaire), les objectifs poursuivis sont souvent « utilitaires » ou « commerciaux », selon les secteurs.

[8] National Institute of Standards and Technology (USA)

Le premier secteur concerné est celui de « **l'identité civile et la lutte contre la fraude administrative**», où ces nouvelles technologies sont mises à profit pour fiabiliser le vote électronique (ex. Benin, Burkina faso) ou le recensement d'état-civil (ex. Inde, Gabon), pour détecter des personnes non autorisées lors de grands événements (ex. Marathon de Hangzhou en Chine), lutter contre le trafic animal (ex. ChimpFace : surveillance des chimpanzés vendus sur les réseaux sociaux), ou encore pour vidéo-verbaliser (ex. téléphone au volant, non-port de la ceinture de sécurité, etc.).

Un deuxième domaine d'intégration des technologies de reconnaissance faciale concerne la **« sphère privée et la sécurité numérique »,** où leur usage se démocratise massivement pour déverrouiller l'accès à son smartphone, son domicile ou son véhicule, pour retirer de l'argent (ex. les distributeurs automatiques de billets testés en Espagne pour la société CaixaBank), payer ou ouvrir un compte bancaire (ex. de la Société Générale) ou bénéficier de services personnalisés (ex. miroir interactif suggérant des actions et gérant les stocks de produits associés à chaque personne identifiée, diffusion de musique ou autres services au franchissement de la porte du domicile).

Le secteur de la **« santé, prévention ou de l'aide à la personne »** bénéficie également de cette innovation, et les technologies de reconnaissance faciale sont déployées pour réaliser des diagnostics de maladies rares (ex. Face2Gene - revue Nature Medicine), aider les non-voyants en décryptant l'environnement et en transmettant les informations recueillies oralement (ex. MyEye 2.0), combattre la fatigue et le manque d'attention du conducteur de véhicule (ex. Driverfocus du SUV SUBARU Forester), rechercher les parents d'enfants abandonnés (ex. New Delhi et les enfants de « la génération perdue » - ONG Bachpan Bacho Andolan de Kailash Satyarthi). Mais le secteur le plus porteur de dispositifs de reconnaissance faciale est celui du **« commerce ».** Les technologies sont principalement exploitées pour améliorer l'expérience utilisateurs, augmenter les performances de vente, diminuer les ressources nécessaires et optimiser les offres commerciales :

- Le secteur des transports cherche à fluidifier l'accès aux aérogares en limitant les temps de contrôle (ex. aéroports d'Atlanta, Changi, Paris), voire à remplacer les titres de transports (ex. métro de Londres ou projets pour les transports en commun parisiens - Audition de V. Pécresse au Sénat – Février 2019).
- Dans les espaces publics, l'objectif est de détecter des dysfonctionnements d'exploitation nécessitant l'intervention de personnels (escalators en panne, poubelles débordantes, distributeurs vides, ..).
- Dans le domaine du commerce et du marketing, la technologie fournit une offre totalement personnalisée aux clients de services ou produits. Les dispositifs recueillent les émotions des clients en réaction aux publicités et adaptent en conséquence leurs messages publicitaires. Des groupes hôteliers investissent sur des robots de services disponibles 24h/24, qui délivrent des commandes aux clients (ex. Space egg de la société Alibaba) et assurent un service toujours plus personnalisé en événementiel (ex. RecoBooth qui permet l'accueil personnalisé des clients, une communication adaptée, une consultation du programme de fidélité, ...).

Enfin, dans le domaine **« militaire »**, les armées suivent les développements de la reconnaissance faciale, non seulement pour tout ce qui a trait de façon classique à la protection de leurs bases (casernes, arsenaux, bases aériennes, états-majors etc.), mais aussi pour tout ce qui concerne la biométrie en opération (suivi des interprètes, des employés de recrutement local, des contacts et des VIP, des personnes suspectes ou capturées, etc.), et ce qui relève du suivi logistique (sanitaire notamment) et tactique des opérations, dans la perspective d'un commandement assisté par l'IA (ou intelligence artificielle).

1- Les premières utilisations en France

Si la reconnaissance faciale constitue un sujet d'attention particulier dans la presse, il n'en est pas moins vrai que l'utilisation de cette technologie reste à ce jour cantonnée à des contextes très encadrés et à titre expérimental. Le déploiement existant le plus pérenne est le système automatisé PARAFE fonctionnant sur un mécanisme d'authentification limitant les enjeux en termes de traitement de données biométriques. Différentes expérimentations se développent quant à elles, toujours sous l'œil attentif de la CNIL, notamment à l'initiative d'entreprises concernées par des impératifs sécuritaires majeurs (ex : ADP – aéroports de Paris) ou par des enjeux concurrentiels d'optimisation du service apporté aux passagers, mais également d'autorités publiques.

- **L'utilisation à des fins préventives et sécuritaires par des organismes privés et/ou publics**

Essentiellement motivés par des objectifs de sécurité sur fond de menace terroriste, mais aussi de fluidité des contrôles, les dispositifs de reconnaissance faciale commencent à se déployer sur le territoire national.

De tels dispositifs intègrent peu à peu les aéroports et les gares françaises. Des expériences sont menées par GEMALTO à Roissy et Orly (PARAFE), et la société portugaise Vision-Box à la Gare du Nord (e-Gate).

Le système automatisé PARAFE (Passage Automatisé Rapide aux Frontières Extérieures), inauguré en 2009 à l'aéroport Roissy-Charles de Gaulle, s'est étendu à d'autres aéroports français (Orly, Nice-Côte d'Azur, Lyon-Saint-Exupéry) et modernisé pour intégrer une authentification biométrique multimodale, dont la reconnaissance faciale. Les visages des passagers sont scannés et comparés avec la photographie stockée dans le microprocesseur du passeport biométrique. La comparaison confirmant l'authentification déclenche l'ouverture du sas sous 10 à 15 secondes.

Plusieurs expérimentations permettant d'évaluer les éventuelles contraintes résultant de la mise en œuvre de dispositifs de reconnaissance faciale et le ressenti des personnes ont été menées dans le secteur aérien, avec l'accord de la CNIL, dans des conditions réelles (parcours passagers conformes à la configuration des aérogares, utilisation des systèmes de vidéoprotection existants) :

- identification biométrique (reconnaissance faciale et empreinte digitale) des passagers volontaires en entrée et sortie de salle d'embarquement[9] ;

- reconnaissance biométrique des visages de participants volontaires circulant dans des zones délimitées des aérogares d'Orly et de Roissy-Charles de Gaulle[10],

- expérimentation des Aéroports de Paris et d'Air France visant à fluidifier le parcours passagers par l'automatisation des procédures d'enregistrement, d'embarquement et de contrôle, le visage devenant alors une carte d'embarquement et un document d'identité.

Dans tous ces cas, le dispositif mis en œuvre reposait sur le volontariat des personnes dont les données étaient traitées. Les personnes ne souhaitant pas participer à l'expérimentation pouvaient emprunter un chemin alternatif, les gabarits de leurs visages réalisés à la volée étaient immédiatement supprimés à l'issue de la comparaison. Le dispositif testé bénéficiait de moyens techniques dédiés, sécurisés, dont l'accès était réservé à des personnels spécifiquement habilités.

- **Le projet porté par le Conseil régional de Provence-Alpes-Côte d'Azur**

Afin de mieux sécuriser les établissements scolaires tout en fluidifiant les entrées, le conseil régional de Provence-Alpes-Côte d'Azur (PACA) a, pour sa part, proposé à deux lycées d'expérimenter un dispositif de contrôle d'accès en partie fondé sur des techniques biométriques, en particulier la comparaison faciale. Le dispositif mis en œuvre consiste à opérer un traitement sur les images du visage d'une personne, lequel permet d'obtenir un gabarit, qui, à son tour, fait l'objet d'un chiffrement. La seule donnée conservée en base est le gabarit chiffré, la clé de déchiffrement étant conservée sur le support individuel détenu par la personne concernée. Le système biométrique ne s'active que sur présentation de ce support individuel d'identification, ce qui déclenche une prise d'images du visage. Là aussi, seuls les lycéens volontaires participent à cette expérimentation. Les données collectées (photographies prises sous différents angles) sont détruites dès lors que la comparaison est effectuée. Les gabarits stockés, chiffrés dans la base de données, ne permettent pas de recréer la photographie dont ils sont dérivés, et les données relatives à l'identité des personnes concernées sont conservées de manière séparée.

- **L'expérience du Carnaval de Nice**

Souvent citée pour les projets et expérimentations de nouvelles technologies qu'elle initie, la municipalité de la ville de Nice a mis en œuvre la première expérience impliquant de la reconnaissance faciale sur la voie publique à l'occasion de la 135ème édition du Carnaval de la ville, au mois de février 2019.

L'objectif, tel qu'expliqué par Sandra Bertin, Directrice de Police municipale, en charge du déploiement du projet, était de tester l'efficacité d'un tel dispositif dans les conditions réelles d'un très

[9] cf. délibération de la CNIL n° 2015-432 du 10 décembre 2015
[10] cf. délibération de la CNIL n°2016-188 du 30 juin 2016

grand évènement. Afin de permettre l'expérimentation, il a été constitué en amont un fichier de photographies de personnes volontaires ayant pour objet de servir de points de comparaison avec les images qui seraient issues des caméras de vidéoprotection de la ville dédiées temporairement à l'expérience et placées au niveau d'une entrée choisie du Carnaval. Plusieurs scénarios ont été mis en place afin de mesurer par exemple les capacités d'interpellation à la suite d'un signalement déclenché par le dispositif. Il a notamment été testé l'efficacité du logiciel sur de vrais jumeaux, une personne portant un casque de moto, ou une importante différence d'âge entre la photographie initiale et l'image captée par la caméra de vidéoprotection.

Consultée préalablement à la mise en œuvre de l'expérimentation, la CNIL a émis une série de recommandations, en application des exigences légales et règlementaires (RGPD), relatives notamment, à l'information préalable des personnes souhaitant emprunter l'entrée dédiée à l'expérimentation, la collecte de leur consentement et la traçabilité de celui-ci, la limitation de la durée de conservation des données collectées au seul temps de l'expérimentation, la suppression immédiate par le logiciel des gabarits des personnes volontaires entrant dans le champ de la caméra, mais ne figurant pas dans le fichier des personnes volontaires.

Selon Sandra Bertin, l'expérience a été un succès en ce qu'elle a permis de révéler la très grande efficacité du logiciel testé dans des conditions réelles d'affluence.

- **L'utilisation de la reconnaissance faciale dans un cadre judiciaire**

La Police Technique et Scientifique a recours, pour certaines affaires, à la reconnaissance faciale. Grâce à un logiciel d'analyse, les scientifiques peuvent, dans un ensemble important de vidéos saisies, rechercher une ou plusieurs personnes. Le logiciel offre la possibilité de sélectionner un ou plusieurs visages dans une des vidéos ou d'importer quelques photographies de visages ciblés par l'enquête, et de rechercher leur présence dans l'ensemble des vidéos. Ces analyses sont demandées dans un cadre légal à la suite d'une réquisition faite par des officiers de police judiciaire ou d'une ordonnance de commission d'expert d'un juge d'instruction. Le traitement d'antécédents judiciaires (TAJ) est pour l'instant le seul fichier comportant une photographie dont l'usage est autorisé à des fins de reconnaissance faciale.

