RECONNAISSANCE FACIALE

POUR UN DEBAT À LA HAUTEUR DES ENJEUX

La reconnaissance faciale est de plus en plus présente dans le débat public au niveau national, européen et mondial et soulève en effet des questions inédites touchant à des choix de société. C'est pourquoi la CNIL avait appelé, en 2018, à un débat démocratique sur ce sujet, ainsi que plus largement sur les nouveaux usages de la vidéo. Elle souhaite aujourd'hui contribuer à ce débat, en présentant les éléments techniques, juridiques et éthiques qui doivent selon elle être pris en compte dans l'approche de cette question complexe.

Introduction **2**

I - La reconnaissance faciale : de quoi parle-t-on exactement ? **3**

1. La reconnaissance faciale est une technologie biométrique de reconnaissance des visages 3
2. La reconnaissance faciale n'est pas synonyme de vidéo « intelligente » 4
3. Derrière « la » reconnaissance faciale, des cas d'usage pluriels 4

II - Les impacts de la reconnaissance faciale : quels sont les risques de cette technologie ? **6**

1. Des données particulièrement sensibles, faisant l'objet d'une protection particulière 6
2. Une technologie sans contact et potentiellement omniprésente 7
3. Un potentiel de surveillance inédit, pouvant mettre en cause des choix de société 7
4. Des technologies faillibles et coûteuses, appelant un bilan complet et lucide 8

III - Expérimenter la reconnaissance faciale ? Dans un cadre précisé et avec méthode **9**

1. Première exigence : tracer des lignes rouges, avant même tout usage expérimental 9
2. Deuxième exigence : placer le respect des personnes au cœur de la démarche 10
3. Troisième exigence : adopter une démarche sincèrement expérimentale 10

IV - Quel rôle pour la CNIL dans la régulation de la reconnaissance faciale ? **11**

Introduction

Il y a plus d'un an, la CNIL appelait à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo, et en particulier sur les dispositifs de reconnaissance faciale. Le recours croissant à ces systèmes, ainsi que la prise de conscience par les pouvoirs publics des opportunités et des risques qu'ils soulèvent, placent aujourd'hui cette technologie au centre du débat public.

Ce débat est essentiel, **car, derrière les aspects techniques, il s'agit de procéder à des choix politiques et de dessiner certains contours du monde de demain :** face à la puissance de cette technologie, comment concilier la protection des libertés et droits fondamentaux avec des impératifs de sécurité ou des enjeux économiques ? Comment préserver l'anonymat dans l'espace public ? Quelles sont les formes de surveillance acceptables en démocratie ?

De tels choix ne peuvent être opérés à l'abri des regards ou du contrôle démocratique, par à-coups ou par accumulation, sans vision d'ensemble, d'initiatives ponctuelles et localisées. Sinon, le risque est grand que ces choix nous échappent, que des glissements progressifs conduisent à un changement de société non anticipé et non souhaité, que nous soyons, un jour, devant un fait accompli. Le choix politique ne doit pas être dicté purement et simplement par les possibilités techniques. De même, le débat politique ne doit pas se résumer à la question de savoir comment rendre « acceptables » certaines transformations numériques. Bien au contraire, le rôle du « politique » est de déterminer, parmi les usages possibles de ces technologies, lesquels sont réellement souhaitables, et de ne traiter l'enjeu de l'acceptabilité qu'à la fin du raisonnement, comme ultime étape et non comme postulat.

Tenir ce débat en France, c'est aussi permettre à notre pays de contribuer, en position de force, à un débat qui se joue aux niveaux européen et international, et de choisir librement son modèle de société numérique. Nous devons bâtir un véritable modèle européen, face aux usages parfois débridés ou déraisonnables de la reconnaissance faciale à travers le monde. Le moratoire décidé à San Francisco, au cœur d'une Californie en pointe sur la transformation numérique, symbolise au moins une chose : la vigilance, en matière de reconnaissance faciale, n'est pas d'arrière-garde.

Ce débat, proactif et prospectif, doit être à la hauteur des enjeux. La CNIL entend y verser aujourd'hui une première contribution, essentiellement de méthode.