2- Une utilisation en large progression à l'étranger

La reconnaissance faciale connaît au niveau international un développement nettement plus important et abouti qu'en France. De nombreux pays connaissent des déploiements à grande échelle et l'utilisation sur la voie publique s'illustre également à travers plusieurs exemples, non limités à la question sécuritaire.

- **L'utilisation à des fins d'enquête par Europol**

L'Agence européenne de police criminelle, ayant pour objectif de faciliter l'échange de renseignements entre polices nationales, en matière de stupéfiants, de terrorisme, de criminalité

internationale et de pédophilie, utilise depuis environ deux ans un dispositif de reconnaissance faciale. La technologie, développée à travers un outil élaboré en interne à l'Agence, est utilisée à des fins d'enquête et non pour de la détection en temps réel. Elle fonctionne avec des algorithmes commerciaux, permet à ce jour l'identification à partir de photographies de face mais pourrait, à court terme, également fonctionner à partie de clichés de profil. Les supports, tant vidéos que photographiques, peuvent faire l'objet de recherches à l'aide du dispositif conçu.

Les cadres d'utilisation les plus fréquents sont notamment la recherche dans des volumes importants de données (saisies d'ordinateurs ou téléphones), la lutte contre la fraude documentaire dans le cadre criminel ou anti-terroriste (faux documents en cours d'utilisation qui correspondraient à des suspects connus d'Europol), ou encore l'exploitation de sources ouvertes, telles que des vidéos mises en ligne à des fins de propagande terroriste.

- **La sécurisation de villes et sites sensibles**

Mexico, capitale de 22 millions d'habitants, a développé le programme de sécurité urbaine le plus ambitieux au monde (si l'on excepte la Chine). En 2017, THALES, allié à TELMEX (leader des télécoms au Mexique) a intégré 7 000 nouvelles caméras (qui en compte au total 20 000) au projet « Ciudad segura », qui a permis depuis 2009 des avancées spectaculaires en matière de réduction de la délinquance (-56%) ou de temps d'intervention des forces de sécurité ou de secours. La reconnaissance faciale adossée à ce programme est gérée par la société chinoise DAHUA, qui occupe une place centrale dans ce dispositif.

Sur le continent nord-américain, les polices des villes de New York et Chicago, l'état de Hawaï utilisent le système "Amazon Rekognition", et le Ministère de la sécurité intérieure s'apprête à déployer dans un nombre important d'aéroports les mêmes systèmes de reconnaissance faciale que ceux déjà en service dans les plus importants hubs du pays. Delta Air Lines a récemment annoncé le lancement du premier terminal "biométrique" à Atlanta. British Airways a également récemment installé des technologies biométriques afin d'identifier ses clients dans les aéroports de New York, Orlando, et Miami.

L'exemple récent du renforcement de la sécurité autour de la Maison Blanche à Washington DC par les services secrets, avec des caméras connectées à un nouveau système de reconnaissance faciale, a relancé le débat de la surveillance de masse aux Etats-Unis.

Les 12 millions de moscovites vont bientôt bénéficier des services de 7 000 nouvelles caméras couplées à de la reconnaissance faciale, s'ajoutant à plus de 170 000 dispositifs vidéo déjà existants. La Russie est en effet l'un des pays les plus en pointe sur le sujet de la reconnaissance faciale. En juillet 2018, les 850 000 supporteurs étrangers du Mondial de football ont servi de sujets d'expérience d'un vaste système de surveillance vidéo couplé à de la reconnaissance faciale (ID Fan).

- **La construction d'un état-civil numérique en Inde**

L'Inde est le pays où plus d'un milliard de personnes ont été enrôlées depuis 2010, lesquelles se sont vu attribuer un numéro d'identification unique à 12 chiffres une fois leurs données biométriques enregistrées. Introduit comme une démarche volontaire pour lutter contre la fraude fiscale, le système concerne désormais le règlement des impôts, les allocations et services sociaux fournis par l'Etat fédéral et les gouvernements locaux.

- **Des utilisations et expérimentations sur le continent européen**

A l'été 2019, l'aéroport de Londres-Heathrow disposera de l'un des plus importants systèmes d'identification biométrique au monde, adoptant la reconnaissance faciale à chaque étape du parcours voyageur (de l'enregistrement aux couloirs de sécurité, en passant par les portes d'embarquement et la récupération des bagages). Ce projet représente un coût total de 50 M £ soit 57 M €.

À Madrid, une expérimentation de reconnaissance faciale a été mise en œuvre dans la plus grande gare routière du pays (20 millions de passagers par an). Ce dispositif est conjointement exploité par le service de sécurité privée de l'opérateur (Grupo Avanza), qui exploite en temps réel le réseau de vidéosurveillance, et la Guardia Civile espagnole qui fournit la base de données des personnes à comparer. Les résultats positifs sont collectés par l'opérateur privé pour transmission et exploitation par un agent de la Guardia.

Une expérimentation a été initiée à l'été 2018 dans la gare Südkreuz de Berlin, fruit d'une collaboration entre le Ministère de l'Intérieur et la Deutsche Bahn, à des fins de lutte contre le terrorisme.

- **Le cas particulier de la Chine**

Le cas le plus avancé et médiatisé reste incontestablement celui de la Chine. La technologie y a transformé de nombreux aspects de la vie quotidienne, de l'accès à certaines zones ou locaux, au paiement ou à la détection de personnes recherchées.

Ainsi, les employés du géant du commerce en ligne Alibaba à Shenzhen peuvent-ils accéder à leurs locaux en montrant leur visage. Les passagers des voitures de Didi Chuxing (leader du VTC en Chine) utilisent le logiciel Face++ pour leur permettre de confirmer que le conducteur est bien légitime. Les membres du personnel de Baidu (le « Google chinois ») peuvent régler avec leur visage au restaurant de l'entreprise. Face++ est également utilisé par les gouvernements locaux pour identifier les criminels présumés, à partir des caméras de surveillance qui sont omniprésentes au sein du pays (la Chine en comptera près de 450 millions à l'horizon 2020). Une start-up chinoise a récemment dévoilé au CES de Las Vegas un concept car électrique (Byton) qui identifie le propriétaire de la voiture grâce à la reconnaissance faciale, récupère son profil depuis un service hébergé sur le Cloud et l'accueille en conséquence personnellement, tout en ajustant les sièges et la température.

D. Quel encadrement juridique ?

Au nombre des biométries disponibles (empreintes digitales, iris, voix, etc.), la reconnaissance faciale est particulière, basée sur la capture d'une photographie du visage d'une personne, à laquelle est appliqué un procédé technique permettant d'extraire des caractéristiques, le « gabarit ». C'est à partir de cette représentation mathématique du visage que la comparaison faciale est effectuée. L'usage qui peut être fait de cette catégorie de données est strictement encadré par les dispositions relatives à la protection des données.

1- La réglementation relative à la protection des données à caractère personnel applicable

- **Le principe d'interdiction des traitements de données biométriques**

Dès lors qu'une image numérique[11] contient le visage, clairement visible, d'une personne qui peut ainsi être identifiée, elle doit être considérée comme une donnée à caractère personnel, dont le traitement est strictement encadré par la législation. Ainsi, aux termes de l'article 9 du règlement général sur la protection des données (RGPD) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, le traitement des données biométriques aux fins d'identifier une personne physique de manière unique est interdit.

Les données biométriques ne sont pas des données à caractère personnel "comme les autres" et ont un caractère particulièrement sensible. «*Elles présentent en effet la particularité de permettre à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir. À la différence de toute autre donnée à caractère personnel, la donnée biométrique n'est donc pas attribuée par un tiers ou choisie par la personne: elle est produite par le corps lui-même et le désigne ou le représente, lui et nul autre, de façon immuable. Elle appartient donc à la personne qui l'a générée et tout détournement ou mauvais usage de cette donnée fait alors peser un risque majeur sur l'identité de celle-ci*[12] ».

Ce même article (art. 9-2-g) prévoit toutefois certaines exceptions et la possibilité de traiter ces données, notamment « *si la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée* », si « *le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un Etat membre qui doit être proportionné à l'objectif poursuivi,*

[11] Aux termes du considérant 51 du RGPD, les photographies ne relèvent de la définition de données biométriques (lesquelles méritent une protection spécifique dès lors qu'elles sont particulièrement sensibles du point de vue des libertés et des droits fondamentaux) que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique.

[12] Cf. note d'observations du 25 octobre 2011 de la CNIL concernant la proposition de loi n° 682 relative à la protection de l'identité

respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ». Il précise i*n fine* que « *Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement (…) des données biométriques* ».

Aussi, l'article 27 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, dispose-t-il que les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes, sont autorisés par décret en Conseil d'Etat pris après avis de la CNIL.

Les dispositions nationales de transposition de la directive (UE) 2016/680 « Police-Justice », qui établit les « *règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* », prévoient, quant à elles, que « *Le traitement de données [biométriques]est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et soit s'il est autorisé par une disposition législative ou réglementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée »*[13].

- **Des exigences de nécessité et proportionnalité**

Le Conseil Constitutionnel a régulièrement rappelé, aux termes de sa jurisprudence, la compétence du législateur et la conciliation qu'il lui appartient d'opérer entre la sauvegarde de l'ordre public et le respect des autres droits et libertés constitutionnellement protégés (cf. notamment Décision n°2012-652DC du 22 mars 2012 portant sur la loi relative à la protection de l'identité).

Le Conseil d'Etat, pour sa part, s'assure notamment que les mesures de collecte et de traitement des données personnelles ne constituent pas une atteinte disproportionnée à la vie privée, notamment protégée par la CEDH[14]. Il a ainsi rappelé que l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée, qui résulte de l'article 2 de la Déclaration de 1789, que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives, ne peut être légalement autorisée que si elle répond à des finalités légitimes et si le choix, la collecte et le

[13] Cf. art. 70-2 de la loi du 6 janvier 1978 modifiée

[14] Cf. art. 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales :
« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

traitement des données sont effectués de manière adéquate et proportionnée au regard de ces objectifs (cf. CE Ass.26/10/2011, Association pour la promotion de l'image et autres).

Il résulte de ces dispositions et jurisprudences que la mise en œuvre de dispositifs de reconnaissance faciale par un organisme privé ou public ne saurait être envisagée sans qu'une réflexion portant sur l'évaluation de la nécessité de mettre en place un traitement de données biométriques et sur la proportionnalité des modalités de sa mise en œuvre soit préalablement menée. Quelle que soit la base légale du traitement (consentement, intérêt légitime ou intérêt public du responsable de ce traitement de données sensibles), une analyse d'impact relative à la protection des données (AIPD) doit être effectuée, notamment afin de documenter l'appréciation opérée des risques pour les droits des personnes, et des mesures prises pour les limiter. Que le dispositif ait un caractère expérimental ou pérenne, l'ensemble des formalités doivent être remplies : le responsable de traitement doit ainsi respecter le règlement type « biométrie sur les lieux de travail » adopté par la Commission nationale de l'informatique et des libertés (CNIL) le 10 janvier 2019, et notamment justifier le recours à la biométrie par des considérations spécifiques, dès lors que le dispositif de reconnaissance faciale a pour finalité le contrôle d'accès aux locaux, applicatifs ou outils professionnels ; ce traitement de données biométriques doit être autorisé par décret en Conseil d'Etat pris après avis de la CNIL s'il a par exemple pour objet de prévenir ou détecter des infractions pénales.