Pour un débat éclairé, **les termes du débat doivent eux-mêmes être clairs, en sachant ce que recouvre la notion de reconnaissance faciale**, afin d'éviter tout amalgame entre des cas d'usage de cette technologie qui ne soulèvent pas tous les mêmes difficultés, ou avec des technologies voisines de nature différente (I). Ensuite, les risques liés **à cette technologie doivent être mesurés** pour que notre démocratie décide, avec lucidité, lesquels de ces risques elle refuse et lesquels elle assume moyennant des garanties appropriées (II). Ce débat s'inscrit par ailleurs dans un cadre juridique bien précis, dans lequel devra également s'inscrire tout usage, même expérimental, de la reconnaissance faciale : le cadre européen protégeant les données personnelles de nos concitoyens, modernisé par le Règlement général sur la protection des données (RGPD) et la directive dite « police-justice » du 27 avril 2016 (III). Enfin, la CNIL entend rappeler le rôle, de conseil et de contrôle, qu'elle joue et continuera pleinement à jouer, en toute indépendance, dans la mise en œuvre de ces technologies (IV).

I - La reconnaissance faciale : de quoi parle-t-on exactement ?

Le débat actuel est parfois faussé par une mauvaise connaissance de cette technologie et de ses modalités exactes de fonctionnement, qui peut conduire à mal en décrire les risques, tout comme les confusions entre la reconnaissance faciale et des technologies voisines utilisant elles aussi des images. Une autre difficulté réside dans l'usage du singulier : « la » reconnaissance faciale. Or, il existe une grande diversité d'usages, qui ne soulèvent pas les mêmes enjeux, notamment en termes de contrôle des personnes sur leurs données. Le risque est grand, en extrapolant à partir de cas d'usage bien installés, de porter un jugement d'ensemble erroné sur cette technologie.

1. La reconnaissance faciale est une technologie biométrique de reconnaissance des visages

La reconnaissance faciale est une **technique informatique et probabiliste** qui permet de reconnaître automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier.

La reconnaissance faciale appartient à la catégorie plus large des techniques biométriques. La biométrie regroupe l'ensemble des procédés automatisés permettant de reconnaître un individu à partir de la quantification de ses caractéristiques physiques, physiologiques ou comportementales (empreintes digitales, réseau veineux, iris, etc.). Ces caractéristiques sont qualifiées de « données biométriques » par le RGPD, parce qu'elles permettent ou confirment l'identification unique de cette personne.

C'est le cas des visages des personnes ou, plus précisément, de leur traitement technique par les dispositifs de reconnaissance faciale : à partir de l'image d'un visage (une photographie ou une vidéo), on peut réaliser un modèle représentant, d'un point de vue informatique, certaines caractéristiques de ce visage (on parle alors de « gabarit »). Ce gabarit est censé être unique et propre à chaque personne et il est, en principe, permanent dans le temps. Le dispositif permet ensuite, dans une phase de reconnaissance, la comparaison de ce modèle avec d'autres modèles, préalablement réalisés ou calculés en direct à partir de visages repérés sur une image, photo ou vidéo. La « reconnaissance faciale » se fait donc en deux temps : **la collecte du visage et sa transformation en un gabarit, puis la reconnaissance de ce visage par comparaison du gabarit correspondant avec un ou plusieurs autres gabarits.**

Comme tout procédé biométrique, la reconnaissance faciale peut remplir **deux fonctions distinctes** :

- **l'authentification d'une personne**, qui vise à vérifier qu'une personne est bien celle qu'elle prétend être. Dans ce cas, le système va comparer un gabarit biométrique préenregistré (par exemple, stocké dans une carte à puce) avec un seul visage, par exemple celui d'une personne qui se présente à un point de contrôle, afin de vérifier si cette personne est la même. Cette fonctionnalité repose donc sur la comparaison de deux gabarits.

- **l'identification d'une personne**, qui vise à retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données. Dans ce cas, le système doit effectuer un test sur chaque visage capté pour générer un gabarit biométrique et vérifier si celui-ci correspond à une personne connue du système. Cette fonctionnalité repose ainsi sur la comparaison d'un gabarit avec une base de données de gabarits. Par exemple, elle permet de lier un « état civil » (nom, prénom) à un visage, si la comparaison est faite avec une base de photographies associées à un nom et un prénom. Elle peut aussi consister à suivre la trajectoire d'une personne dans une foule, sans nécessairement faire le lien avec l'état civil de la personne.