2- La réglementation applicable en matière de vidéoprotection

Les dispositifs de reconnaissance faciale, compte tenu des avancées technologiques qu'ils connaissent, peuvent désormais fonctionner dans un environnement « non-contrôlé »[15]. Les gabarits des personnes sont alors calculés sur la base d'images de visages capturées dans un flux ou une foule de personnes filmées à l'aide de réseaux de caméras. Les dispositifs d'analyse automatisée du flux vidéo, pouvant embarquer des modalités de reconnaissance faciale, reposent généralement sur des systèmes de vidéoprotection, régis par le code de la sécurité intérieure, qui doivent satisfaire aux exigences de protection des données[16], quelles que soient les dispositions applicables[17]. Il s'agit en principe, depuis l'entrée en application du « Paquet européen », du RGPD, mais si la finalité poursuivie relève de la

[15] En pratique, les personnes ne passent pas à travers un portail biométrique, ni ne se présentent devant un lecteur pour permettre le calcul et la comparaison de leur gabarit facial (tel que pour l'authentification biométrique mise en œuvre dans le cadre du contrôle aux frontières avec PARAFE, par exemple)

[16] Art. L. 252-1 du Code de la sécurité intérieure : « *les enregistrements visuels de vidéoprotection répondant aux conditions fixées aux articles L.251-2 et L. 251-3 sont soumis aux dispositions du présent titre, à l'exclusion de ceux qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques, qui sont soumis à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* ».

[17] L'image d'une personne enregistrée par une caméra permettant d'identifier la personne concernée, elle constitue une donnée à caractère personnel ; un système de vidéoprotection est, quant à lui, un traitement automatisé de ces données.

directive « Police-Justice » du 27 avril 2016[18] et que le traitement est mis en œuvre par une « autorité compétente », les dispositions applicables sont celles du chapitre XIII de la loi "Informatique et Libertés".

Outre les formalités préalables qu'ils doivent accomplir en application de l'article 70-3 de la loi « Informatique et libertés », les responsables de traitement sont désormais assujettis à de nouvelles obligations : notification à l'autorité de contrôle de toute violation de données personnelles, tenue d'un registre, désignation le cas échéant d'un délégué à la protection des données. Au surplus, dans de très nombreux cas, une analyse d'impact sur la protection des données (AIPD) doit être réalisée.

Les responsables de traitement doivent également veiller à ce que les personnes qui souhaitent exercer les droits qui leur sont reconnus (droits d'information, d'accès, à l'effacement des données) obtiennent satisfaction.

3- La rareté des fichiers utilisables dans la sphère régalienne

Compte tenu du contexte sécuritaire dans lequel la reconnaissance faciale pourrait être utilisée, plusieurs fichiers sont régulièrement cités pour permettre d'identifier, dans le domaine public, des personnes recherchées ou susceptibles de commettre de graves actes répréhensibles. Pour autant, à ce jour, les textes encadrant leur fonctionnement ne le permettent pas toujours.

- **Le Fichier des personnes recherchées (FPR)**

Le FPR recense, en différentes catégories, toutes les personnes faisant l'objet d'une mesure de recherche ou de vérification et a vocation à faciliter l'action des services de police et de gendarmerie, des autorités judiciaires, militaires ou administratives. L'inscription au FPR intervient notamment pour des motifs d'ordre public, tels que la prévention de menaces contre la sécurité publique ou la sûreté de l'Etat. Il est loisible que les photographies des personnes enregistrées au titre des catégories « S » (sûreté de l'Etat), « M » (mineurs fugueurs) ou « V » (évadés) pourraient être considérées mobilisables par certains acteurs de la sphère régalienne pour lutter contre la criminalité particulièrement grave ou protéger des personnes vulnérables en recourant à des dispositifs de reconnaissance faciale. Cependant, le décret du 28 mai 2010 créant le FPR précise que la photographie ne peut faire l'objet d'un dispositif de reconnaissance faciale.

- **Le traitement des antécédents judiciaires (TAJ)**

En application des articles 230-6 à 230-11 du code de procédure pénale, le traitement des antécédents judiciaires est utilisé dans le cadre d'enquêtes judiciaires (recherche des auteurs d'infractions) et

[18] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

d'enquêtes administratives (comme par ex. les enquêtes préalables à certains emplois publics ou sensibles). Il comprend des informations concernant des personnes mises en cause, des victimes, ou des personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort, de blessures graves ou d'une disparition au sens des articles 74 et 74-1 du code de procédure pénale. Au nombre des données enregistrées, figure la photographie, qui comporte des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale.

- **Le fichier des titres électroniques sécurisés (TES)**

Le fichier TES regroupe les traitements de données à caractère personnel relatifs aux passeports et aux cartes nationales d'identité (cf. décret n°2016-1460 du 28 octobre 2016 modifié). Il vise, d'une part, à faciliter l'établissement, la délivrance, le renouvellement, l'invalidation et le retrait des titres concernés et, d'autre part, à prévenir et détecter leur falsification et contrefaçon. *In fine*, il centralise notamment, dans une base de données, l'image numérisée du visage de l'ensemble des demandeurs de carte nationale d'identité et de passeport, et réunit ainsi les données biométriques relatives à la quasi-totalité de la population française.

La création de ce traitement a conduit à un débat, notamment parlementaire, qui a généré des interrogations sur la collecte, la centralisation, le fichage, la sécurité et le détournement de données biométriques. Aussi, le gouvernement a-t-il demandé à l'ANSSI et à la DINSIC de se pencher sur le fonctionnement de ce fichier afin d'émettre différentes recommandations. La CNIL, quant à elle, a relevé dans sa délibération n°2016-292 du 29 septembre 2016 portant avis sur le projet de décret, que « le II de l'article 3 (…) prévoit que le traitement TES ne comportera pas de dispositif de recherche permettant l'identification à partir de l'image numérisée du visage ou des empreintes digitales. Les données biométriques ne seront accessibles qu'à partir des données d'identité, ce qui permettra de vérifier l'identité avancée par le demandeur, mais non de rechercher l'identité d'une personne à partir de ses empreintes ou de sa photographie ». Elle a par ailleurs souligné « que l'effectivité de cette exclusion, qui suppose la mise en œuvre de mesures de sécurité strictes et un contrôle permanent des accès aux données ainsi que de leur utilisation, doit impérativement être assurée ».

La décision du Conseil d'Etat du 18 octobre 2018 a entériné la création du traitement TES par la voie réglementaire, mettant en avant son efficacité contre la fraude, qui est un motif d'intérêt général , et relevant notamment qu'il ne dispose pas de dispositif de recherche permettant l'identification à partir de l'image numérisée du visage (…). La collecte et le traitement de données personnelles et sensibles « *ne portent pas au droit des individus au respect de leur vie privée une atteinte disproportionnée aux buts de protection de l'ordre public en vue desquels ce traitement a été créé*».

II. ENJEUX ET PRECONISATIONS

A. Les enjeux techniques pour les industriels

1- Les enjeux de développement rencontrés par l'industrie française

Dans ce monde où les technologies sont reines, et les droits des citoyens à géométrie variable selon les régimes qui les utilisent, les industriels français ont une réputation d'excellence et une longue expérience de la biométrie, ce qui les place idéalement sur ces marchés. Reste que l'avènement du « deep learning » leur impose désormais de disposer d'énormes bases de données propres à doper leurs algorithmes. L'absence de cadre légal permettant en France de les « faire travailler » leur interdit, sauf exception pour l'instant, de tester leurs solutions en conditions réelles sur le territoire.

- **Un marché grandissant**

De nombreuses études récentes montrent que le marché de la reconnaissance faciale est en très forte croissance. Le cabinet Markets&Markets prévoit une augmentation annuelle de 14% pour atteindre en 2022 près de 8 milliards de dollars. La progression annuelle est encore plus élevée selon le cabinet Allied Market Research qui l'évalue à 21% par an avec une valorisation de 9,6 milliards $ en 2022. Selon le même cabinet, la zone Asie/Pacifique devrait connaître la plus forte expansion et si l'on en croit l'étude réalisée par GenMarket Insights, la Chine devrait même représenter près de 45% du marché en 2023 avec une progression annuelle de 30%. Le marché est actuellement principalement dominé par les industriels américains (Aware, Daon, FaceFirst,etc.), chinois[19] et japonais (NEC, Ayonix,…).

La France demeure l'un des principaux acteurs dans le domaine des solutions biométriques. En 1974, la société Morpho a d'ailleurs mis en service le premier système automatisé d'identification biométrique pour le compte du FBI. Idémia (ex Morpho) et Thales (qui vient de racheter Gemalto) sont les deux leaders français qui conçoivent et développent partout dans le monde des solutions biométriques, dont la reconnaissance faciale.

Au-delà de ces grands industriels, on comptabilise d'autres entreprises qui évoluent plus sur des marchés de niche. C'est le cas des sociétés AXIS, Aquilae, Komanche, ALCEA, de la société Eldim retenue par Apple pour le développement du système FaceID, de la société Reminiz désignée comme l'une des start-up les plus innovantes lors du dernier CES à Las Vegas. Ce savoir-faire est reconnu à l'international et certains pays comme les Etats-Unis ont recours à des solutions françaises qui jouissent

[19] La Chine, où la sécurité est prépondérante et les questions éthiques moins prégnantes, est en train d'investir massivement dans des start-up telles que CloudWalk, Megvii (Face++) et SenseTime. Cette dernière a réussi à lever en mois de deux mois 1,2 milliard de dollars auprès d'investisseurs dont le géant chinois Alibaba, démontrant l'intérêt majeur pour ces nouvelles technologies.

d'un niveau de confiance plus élevé que celles d'autres pays. Compte tenu du cadre réglementaire plus contraint dans notre pays, les solutions développées par les industriels français sont majoritairement commercialisées en dehors de la France, ce qui n'est pas sans poser des problèmes pour des groupes français qui ne peuvent pas mettre en avant de références hexagonales.

- **Le rôle à jouer par l'industrie française**

L'utilisation grandissante de l'Intelligence Artificielle (IA) dans les technologies de reconnaissance faciale risque de pénaliser fortement les industriels français. En effet, pour être plus efficaces, les algorithmes doivent être entraînés à partir de bases contenant un très grand nombre d'images de visages variés provenant d'origines différentes. La réglementation française contraint fortement l'utilisation de telles bases de données, ce qui n'est pas le cas dans d'autres pays.

A titre d'exemple, pour améliorer son algorithme d'IA, la société chinoise Cloudwalk a acheté au Zimbabwe la totalité de sa base de données contenant des visages de ses citoyens.

Il résulte de ces éléments que le maintien d'un rôle et d'une place significatifs par les acteurs industriels français en cette matière nécessite qu'ils puissent parfaire les performances des algorithmes.

D'autant que, comme dans d'autres domaines stratégiques, l'usage par la France de technologies de reconnaissance faciale étrangères pourrait porter atteinte à la souveraineté de notre pays, le risque d'introduction de portes dérobées – pouvant permettre à des puissances ou acteurs tiers d'obtenir des informations de sécurité à des fins d'espionnage ou de déstabilisation – ne pouvant être écarté.

Dans ce contexte, il semble indispensable de donner aux industriels français la possibilité de constituer des bases de données contenant des visages à des fins uniques de R&D et ainsi de permettre le développement de solutions de reconnaissance faciale par ces derniers.

2- Des exigences et défis techniques pour créer la confiance

Les impératifs techniques relatifs à la reconnaissance faciale sont, comme dans toute technologie innovante, nombreux et constituent des défis auxquels les solutions devront apporter des réponses avant tout déploiement. Les exigences préalables au bon fonctionnement des dispositifs, mais également les risques inhérents à la nature de ces derniers, devront être anticipés et traités, dans l'objectif de garantir la pérennité du développement de la technologie et de son déploiement, fondée sur une confiance assurée.

- **Des données d'entrée qualitatives**

La qualité des données d'entrée est un paramètre qui détermine de façon substantielle la performance d'un système de reconnaissance faciale. Cela est particulièrement vrai pour les utilisations du type contrôle d'accès (sites sensibles, aéroports,…), pour lesquelles les photographies de visages captées lors de l'opération d'enrôlement doivent être de très bonne qualité.

Pour d'autres usages de la reconnaissance faciale, il est intéressant de disposer d'images différentes de chaque personne enrôlée : vues de face, de profil et sous différents angles, voire 3D. En effet, pour éviter que l'algorithme n'incorpore au cours de son auto-apprentissage une spécificité biaisée, il est important que les données soient hétérogènes et nombreuses (hommes, femmes, foncés, clairs, petits, grands, etc.).

La qualité et la quantité de données que les algorithmes sont susceptibles de traiter sont donc des paramètres importants, qui impactent directement la puissance de calcul nécessaire pour permettre le traitement de ces données dans des délais cohérents avec l'objectif recherché.

- **Des mesures de performance et retours d'expériences**

Compte tenu des difficultés de mise en œuvre des solutions de reconnaissance faciale, il n'est aujourd'hui pas possible de bénéficier d'évaluation statistique de leur performance. L'évolution technologique extrêmement rapide ne permet pas non plus de figer un niveau de référence minimum, base d'une possible normalisation.

De fait, les principaux fournisseurs de solutions qui souhaitent « s'étalonner » participent au « Face Recognition Vendor Test » (FRVT) du NIST américain, référence dans le domaine. Celui-ci teste les solutions proposées sur une base principale d'environ 26 millions de portraits (d'environ 12 millions de personnes), et sur plusieurs bases de plus petites tailles : 3 millions d'images extraites de webcam, 2,5 millions de photographies de professionnels et amateurs, 90 000 visages extraits de vidéosurveillance.

Ce classement, s'il a le mérite d'exister, doit être interprété avec prudence car les résultats de ces « compétitions » restent très dépendants des conditions de test.

Certains pays réalisent ponctuellement des tests, à échelle 1, très coûteux, pour évaluer les algorithmes (exemples britanniques et singapouriens) quand l'office fédéral de police criminelle allemand (BKA) investit régulièrement sur des tests de grande ampleur (cf. publication de 2007 sur les tests conduits avec le concours de la Deutsche Bank[20] ou les essais conduits à la gare ferroviaire de Berlin en 2018[21]).

Faute de tests officiels, ce sont les analyses critiques ponctuelles et souvent partisanes qui sont relayées par voie de presse ou sur Internet. Elles présentent le plus souvent la reconnaissance faciale comme une technologie peu mature avec une fiabilité faible, comme l'illustrent les exemples suivants :

- Cardiff, lors de la finale de la Ligue des Champions en 2017 : la police britannique a constaté un taux d'erreurs de 92% et plus de 2000 personnes ont été identifiées à tort comme de potentiels criminels ;
- Carnaval de Notting Hill en 2017 : le test réalisé a relevé 35 cas de faux positifs et l'arrestation d'un innocent ;

[20] https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/Foto-Fahndung/foto-fahndung_node.html

[21] https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/10/gesichtserkennung-suedkreuz.html

- L'application Rekognition d'Amazon a identifié 28 criminels parmi les membres du congrès américain.

La performance d'un dispositif de reconnaissance faciale étant une donnée clef de son acceptabilité, il semble nécessaire de progresser dans la capacité à l'évaluer. La normalisation semble être un objectif très ambitieux compte tenu du cycle des évolutions technologiques, mais la capitalisation des différentes expériences réalisées sur le territoire national permettrait un état des lieux et mettrait en évidence les bonnes pratiques à partager. Enfin, l'évaluation périodique (constitution de challenges) à partir de cas d'usage simples par une entité « régalienne » pourrait constituer une piste d'évolution envisageable.

- **Des risques de contournement de la technologie**

Par expérience, dès l'émergence d'une nouvelle technologie, les plus ingénieux des opposants ou des délinquants s'emploient à inventer un moyen de s'y soustraire ou de la contourner. Il va de soi que la dissimulation du visage constitue une manière très facile de se soustraire à l'acquisition de la donnée essentielle : visage penché, capuche dans le domaine public, mais aussi, dans certains contextes particuliers, port du voile, de casque et de masque ...

Des expériences ont prouvé qu'il était parfois simple de leurrer un système de reconnaissance faciale lorsqu'il est utilisé comme contrôle d'accès. La présentation de faux visages (photographie 2D ou reproduction 3D de visages[22]) est également de nature à leurrer certains dispositifs, pour éviter le recours plus lourd aux traditionnelles pratiques de chirurgie esthétique.

Par ailleurs, la société israélienne D-ID a mis au point une solution qui protège les images et les vidéos contre les logiciels de reconnaissance faciale, démontrant ainsi qu'il est aujourd'hui possible de les contourner.

L'ensemble de ces techniques de contournement doivent faire l'objet de tests approfondis et réalisés par des organismes spécialisés afin de mesurer la robustesse du système de reconnaissance faciale face aux risques d'erreurs.

- **Des risques en matière de cyber sécurité**

Le vol de données est sans nul doute l'une des principales menaces qui visent les systèmes biométriques. De nombreux exemples de compromission sont régulièrement relayés sur Internet. En 2015, environ 5 millions d'empreintes digitales ont été dérobées par des hackers qui se sont introduits dans les systèmes de l'OPM (organisme en charge des fonctionnaires aux Etats-Unis). Plus récemment, un chercheur français en Cyber Sécurité, Elliot Alderson, a indiqué au gouvernement indien l'exposition sur Internet de plus de 300 000 données personnelles incluant les cartes d'identité Aadhaar contenant les données biométriques des citoyens indiens.

[22] En décembre 2018, une équipe du magazine Forbes a mis au point une technique consistant à fabriquer une reproduction 3D du visage d'une personne et à la présenter à plusieurs smartphones. Dans 4 cas sur 5, le leurre a permis de déverrouiller le smartphone.

L'impact est d'autant plus fort que, contrairement à un mot de passe qui aurait été subtilisé par un tiers malveillant, il n'est pas possible de modifier une donnée biométrique une fois qu'elle a été compromise. Même si une part significative des citoyens n'hésitent pas à afficher leur photographie dans la sphère publique via les réseaux sociaux, le vol d'une image constitue une atteinte à la vie privée des personnes, voire à leur sécurité dans certains contextes (divulgation de la photographie d'un agent des services secrets par exemple).

L'usage malveillant de données biométriques dérobées reste aujourd'hui limité ; néanmoins l'usurpation d'identité pourrait représenter une menace à l'avenir. De la même manière, un tiers malveillant pourrait remplacer les données biométriques de référence d'une personne enrôlée dans le système de reconnaissance faciale. En fonction du cas d'usage mis en œuvre, l'impact peut conduire à un accès non autorisé à un espace contrôlé, à la dissimulation d'une personne recherchée, etc. Les risques de déni de service (dispositif de reconnaissance faciale rendu volontairement inopérant) et de destruction volontaire ou accidentelle des données biométriques ne doivent pas non plus être négligés.

Au-delà des vulnérabilités intrinsèques liées à la technologie (dont la capacité de reconstitution de l'image d'une personne à partir des données caractéristiques biométriques obtenues par application de couches de réseaux de neurones sur l'image d'origine), son implémentation sur des systèmes informatiques présente également de nombreuses vulnérabilités techniques, organisationnelles dont les principales peuvent affecter tout ou partie de ses composants :

- Vulnérabilités dans le système d'acquisition : usurpation du capteur conduisant à l'injection de données biométriques volontairement erronées dans le dispositif ;
- Vulnérabilités dans le système de traitement d'image : manipulation frauduleuse de données durant le traitement ;
- Vulnérabilités dans le système de stockage, notamment la base de données (BDD) : accès non autorisé, modifications / suppressions non autorisées de données.

Face à ces menaces et vulnérabilités, il conviendra d'apporter une attention particulière à la conduite d'une analyse de risques du système de reconnaissance faciale et de mettre en place les mesures de Cyber Sécurité adaptées depuis la phase de conception jusqu'à la mise en production et la gestion sécurisée dans le temps du dispositif.

Parmi toutes les mesures envisageables, on retiendra quelques principes clés à respecter :

- Séparer le stockage des données biométriques de visage de celui des données d'identification des personnes concernées ;
- Privilégier, dès lors que le cas d'usage le permet, le stockage des données biométriques de visage sur un support détenu par la personne ;

- Eviter la duplication des données biométriques qui augmente les risques de leur exposition aux menaces et vulnérabilités : il faudra dans ce cas déployer plus d'efforts pour y apporter les réponses en termes de sécurité adaptées ;
- Mettre en place des mécanismes de chiffrement robustes, conformes aux pratiques les plus récentes et les plus exigeantes, afin de protéger les données biométriques dans toutes les étapes de leur traitement ;
- Ajouter un mécanisme de traçabilité et de non répudiation des usages réalisés dans le cadre du dispositif de reconnaissance faciale et apporter les moyens à une autorité tierce de vérifier qu'ils sont bien conformes à ceux définis initialement.

La norme ISO/IEC 24745:2011 (version draft), référence en matière de protection des données biométriques, décrit la démarche complète d'une mise en œuvre sécurisée et fiable des systèmes biométriques.

L'ANSSI propose également un ensemble de documents de recommandations en matière de sécurisation des systèmes d'information[23] dont celui relatif à la vidéoprotection[24]. Une mise à jour pourrait être envisagée pour ces systèmes de vidéoprotection, couplés à un dispositif de reconnaissance faciale.

A l'instar des hébergeurs de données de santé, la mise en place de procédures d'agrément d'un hébergeur de données biométriques de visage permettrait de valider sa capacité à protéger ces données contre tout risque de vol, d'altération ou de destruction.

La qualification par l'ANSSI des solutions de reconnaissance faciale, pour des besoins de sécurité, devrait également être envisagée.

Préconisations

→ Encourager et faciliter l'apprentissage de l'algorithme en permettant la constitution, à des fins de recherche et développement, de bases de données juridiquement exploitables

→ Centraliser et consolider les bonnes pratiques techniques encadrant le fonctionnement des dispositifs de reconnaissance faciale

[23] https://www.ssi.gouv.fr/entreprise/bonnes-pratiques

[24] https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/dispositifs-de-videoprotection/

B. L'acceptation par la population : les enjeux d'information et d'encadrement

Si l'efficacité de la reconnaissance faciale pour prévenir la commission d'infractions n'a pas encore été officiellement prouvée, les dispositifs mis en œuvre par certains Etats ayant jusqu'à aujourd'hui uniquement permis de reconstituer a posteriori les déplacements des auteurs d'attentats, mais non de les appréhender avant qu'ils ne passent à l'acte, la question de son déploiement en France est régulièrement abordée dès lors que le contexte et les circonstances s'y prêtent[25].