Dans les deux cas, les techniques de reconnaissance faciale reposent sur une **estimation de correspondance** entre des gabarits : celui qui est comparé et celui ou ceux servant d'étalon. Elles sont, de ce point de vue, **probabilistes** : de la comparaison se déduit une probabilité, plus ou moins forte, que la personne soit bien celle que l'on cherche à authentifier ou à identifier ; si cette probabilité dépasse un seuil déterminé dans le système, celui-ci va considérer qu'il y a correspondance.

2. La reconnaissance faciale n'est pas synonyme de vidéo « intelligente »

La reconnaissance faciale prend place dans une palette plus large de techniques de traitement d'images vidéo. Ainsi, les caméras de vidéoprotection (dans les lieux publics) ou de vidéosurveillance (dans les lieux non ouverts au public) permettent de filmer les personnes se situant dans un espace délimité, et notamment leur visage, mais elles ne permettent pas en tant que telles de reconnaître automatiquement des individus. Il en est de même de la simple prise de photographies : un appareil photo n'est pas un système de reconnaissance faciale car les photographies des personnes doivent faire l'objet d'un traitement spécifique pour en extraire des données biométriques.

La seule détection de visages par des caméras dites « intelligentes » ne constitue pas davantage un dispositif de reconnaissance faciale. Si elles soulèvent elles aussi d'importantes questions en termes éthiques ou d'efficacité, les techniques informatiques de détection de comportements anormaux ou d'événements violents, de reconnaissance d'émotions sur les visages ou même de silhouettes ne constituent pas généralement pas des systèmes biométriques.

Ces illustrations ne sont cependant pas sans lien avec la reconnaissance faciale, car celle-ci peut être associée à d'autres dispositifs. En effet, à la différence par exemple des systèmes de captation et de traitement vidéo, qui nécessitent la mise en place de dispositifs physiques, la reconnaissance faciale est une fonctionnalité logicielle qui peut être mise en œuvre au sein de systèmes existants (caméras, base de données de photos, etc.). Cette fonctionnalité peut donc être connectée, branchée sur une multitude de systèmes, et combinée avec d'autres fonctionnalités.

Le débat autour de la reconnaissance faciale doit tenir compte de ce continuum technologique. Il s'agit de ne pas plaquer sur des besoins opérationnels précis des technologies inutilement intrusives, alors que des techniques ou des mesures ayant un moindre impact seraient tout autant, voire plus efficaces. Mais il faut aussi intégrer dans l'équation **la possibilité de combiner, dans la pratique, ces différents dispositifs, avec pour effet une démultiplication de leur impact pour les personnes.**

3. Derrière « la » reconnaissance faciale, des cas d'usage pluriels

La reconnaissance faciale peut poursuivre des finalités très diverses, aussi bien commerciales que liées à la sécurité publique. Elle peut s'inscrire dans des lieux très différents : dans la relation personnelle entre un utilisateur et un service (accès à une application), pour l'accès à un endroit spécifique (filtrage physique), ou sans limitation particulière dans l'espace public (reconnaissance faciale « à la volée »). Elle peut s'adresser à tout un chacun : client d'un service, salarié, simple badaud, personne recherchée ou mise en cause dans une procédure judiciaire ou administrative, etc. Certains usages sont déjà quotidiens et massivement répandus ; d'autres sont à ce stade, en France du moins, à l'état de projets, de spéculations, voire même absents du débat.

Plus précisément, si l'on parcourt le champ des usages potentiels, une gradation peut être envisagée, en fonction du degré de contrôle des personnes sur leurs données personnelles, de leur marge d'initiative dans le recours à cette technologie, des conséquences qui en découlent pour elles (en cas de reconnaissance ou de non-reconnaissance) et de l'ampleur des traitements mis en œuvre. La reconnaissance faciale se basant sur un gabarit stocké dans un support individuel (carte à puce, ordiphone, etc.) détenu par la personne, utilisée à des fins d'authentification, dans un usage strictement personnel, sur une interface dédiée, ne soulève pas les mêmes enjeux qu'un usage à des fins d'identification, dans un environnement non maitrisé, sans démarche active des personnes, comparant le gabarit de chacune des personnes passant dans le champ des caméras avec les gabarits d'une large population stockée en base. La palette est, entre ces deux extrémités, très nuancée.

Certains usages sont, dans leur conception, placés sous l'entier contrôle de l'utilisateur. **L'authentification** peut ainsi être utilisée afin de permettre **l'accès à des services ou des applications dans un cadre purement domestique**. Elle est ainsi massivement utilisée, en substitution de l'authentification par mot de passe, par les détenteurs d'ordiphones pour déverrouiller leur appareil.