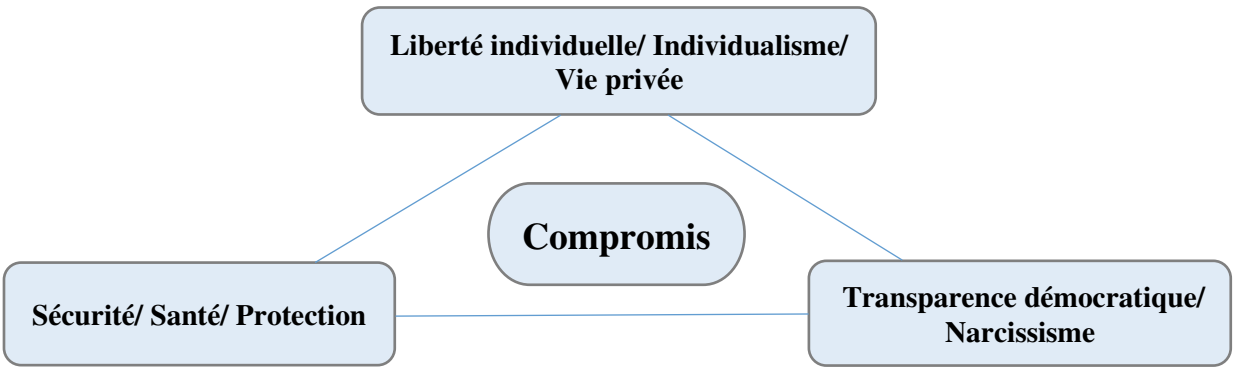
Aussi est-il nécessaire d'examiner sous quelles conditions la technologie de reconnaissance faciale pourrait participer au renforcement du contrôle auquel la population est susceptible d'aspirer dans un contexte sécuritaire.

1- L'accueil sociologique à géométrie variable des nouvelles technologies par les populations

Manifestement, la culture chinoise est plus encline à accepter une intrusion de surveillance de la vie privée que la culture française, très jalouse des libertés individuelles. Les pratiques présentées ci-avant inquiètent probablement à juste titre les Occidentaux, et les autorités publiques de certains pays ont déjà pris des mesures pour éviter ce « Big Brother technologique »[26]. Cependant, l'analyse sociologique montre une certaine ambivalence de nos contemporains vis-à-vis de ces technologies.

- **Des aspirations divergentes**

Selon J-.G. Ganascia, les Français sont partagés entre trois aspirations divergentes : la liberté individuelle, la sécurité et la transparence. C'est ce tiraillement, cette tension, que le sociologue a conceptualisé dans la notion de « *trilemme* ». Cette tension nécessite un état de compromis, d'équilibre, qui peut être schématiquement représenté par le triangle suivant :



[25] Cf. à titre d'illustration les récentes modifications législatives proposées en ce sens par MM. Ciotti et Karoutchi

[26] Projet de loi interdisant l'utilisation de la technologie de reconnaissance faciale dans toute la ville de San Francisco

Ce « *trilemme* » évolue selon les époques car les différentes notions qui constituent ces aspirations évoluent elles-mêmes au cours du temps. En cela, l'exemple de l'intimité est de ce point de vue éclairant.

- **Un rapport ambivalent à l'intimité**

Au XXI^{e} siècle, dans le domaine public, la ville est l'un des derniers refuges de l'intimité. L'individu contemporain ne trouve cette intimité, cet anonymat, que dans la cité. Néanmoins, le désir contemporain d'intimité est à nuancer et peut paraître ambivalent avec, d'une part, la recherche de l'anonymat dans les villes, et d'autre part, une expression de l'intime dans l'espace public de plus en plus prescrite comme valeur d'authenticité dans une société où l'intimité est surexposée. Emissions de télé-réalité, utilisation des réseaux sociaux : nos contemporains étalent massivement leur vie privée.

Selon le sociologue Dominique Cardon, nos contemporains n'hésitent pas à se montrer, pour témoigner de leur singularité, mais n'en sont pas moins soucieux de leur vie privée, dont ils désirent garder le contrôle. Cette idée est partagée par le psychiatre Serge Tisseron, qui considère que des personnes peuvent décider d'afficher une grande part de leur intimité, en particulier parce qu'elles se sentent libres d'arrêter à tout moment. En cela, il semble que l'acceptation de la reconnaissance faciale par la population exige que celle-ci puisse être désactivée dès lors que son usage n'est plus nécessaire.

- **Le potentiel impact de la reconnaissance faciale sur la vie mentale et sociale**

On peut également se demander en quoi les logiciels de reconnaissance faciale, aujourd'hui capables d'analyser nos émotions, sont susceptibles de changer notre vie mentale. En effet, selon Serge Tisseron, les émotions sur un visage traduisent les intentions d'une personne, lesquelles reflètent une partie de son âme. Dans ce cas, le logiciel pourrait les deviner, et le risque est que, dans les lieux publics, les personnes adoptent finalement des expressions neutres, sans émotion, pour se protéger. Cela conduirait à appauvrir la vie mentale des personnes, en devenant moins capables de percevoir de telles émotions chez elles et chez les autres, et pourrait *in fine* générer un encouragement à l'isolement et une mise en avant de la culture de l'apparence.

- **Une réticence générale mais des comportements contradictoires**

Les enquêtes sociologiques montrent en Occident (le cas de l'Asie est spécifique) une méfiance de plus en plus forte quant à l'utilisation de données personnelles par le biais des nouvelles technologies, notamment vis-à-vis des GAFAM. Selon Dominique Cardon, cette crainte s'est développée à partir de 2013 avec l'affaire Snowden. Auparavant, l'intrusivité des nouvelles technologies n'était pas réellement perçue par les utilisateurs, en dehors des publicités personnalisées qui donnent le sentiment d'être espionné et invitent à la déconnexion. La fondation Jean Jaurès a publié le 22 octobre 2018 un article de Maxime des Gayets et Chloé Morin « *Opinion, sensibilisation, manipulations... Le jeu faussé de la protection des données* », qui montre que si les Français sont de plus en plus réticents à laisser leurs données personnelles, ils adoptent cependant des comportements contradictoires.

Comme cela a été présenté *supra*, les contemporains arbitrent au sein du *trilemme*. Néanmoins, une quatrième aspiration (avantages divers…) peut donner lieu à des choix différents. Les particuliers eux-mêmes peuvent étaler leur vie privée, mais aussi celles de leurs proches, dans une volonté de narcissisme ou pour tirer des avantages pécuniaires. C'est ainsi que les personnes acceptent de laisser leurs données biométriques sur certains sites des GAFAM. Sur les sites d'achat en ligne, le fait de pouvoir bénéficier d'offres de réduction et de cadeaux est la première raison invoquée par les internautes acceptant de fournir des données personnelles (69 %, étude CSA mai 2018). Qualifiée de « braquage indolore » l'exploitation des données personnelles ne semble pas avoir de coût immédiat et aisément mesurable (en dehors de l'usurpation des coordonnées bancaires), et pourtant, les GAFAM exploitent ces données à des fins commerciales, qui peuvent donner lieu à de la surveillance.

Bien que certains des grands acteurs, qui incluent les GAFAM tels que Microsoft,[27] prennent des positions officielles sur les limitations qu'il conviendrait d'apporter à l'utilisation des technologies de reconnaissance faciale, les risques de dérive liés à une utilisation commerciale massive par les géants de l'internet restent latents. Cette question ne s'inscrivant pas dans le cadre d'une utilisation à des fins sécuritaires, elle ne sera pas davantage développée par le présent rapport.

2- Une tolérance grandissante aux dispositifs sécuritaires renforcés

- **Des populations moins réticentes aux lois restrictives de liberté**

Comme cela a été constaté pour le cas de la Chine, mais plus largement pour l'Asie, il semble qu'il existe une adhésion des habitants de certains pays pour une vie dans une société plus sûre, au prix d'un certain effacement de la liberté individuelle. Là se trouve, selon Dominique Wolton, le conflit entre l'intérêt de la société et l'intérêt de l'individu. En Occident aussi, on constate une tolérance grandissante aux dispositifs sécuritaires renforcés. Une première « encoche » dans les respects des libertés individuelles apparaît après les attentats du 11 septembre 2001, avec le *Patriot Act*, cette loi antiterroriste qui octroie d'importants pouvoirs aux services de sécurité, dont la détention sans limite et sans inculpation de toute personne soupçonnée de projet terroriste. Cette loi était d'abord considérée comme une loi d'exception dont les dispositions devaient initialement durer quatre ans. En juillet 2005, le Congrès a rendu permanentes 14 des 16 dispositions du texte. Après une longue bataille parlementaire au cours de l'hiver 2005-2006, la plupart des moyens accordés aux forces de l'ordre ont été pérennisés.

Bien que ce texte soulève depuis son adoption de vives critiques de la part des associations de défense des Droits de l'Homme et de juristes, qui dénoncent des atteintes aux libertés, il a été en vigueur jusqu'en juin 2015 et remplacé ensuite par le *Freedom Act*. Hormis quelques associations concernées par les droits fondamentaux, l'Amérique n'a pas combattu ce dispositif législatif pourtant liberticide par certains

[27] https://www.zdnet.fr/actualites/microsoft-ne-veut-pas-vendre-de-reconnaissance-faciale-sans-condition-39883653.htm

aspects. En France, la survenue des attentats de 2015 a soulevé la question d'un « *Patriot Act* à la française ». L'état d'urgence décrété par le Président de la République a constitué une première réponse pour assurer la protection des citoyens. Ce régime d'exception a été reconduit à plusieurs reprises avant d'être remplacé le 1er novembre 2017 par une loi antiterroriste qui inscrit certaines mesures de manière durable dans notre droit.

- **La « risquophobie » plaide pour une société de plus en plus protectrice**

Dans une étude sur la perception des risques (Académie des technologies, 2016), le sociologue Gérald Bronner et le physicien Étienne Klein ont décrit cette « risquophobie » actuelle, mère du principe de précaution. Les personnes présentent de plus en plus une aversion au risque et exigent des garanties maximales dans toutes leurs entreprises. Le temps des aventuriers est-il révolu ? Peut-on progresser sans prendre de risque ? Cette aversion au risque trouve un écho dans les aspects sécuritaires, avec une demande accrue de sécurité. Conséquence paradoxale de cette « risquophobie » : il semble que plus un pays est sûr, plus les exigences de sécurité augmentent, quitte à restreindre davantage certaines libertés. Les populations occidentales estiment probablement que dans un État démocratique occidental, le risque d'atteinte aux libertés publiques reste finalement faible et peut toujours être contrôlé par la représentation parlementaire. En revanche, ce risque d'atteinte aux libertés publiques, à la vie privée, est davantage présent dans les entreprises, qui peuvent utiliser des données personnelles ayant trait à la vie privée.

En conséquence, si la population semble prête, pour renforcer sa sécurité, à accepter le recours à de nouveaux moyens technologiques (tels que la reconnaissance faciale), alors qu'ils sont particulièrement intrusifs au regard de la vie privée, les dangers qu'engendrerait un usage permanent, potentiellement insidieux de ce type de dispositifs nécessitent qu'ils ne puissent être activés que dans des contextes particuliers, de manière proportionnée, limitée dans le temps, et en toute transparence pour les personnes. A défaut, le risque serait de voir s'évanouir des pans de liberté, vraisemblablement sans retour en arrière possible.

3- L'exigence d'information et de communication : une condition indispensable de l'acceptation

Le constat des très nombreuses craintes générées par la reconnaissance faciale pourrait probablement trouver une partie de réponse dans l'information, la communication et le dialogue qui devraient entourer, et surtout précéder toute mise en œuvre de ces typologies de dispositif. Cela serait particulièrement vrai pour l'espace public, où les réticences et appréhensions sont les plus importantes. A titre d'exemple, il devrait être envisagé de soumettre l'adoption d'un cadre juridique dédié à certains mécanismes de débats démocratiques existants tels qu'un débat public et/ou la mise en place d'une mission d'information parlementaire.

4- Une démarche de mise en œuvre graduée pour une meilleure acceptation

Dans ce contexte de défiance et de réticence, et face à des technologies qui ne sont pas encore arrivées à maturité, il ne peut pas être envisagé de déployer de manière massive la reconnaissance faciale. L'approche doit être progressive dans un souci de pédagogie et afin de répondre à plusieurs objectifs :

- Permettre aux industriels d'améliorer la fiabilité de leurs solutions, notamment dans des situations environnementales moins favorables ;
- Enrichir les bonnes pratiques d'utilisation et d'implémentation de ces technologies au fur et à mesure de leur mise en œuvre ;
- Expliquer, informer et démontrer la valeur ajoutée durable de ces dispositifs et leurs capacités à soutenir et accompagner les évolutions sociétales.

Poussée par un effet de mode, la mise en œuvre de la reconnaissance faciale pâtit parfois d'un manque de réflexion en amont sur la stratégie et l'organisation à mettre en place pour qu'elle se transforme en succès. On constate qu'il y a défiance dès lors que la destination d'un dispositif n'est pas claire ou connue. Il apparaît donc indispensable de bien définir, avant toute mise en œuvre d'un système de reconnaissance faciale, les objectifs visés, les gains attendus, la manière de les mesurer et les moyens organisationnels à prévoir pour traiter efficacement les informations qu'il génère.

Préconisations

→ Organiser / susciter un débat public et/ou une mission d'information parlementaire sur les risques et enjeux liés à la reconnaissance faciale dans l'espace public

→ Garantir une information claire et transparente des personnes concernées s'agissant notamment des espaces soumis à un dispositif de reconnaissance faciale

→ Prévoir une méthodologie de mise en œuvre graduée

C. La nécessité d'un cadre juridique dédié : les évolutions indispensables

1- Faciliter la faisabilité juridique des expérimentations

L'étude du cadre juridique existant révèle l'absence de dispositions légales et/ou règlementaires spécifiques dédiées aux expérimentations de technologies nouvelles. Les traitements de données à caractère personnel impliqués par la mise en œuvre de telles technologies sont à ce jour soumis aux mêmes obligations juridiques que les traitements qui seraient engagés à long terme ou sur une période indéterminée. Tel qu'indiqué ci-avant, les traitements de données à caractère personnel de type biométriques, par principe prohibés, ne connaissent pas non plus de dérogation particulière en matière d'expérimentation.

Il est ressorti de nombreux entretiens menés tant auprès d'industriels, notamment les sociétés Idemia et Digital Barriers, que d'acteurs clés tels que la SNCF, la nécessité de pouvoir mener plus souvent et régulièrement des expérimentations permettant de tester l'efficacité de solutions technologiques impliquant l'utilisation de données à caractère personnel, et notamment de données biométriques s'agissant des outils de reconnaissance faciale. L'objectif serait double : d'une part, de permettre aux algorithmes mis en œuvre par les logiciels de s'enrichir et s'améliorer, et d'autre part, de bénéficier de retours d'expérience concrets lors de l'implémentation de tels outils.

Par deux délibérations, respectivement du 10 décembre 2015 et du 30 juin 2016, la CNIL a autorisé la société Aéroports de Paris (ADP) à mettre en œuvre un traitement de données à caractère personnel biométriques, à des fins d'expérimentation de technologies de reconnaissance faciale. Dans les deux cas, l'autorité administrative a limité l'émission de cette autorisation au seul cadre expérimental. La délibération du 30 juin 2016 mentionnait notamment : « *si, à l'avenir, il était envisagé de déployer un tel système, la Commission examinerait avec attention la proportionnalité du dispositif projeté au regard de la finalité recherchée et des risques majeurs portant sur la liberté d'aller et venir anonymement et plus généralement sur les libertés individuelles.* »

L'expérience rendue possible par cette dernière autorisation consistait notamment en l'installation d'un logiciel de reconnaissance faciale sur l'exploitation du flux provenant de caméras déjà installées dans le cadre du système de vidéoprotection des aérogares d'Orly et de Roissy-Charles de Gaulle. Ces caméras, installées à certains points de passage des aérogares, permettaient donc un traitement de données biométriques concernant non seulement des salariés volontaires et consentants de l'entreprise pour participer à l'expérimentation, mais également d'autres personnes circulant dans l'aéroport. A ce titre, la CNIL a rappelé dans son autorisation les conditions juridiques indispensables en matière de protection des données personnelles que l'expérimentation devait respecter pour être valablement mise en œuvre (notamment, l'information préalable des personnes concernées, l'existence d'une alternative à ces points de passage entrant dans le champ de l'expérimentation, mais également la « suppression immédiate » des

données biométriques, appelées « gabarits », concernant les personnes non volontaires passant dans le champ des caméras).

Depuis l'entrée en vigueur du RGPD, le 25 mai 2018, la CNIL ne délivre plus d'autorisations que dans certains domaines spécifiques. Si l'autorité peut toujours, voire doit, dans certains cas, être consultée sur ce type de sujets, notamment sur la base des études d'impact réalisées par les responsables de traitement eux-mêmes, elle ne peut s'opposer a priori à leur implémentation. C'est notamment ce qu'elle a fait s'agissant de l'expérimentation mise en œuvre par la police municipale de Nice lors du Carnaval de la ville au mois de février 2018. Ici encore, la CNIL avait recommandé le respect de l'ensemble des exigences légales et règlementaires applicables aux traitements de données à caractère personnel et plus particulièrement biométriques.

Si, dans ces différents cas de figure, l'expérimentation a pu être mise en œuvre, il ressort que la possibilité de tester l'efficacité des dispositifs de reconnaissance faciale dans des contextes factuels réalistes et notamment parmi des foules, reste considérablement limitée et contrainte. A ce titre, il apparaît utile de considérer l'élaboration d'un cadre juridique dédié encadrant spécifiquement les expérimentations. En effet, si les traitements de données à caractère personnel à des fins d'expérimentation peuvent être mis en œuvre sur la base de l'intérêt légitime du responsable de traitement, il en est autrement lorsqu'il est question de données à caractère biométrique. En application de l'article 9 du RGPD, les Etats membres de l'Union Européenne sont en mesure de prévoir des conditions supplémentaires dans le cadre desquelles les traitements de données biométriques pourraient être réalisés.

A ce titre, il semblerait pertinent de permettre et d'encadrer, sous la forme d'un décret, les traitements de données à caractère personnel biométriques, à des fins d'expérimentation de technologies nouvelles. Les typologies de technologies seraient précisément définies par le texte réglementaire et incluraient la reconnaissance faciale. Il serait également envisageable que le texte règlementaire soit limité aux seuls traitements mis en œuvre à des fins de reconnaissance faciale.

Le texte pourrait notamment établir :

- Les conditions relatives aux cas d'usage précis dans le cadre desquels l'expérimentation pourra être menée : par exemple des grands évènements, complexes sportifs, sites privés ouverts au public à enjeux sécuritaires importants ;
- Les conditions matérielles dans le cadre desquelles les expérimentations devront être mises en œuvre : notamment, la durée maximale de l'expérimentation, le nombre de personnes concernées ;
- Les conditions spécifiques relatives au traitement de données qui devront être respectées en lieu et place des exigences légales et règlementaires applicables (RGPD, Loi « Informatique et Libertés ») : notamment, la durée de conservation des données, les modes d'information des personnes concernées, le caractère facultatif du traitement ;

- Les exigences de sécurité matérielles et techniques qui devront être mises en œuvre dans le cadre de l'implémentation des technologies expérimentées.

Conformément aux dispositions de l'article 27 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, un décret en Conseil d'Etat, pris après avis de la CNIL, pourrait autoriser le déploiement expérimental dans certaines situations prédéterminées de logiciels de reconnaissance faciale.

Il devrait également être prévu qu'un bilan d'utilisation soit élaboré et publié par l'entité ayant mis en œuvre l'expérimentation afin de permettre, à terme, la mutualisation des bonnes pratiques.

Pour aller plus loin et encadrer davantage les conditions de mise en œuvre de ces expérimentations dans le respect de la protection des données personnelles et de la vie privée, la CNIL pourrait également publier un règlement type à l'instar de celui publié le 28 mars 2019 s'agissant de la biométrie sur les lieux de travail.

2- Prévoir un texte national spécifique dans le cadre de l'article 3 de la Directive Police-Justice (UE) 2016/680

Le 27 avril 2016, la Directive européenne dite « Police-Justice » relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes[28] à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données a été adoptée.

A l'instar du RGPD, la Directive proscrit par principe le traitement de données à caractère personnel de type biométrique. Le texte européen conditionne l'utilisation de ces données par les autorités compétentes « *uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :*

a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre;

b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; ou

c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée. »

Prise à des fins de transposition nationale de la Directive « Police-Justice », les dispositions de la loi « Informatique et Libertés » prévoient que « *Le traitement de données [biométriques]est possible uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et soit s'il est autorisé par une disposition législative ou réglementaire, soit s'il*

[28] L'article 70-1 de la loi « Informatique et Libertés » modifiée définit une autorité compétente comme *« toute autorité publique compétente ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique ».*

vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée »[29].

Dans le prolongement de la volonté européenne, et sans aller plus loin, le législateur français s'est laissé la possibilité de venir encadrer précisément, par un texte dédié, le traitement de données biométriques dès lors que celui-ci est mis en œuvre par des autorités compétentes et à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

S'agissant de la reconnaissance faciale, la donnée biométrique concernée serait constituée du gabarit biométrique calculé par un logiciel de reconnaissance faciale sur la base de l'image (vidéo ou photographie) de la personne concernée. Dès lors, il semblerait inopportun de considérer que cette donnée a été manifestement rendue publique par la personne quand bien même l'image proviendrait par exemple d'une vidéo prise sur la voie publique ou d'une photographie postée publiquement en ligne. Il convient en effet de relever que la donnée biométrique est constituée par le gabarit biométrique établi à partir de l'image et n'est pas l'image elle-même.

La mise en œuvre d'un dispositif de reconnaissance faciale, impliquant le traitement de données biométriques, devrait donc nécessairement, au-delà du respect des exigences de nécessité absolue et de la mise en œuvre de garanties appropriées, faire l'objet d'un texte législatif ou règlementaire dédié, et ce, y compris afin de permettre l'utilisation de dispositifs de reconnaissance faciale, dans le cadre d'enquêtes et de poursuites judiciaires par les autorités compétentes, bénéficiant de l'exercice de l'autorité publique et des prérogatives de puissance publique.

A ce titre, il conviendrait d'envisager, dans le cadre de la mise en application de la Directive « Police-Justice », qu'un texte législatif, soumis à l'étape préalable du débat démocratique, vienne encadrer les cas et situations dans lesquels les autorités compétentes seraient autorisées à utiliser des technologies de reconnaissance faciale.

Les finalités des traitements de données biométriques devraient être précisément définies par le texte ainsi que les modalités de déclenchement des dispositifs par une autorité (exemples : préfet, magistrat). Il pourrait être notamment prévu de limiter les périodes d'utilisation en termes de durée mais également d'un point de vue géographique :

- utilisation ne pouvant par exemple dépasser une période de trente jours, et prévoyant un nombre d'heures maximum en continu et des pauses obligatoires ;
- lieux particulièrement sensibles et points de passage : gares, aéroports, transports en commun, zones à risques ou récemment impactées par un évènement (par exemple un attentat).

[29] Cf. art. 70-2 de la loi du 6 janvier 1978 modifiée

L'intégration d'un contrôle humain du dispositif et la seconde validation d'une identification pourraient également être une piste opérationnelle à envisager et à intégrer comme une obligation légale.

Le texte pourrait également prévoir de s'appliquer non pas uniquement aux forces de sécurité intérieure, mais également aux services internes de sécurité[30] tels que ceux de la SNCF, de la RATP, d'ADP ou de tout espace privé ouvert au public pertinent. C'est notamment dans ce sens que Monsieur le Préfet Renaud Vedel, Coordonnateur ministériel en matière d'intelligence artificielle, abonde, en soutenant également qu'il pourrait être envisagé de constituer un fichier permanent de données biométriques qui ne serait activé que sur des périodes temporaires déterminées, dans des contextes prévus ou sur des zones particulièrement exposées.

Le texte législatif dédié pourrait également prévoir que les dispositifs de reconnaissance faciale, qui seraient mis en œuvre par les autorités compétentes dans le cadre du texte législatif dédié, ne pourraient être utilisés que sur la base d'un fichier de photographies de personnes constitué et centralisé par le Ministère de l'intérieur. Les conditions d'élaboration et d'utilisation de celui-ci devraient être contrôlées par une autorité administrative indépendante.

Enfin, il pourrait être prévu de prédéfinir les dispositifs utilisables en application du texte législatif afin de garantir un niveau minimum en termes d'efficacité mais également de cyber sécurité.

Préconisations

→ Prévoir un cadre juridique dédié, par un décret en Conseil d'Etat pris après avis de la CNIL, encadrant les traitements de données à caractère personnel mis en œuvre à des fins d'expérimentation

→ En application de la Directive « Police-Justice », créer un cadre légal dédié et précis permettant aux autorités compétentes de mettre en œuvre des dispositifs de reconnaissance faciale à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales

→ Envisager la constitution d'un fichier, créé et mis à disposition par le Ministère de l'Intérieur, dédié à une utilisation par les autorités compétentes et limité à des cas d'usage déterminés (points de passage stratégiques (gares, aéroports), manifestations, grands évènements) et pour une activation temporaire

[30] « Services internes de sécurité » au sens de l'article L611-1 du Code de la sécurité intérieure

Conclusion

Le constat qui ressort des travaux d'investigation et d'analyse mis en œuvre dans le cadre de l'élaboration du présent rapport semble être l'inévitable développement et la démocratisation de la technologie de reconnaissance faciale ; cela à l'échelle internationale. La France dispose dans son écosystème industriel de pépites technologiques qui peinent à obtenir des références commerciales sur le territoire national et pâtissent de ce qui peut être considéré comme une distorsion administrative et réglementaire au regard d'autres pays.

Si l'efficacité réelle en termes de sécurité de cette technologie ne fait aujourd'hui l'objet d'aucun retour d'expérience officiel, il ressort de la présente étude que l'insuffisance d'expérimentations sur le territoire national en est très certainement l'une des causes. La technologie, elle, n'en est plus à ses débuts et les algorithmes ont en revanche démontré leur efficience.

Compte tenu des enjeux en termes de souveraineté, il semble important que la France puisse occuper une place de choix dans ce challenge technologique mondial afin de :

- bénéficier des emplois et ressources associés à ce marché porteur ;
- disposer d'une technologie totalement maitrisée pour les déploiements à forte connotation sécuritaire ou souveraine ;
- rester dans la compétition sécuritaire et technologique afférente à l'organisation de grands événements planétaires (Coupe du monde de rugby 2023, Jeux Olympiques 2024, etc.).

Au centre de cette démarche, la préservation des intérêts fondamentaux des citoyens, et notamment de leurs libertés individuelles et de leur vie privée, doit en rester le fil conducteur.

Il semble nécessaire de mettre en œuvre au plan national une stratégie graduée, structurée et explicitée autour de déploiements non contestables. Cette stratégie pourrait en particulier s'appuyer sur :

- la construction d'un compromis social fondé sur la transparence et la pédagogie vis-à-vis des citoyens, présentant les enjeux et les objectifs sécuritaires, excluant explicitement toute surveillance de masse ;
- une adaptation du cadre juridique actuel, notamment pour faciliter les expérimentations, permettre et encadrer légalement l'utilisation de la technologie par les autorités compétentes ;
- le soutien aux industriels français pour l'émergence d'une solution adaptée aux activités régaliennes ;
- une montée en puissance progressive et maîtrisée du déploiement des solutions de reconnaissance faciale :
    - au sein des sites privés à forts impératifs sécuritaires comme les Secteurs d'Activité d'Importance Vitale ;

- par les autorités compétentes, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces :
    - pour la sécurisation de grands événements (avec des objectifs et des finalités clairement énoncés et indiscutables du point de vue de la sécurité) ;
    - ponctuellement dans le domaine public dans le cadre d'opérations anti-terroristes, pour des points stratégiques du point de vue du contrôle des flux.

Synthèse des préconisations

Préconisation n°1 : Faire accepter par la population un potentiel déploiement de la reconnaissance faciale sur le territoire national

Si la question de la sécurité semble toujours avoir été au cœur des préoccupations de la population résidant sur le territoire français, la menace terroriste actuelle a sans aucun doute renforcé cet état de fait. Aussi, plusieurs législations sont-elles venues dernièrement consolider, sur le plan juridique, l'arsenal des moyens mis à la disposition des autorités publiques compétentes pour assurer sa protection. Pour autant, l'heure ne paraît pas être celle de l'abandon de pans de libertés fondamentales, au nombre desquelles d'aucuns considèrent que figure la liberté d'aller et venir anonymement dans l'espace public, au bénéfice d'un Etat sûr. Aussi, l'un des défis majeurs à relever consiste à faire comprendre à la population le bénéfice que peut apporter l'implémentation, sous certaines conditions, de dispositifs de reconnaissance faciale.

→ Organiser/ susciter un débat public et/ou une mission d'information parlementaire sur les risques et enjeux liés à la reconnaissance faciale dans l'espace public.

Compte tenu des conséquences qui peuvent être celles de l'installation en nombre de dispositifs de reconnaissance faciale dans l'espace public, en particulier sur la vie privée des personnes qui y circulent, il paraît important que cette question fasse l'objet d'un débat et que l'opinion la plus large s'en saisisse afin de fixer le cadre de notre société de demain. Il pourrait par exemple être envisagé qu'une mission parlementaire *ad hoc* soit créée et que les résultats de ses travaux soient soumis à consultation publique.

→ Garantir une information claire et transparente des personnes concernées, s'agissant notamment des espaces soumis à un dispositif de reconnaissance faciale.

Les dispositifs de reconnaissance faciale sont, dans l'espace public, adossés aux systèmes de vidéoprotection. S'ils peuvent permettre de rechercher dans une foule une personne déterminée, ils supposent toutefois la mise en place d'une surveillance généralisée, à laquelle il est difficile de se soustraire, sauf à être précisément informé des espaces géographiques et périodes où ils sont opérationnels. En conséquence, afin d'écarter toute suspicion d'observation permanente, il est préconisé de mettre en place une information efficiente.

Préconisation n° 2 : Permettre le développement d'une technologie sûre et efficace

Les travaux menés dans le cadre de cette analyse démontrent que l'industrie française spécialisée en matière de reconnaissance faciale semble souffrir d'un manque d'expérimentations *in situ,* qui résulterait de contraintes réglementaires, et qui la ferait ainsi pâtir de retards préjudiciables sur le terrain de la compétitivité internationale. En conséquence, il conviendrait d'adopter des mesures de nature à permettre aux industriels nationaux, qui bénéficient d'une réputation d'excellence en la matière, de poursuivre le développement et les performances de cette technologie.

→ Encourager et faciliter l'apprentissage des algorithmes en permettant la constitution, à des fins de recherche et développement, de bases de données juridiquement exploitables.
Les algorithmes devant être régulièrement entraînés à partir d'images de visages variés, provenant d'origines différentes, les industriels devraient avoir la faculté de constituer et d'utiliser des bases de données à des fins uniques de recherche et développement.

→ Centraliser et consolider les bonnes pratiques techniques encadrant le fonctionnement des dispositifs de reconnaissance faciale.
A défaut d'une normalisation des dispositifs de reconnaissance faciale, dont le risque serait d'être trop vite obsolète au vu de leurs évolutions technologiques, il serait utile de parvenir à une mutualisation des bonnes pratiques, fondées sur les enseignements tirés des différentes expérimentations réalisées, le cas échéant sous l'autorité d'une entité régalienne.

Préconisation n°3 : Faire évoluer le cadre juridique actuel

→ Prévoir un cadre juridique dédié, par un décret en Conseil d'Etat pris après avis de la CNIL, encadrant les traitements de données à caractère personnel mis en œuvre à des fins d'expérimentation.
Qu'il s'agisse de la mise en œuvre de dispositifs de reconnaissance faciale à titre expérimental ou de manière pérenne, le cadre juridique à respecter et les obligations qui incombent aux responsables de traitements sont les mêmes. L'exigence de devoir tester les performances de ces traitements de données à caractère personnel nécessiterait qu'un cadre juridique (par ex. décret en Conseil d'Etat pris après avis de la CNIL) le permette sous certaines conditions (situations de déploiement prédéterminées, bilan d'expérimentation, etc.).

→ En application de la Directive « Police-Justice », créer un cadre légal dédié et précis permettant aux autorités compétentes de mettre en œuvre des dispositifs de reconnaissance faciale à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

Le déploiement de dispositifs de reconnaissance faciale ne paraît pouvoir être envisagé sans une démarche progressive, de nature à gagner la confiance de la population, convaincue de la fiabilité et de l'efficacité de cette technologie. Ces conditions, qui ne sauraient faire l'impasse d'un débat démocratique, seraient propices à l'adoption par le législateur d'un cadre juridique définissant les circonstances, et les modalités selon lesquelles ces traitements de données biométriques pourraient être déclenchés par les autorités compétentes.

→ Envisager la constitution d'un fichier, créé et mis à disposition par le Ministère de l'Intérieur, dédié à une utilisation par les autorités compétentes et limité à des cas d'usage dédiés (points de passage stratégiques tels les gares et les aéroports, manifestations, grands événements) et pour une activation temporaire.

Tant au regard de la nécessité, d'un point de vue technique, de disposer de photographies de qualité, afin de constituer une base de données de références fiables, que d'un point de vue juridique, de lever toute difficulté quant à la possibilité de les utiliser à des fins de reconnaissance faciale, la création d'un fichier spécifique, placé sous l'autorité du Ministère de l'Intérieur, semble souhaitable.

Lexique

Algorithme : description de la suite finie et non ambigüe d'étapes ou d'instructions permettant d'obtenir un résultat à partir d'éléments fournis en entrée, exprimées en langage informatique. Certains algorithmes ont été conçus de sorte que leur comportement évolue dans le temps, en fonction des données qui leur ont été fournies. Ces algorithmes « auto-apprenants » relèvent du domaine de la recherche des systèmes experts et de l'intelligence artificielle.

Données biométriques : (extrait RGPD - Article 4-14) données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

Pour être exploitables ces caractéristiques doivent êtres UNIVERSELLES (utilisables pour tous) UNIQUES (distinguer sans équivoque) INVARIABLES (stabilité dans la durée) ENREGISTRABLES (pour permettre la collecte) MESURABLES (pour permettre la comparaison).

Données à caractère personnel : (extrait RGPD - Article 4-1) toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données sensibles : (CNIL) informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou la vie sexuelle, ou l'orientation sexuelle d'une personne physique.

Intelligence artificielle : programme informatique visant à effectuer, au moins aussi bien que des humains, des tâches nécessitant un certain niveau d'intelligence (Mission Villani 2018) – définition du scientifique Marvin LEE MINSKY « science qui consiste à faire faire aux machines ce que l'homme ferait moyennant une certaine intelligence ».

Vidéoprotection : Les dispositifs dits de « vidéoprotection » filment la voie publique et les lieux ouverts au public et sont soumis aux dispositions du Code de la sécurité intérieure (CSI).

Vidéosurveillance : les dispositifs dits de « vidéosurveillance » concernent les lieux non ouverts au public (locaux professionnels tels que des bureaux ou les réserves de magasins) et sont soumis à la législation relative à la protection des données (le RGPD, la loi du 6 janvier 1978 « Informatique et libertés » modifiée).

Sigles

ANSSI : Agence nationale de la sécurité des systèmes d'information

CNIL : Commission nationale de l'informatique et des libertés

DINSIC : Direction interministérielle du numérique et du système d'information et de communication de l'État

GAFAM : Google, Apple, Facebook, Amazon, Microsoft

RGPD: Règlement général européen sur la protection des données personnelles

CSI : Code de la sécurité intérieure

Annexe 1 : Personnes rencontrées

Jean-Marie BAILLY *Président de la société AQUILAE*

Francis BENSOUSSAN *Vice-Président de la société ALCEA*

Sandra BERTIN *Directrice de Police municipale – Ville de Nice*

Emmanuel BONGIOVANI *Responsable produit SAFEZONE - DIGITAL BARRIERS*

Thomas CAMPEAUX *Directeur des Libertés Publiques et des Affaires Juridiques (DLPAJ) - Ministère de l'intérieur*

Didier CANNESSON *Responsable comptes publics France - IDEMIA*

Dominique CARDON *Professeur de sociologie – Directeur du Médialab de Sciences Po*

Laurent CARO *Directeur Grands comptes stratégiques Europe du Sud Société AXIS*

Frédéric CUPILLARD *Responsable Avant-vente – DIGITAL BARRIERS*

Franck CURINGA *DSSI/ Pôle vidéo protection – Métropole Nice Cote d'Azur*

Philippe DALBAVIE *Conseiller juridique du Préfet de Police de Paris*

Pascal FALLET *Directeur Europe – IDEMIA*

Philippe FAURE *Vice-président Live Face Identification and Video Analytics – GEMALTO*

Gilles FURIGO *Contrôleur général - Délégation interministérielle aux Jeux Olympiques 2024 (DIJOP)*

Xavier FERRY *Directeur Commercial – KOMANCHE* et *Président Directeur Général de FRENCH SHIELD*

Jean-Gabriel GANASCIA *Professeur d'informatique, Président du comité d'éthique du CNRS*

Martin GAUTHIER *Direction des Opérations - Aéroport de Paris (ADP)*

Philippe GENDREAU *Délégué Général Adjoint Sécurité du Groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres (GICAT)*

Mattéo GUILLAUME *Représentant Thomas COLLOMB - COJO Paris 2024*

Christophe JAFART *Chef de projet Vidéo Protection - Aéroport de Paris (ADP)*

Laurent JULIERI *Responsable Reconnaissance Faciale - DIGITAL BARRIERS*

Dominique LEGRAND *Président de l'Association Nationale de Vidéo protection (AN2V)*

Armelle LE HIRE *Responsable Sûreté – SNCF/Gares et connexions*

Eric MARCIANO *Directeur développement de la société ALCEA*

Denis PERRAUD *Chef du département audio-vidéo du Pôle central d'analyses des traces technologiques – Service Central de la Police Technique et Scientifique à Ecully*

Eric PIVOT *Directeur de l'Innovation - Aéroport de Paris (ADP)*

Véronique POULLOT *Responsable du pôle Sûreté, vidéo et sociétal - SNCF, Gares et connexions*

Colonel Michel SANS *Coordination Nationale pour la Sécurité des Jeux (CNSJ)*

Elisabeth SELLOS-CARTEL *Adjointe au Préfet de la DCS, en charge de la vidéo protection - Ministère de l'Intérieur / Délégation à la Coopération de Sécurité*

Serge TISSERON *Psychiatre, Membre de l'Académie des Technologies*

Eric VAUTIER *Responsable de la sécurité des systèmes d'information - Aéroport de Paris (ADP)*

Renaud VEDEL *Préfet / coordonnateur ministériel en matière d'intelligence artificielle / Ministère de l'Intérieur*

Dominique WOLTON *Sociologue, Directeur de recherche au CNRS*

Annexe 2 : Bibliographie

Ouvrages :

CHAARI Anis : «*Classification et reconnaissance des images de visages - Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée* », Editions universitaires européennes 2014

HENNETTE-VAUCHEZ Stéphanie : « *Droits de l'homme et libertés fondamentales* », Dalloz 2017

GATES Kelly A. « *Our biometric future – Facial recognition technology and the culture of surveillance*», NYU Press 2011

MARLET Richard : *« Les experts entrent en scène – La révolution de la science criminelle »*, First Document 2017

MUCCHIELLI Laurent : « V*ous êtes filmés ! Enquête sur le bluff de la vidéosurveillance* », Armand Colin 2018

SZTULMAN Marc : « *La biométrie saisie par le droit public, étude sur la l'identification et la localisation des personnes physiques* », LGDJ 2019

TARKA Bérangère : « *L'utilisation de la reconnaissance faciale – Quelle force probante dans le cadre d'expertises judiciaires ?* » Editions universitaires européennes 2014

TÜRK Alex : « *La vie privée en péril, des citoyens sous contrôle* », Editions Odile Jacob 2011

Articles, Dépêches, Etudes, Rapports, Revues :

O1.NET *« Cinq questions pour tout savoir sur le fichier qui recense l'ensemble des Français »* Gilbert KALLENBORN | 27/10/2018

AFP : « *Controversée, la reconnaissance faciale s'invite partout au CES de Las Vegas* » | 11/01/2019

ATLANTICO : « *Reconnaissance faciale : pourquoi vous ne soupçonnez pas à quel point la technologie qui permet vos selfies va révolutionner le monde* » | 10/01/2019

CNIL : « *Photos et reconnaissance faciale dans la vie numérique : quels usages et quels enjeux pour demain ?* », lettre innovation et prospective n° 4 | mars 2013

COUR DES COMPTES : « *L'organisation et la gestion des forces de sécurité publique* », rapport public 2011, disponible en ligne

CREOGN, « *Numérisation du visage : opportunités et limites de la reconnaissance faciale* », note numéro 18 | Avril 2016

FAIRMAKIT *« Intelligence artificielle et marketing : pourquoi on doit se poser des questions d'éthique »* Volha Litvinets | 28/12/2019

FRANCE.TV – ActualitésTech « *Faut-il voir la reconnaissance faciale d'un mauvais œil ?* » | 27/02/2019

GROUPE DE TRAVAIL G29, Avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles adopté le 22 mars 2012, disponible en ligne

LES ECHOS : « *Vidéoprotection : jusqu'où iront les villes* », 9 janvier 2019 ; « Souriez, l'algorithme vous dévisage » | 8/03/2019

LES ECHOS « *La reconnaissance faciale, nouvel eldorado du transport aérien* » Bruno Trévidic | 11/02/2019

LES ECHOS « *Reconnaissance faciale : Google et Microsoft appuient sur le frein* » Lucas Mediavilla | 14/12/2018

Le FIGARO « *Moscou devient la vitrine de la reconnaissance faciale* » Pierre Avril | 16/01/2019

LE FIGARO : « *Le visage, nouvelle carte d'identité* » | 08/04/2019

LE MONDE « *L'Etat de droit mute doucement vers une forme ultra-sécuritaire* » | 06/11/2018

LE MONDE : « *Le manque de femmes dans l'intelligence artificielle accroît le risque de biais sexistes* » | 3 mars 2019

LIBERATION : « *L'empire du signal, ou les dangers d'un contrôle social par les corps* » | 25 avril 2019

DE MAISON ROUGE Olivier, « *L'identification biométrique et la sécurité publique* – observations sous CE | 18 octobre 2018, n° 404996, Dalloz IP/IT 2019 p. 175

NEXT IMPACT « *Reconnaissance faciale : Microsoft veut un code de conduite et annonce six principes* » | 07/12/2018

NODE-LANGLOIS Fabrice : « *Faut-il interdire la reconnaissance faciale* ? » Le Figaro, Champs libres |16 avril 2019

SIÈCLE DIGITAL « *La reconnaissance faciale : un risque pour les libertés individuelles ?* » Elise Dufour | 01/08/2018

SIÈCLE DIGITAL « *Reconnaissance faciale offre des données pour réduire les biais* » Philippe COLL | 19/02/2019

TOM.TRAVEL *« Heathrow s'équipe du plus important dispositif biométrique de l'industrie »* Hugo Pellegrin | 18/10/2018

ZDNET *« Amazon propose 5 règles pour encadrer la reconnaissance faciale* » Stéphanie Condon | 08/02/2019

ZERO DAY « *Chinese company leaves Muslim-tracking facial recognition database exposed online* » Catalin Cimpanu | 14/02/2019

Sitographie :

www.cnil.fr

www.euractiv.fr/section/politique/news/ la reconnaissance faciale s'impose peu à peu dans la course à la sécurité, 19 octobre 2017

https://www.thalesgroup.com/fr/worldwide/securite/case-study/mexico-le-programme-de-securite-urbaine-le-plus-ambitieux-du-monde Mexico - MàJ Mars 2017

https://actualites.pole-tes.com/ami-securite-jo2024-appel-flash-anr/ Le COFIS (Comité Stratégique de Filière Industries de Sécurité) lance, à partir du 5 mars 2019, quatre appels à manifestation d'intérêt pour la sécurité des JO Paris 2024

www.aiforhumanity.fr : Rapport de la Mission parlementaire du 8 septembre 2017 au 8 mars 2018 confiée par le Premier ministre Edouard Philippe à M. Cédric VILLANI : « *Donner un sens à l'intelligence artificielle – Pour une stratégie nationale et européenne »,* Mars 2018