L'authentification par reconnaissance faciale permet également de **vérifier l'identité d'une personne qui souhaite bénéficier de services offerts par des tiers, publics ou privés**. C'est le cas par exemple du

système ALICEM, qui repose sur la comparaison entre, d'une part, un « selfie » et une vidéo prise en temps réel par l'utilisateur et, d'autre part, la photographie enregistrée dans le composant électronique du passeport ou titre de séjour biométrique détenu par la même personne. Cette opération permet ainsi de créer une identité numérique à partir d'une application mobile (ordiphone, tablette, etc.), qui peut ensuite être utilisée pour accéder de manière sécurisée à des services administratifs en ligne.

S'agissant de l'accès à des services commerciaux, cette authentification biométrique peut par exemple permettre l'ouverture à distance d'un compte bancaire, par comparaison du gabarit biométrique calculé sur la base du traitement d'une photographie d'identité adressée par le client de l'organisme bancaire, avec un autoportrait photographique de cette personne.

L'authentification peut aussi être utilisée aux fins de **contrôle d'accès physique** à un ou plusieurs lieux prédéterminés, par exemple à l'entrée de bâtiments ou à des points de passage particuliers. Cette fonctionnalité est ainsi mise en œuvre dans le cadre du traitement PARAFE de passage aux frontières, où la photographie de la personne se présentant au dispositif de contrôle est comparée avec celle contenue dans son titre d'identité (passeport ou titre de séjour sécurisé).

L'identification peut donner lieu à des applications nombreuses et plus diverses. On peut notamment citer les cas d'usages suivants, constatés ou envisagés en France ou ailleurs en Europe :

- **la reconnaissance automatique de personnes présentes sur une image** aux fins d'identifier par exemple ses relations sur un réseau social, à l'instar de Facebook qui l'utilise, par comparaison entre l'image et les gabarits de toutes les personnes présentes sur le réseau ayant consenti à cette fonctionnalité, pour suggérer l'identification nominative de ces relations ;
- **l'accès à des services**, certains distributeurs de billets reconnaissant leurs clients, par comparaison entre un visage capté par une caméra et la base de données de visages détenue par la banque ;
- **le suivi du parcours d'un passager** d'un service de transport à toutes les étapes de ce parcours, par comparaison entre le gabarit calculé en temps réel de toute personne se présentant à des portiques présents à certaines étapes du parcours (déposes bagages, portiques d'embarquement, etc.) et les gabarits des personnes enrôlées au préalable au sein du dispositif ;
- **la recherche,** dans une base de données comportant des photographies, **de l'état civil d'une personne (victime, suspecte, etc.) non identifiée**, ainsi que le permet par exemple en France le traitement TAJ (Traitement des antécédents judiciaires) ;
- **le suivi des déplacements** d'une personne dans l'espace public, par comparaison entre son visage et les gabarits biométriques des personnes circulant ou ayant circulé dans la zone surveillée, par exemple en cas d'oubli d'un bagage ou à la suite de la commission d'un délit ;
- **la reconstitution du parcours d'une personne** et de ses interactions successives avec des personnes tierces, par une comparaison des mêmes éléments mais réalisée en différé, pour identifier ses contacts par exemple ;
- **l'identification sur la voie publique de personnes recherchées,** par confrontation en temps réel de tous les visages captés à la volée par des caméras de vidéoprotection et une base de données détenue par les forces de l'ordre.

Il ne s'agit là que d'exemples de cas d'usage ou de projets constatés ou envisagés aujourd'hui, en France et en Europe, dont la conformité au cadre juridique n'a donc pas nécessairement été évaluée, pour certains dispositifs d'identification en particulier. Mais les cas d'usage potentiels de la reconnaissance faciale, pour certains effectifs dans d'autres pays, sont bien plus larges. Certains États utilisent la reconnaissance faciale aux fins de vidéoverbalisation de piétons ou de lutte contre la fraude, voire identifient automatiquement l'ensemble des personnes circulant sur la voie publique.

Dans ce contexte, un raisonnement cas d'usage par cas d'usage s'impose. C'est la méthode exigée depuis 1978, confirmée en 2016 au niveau européen, par les textes fondamentaux en matière de protection des données : pour déterminer si un traitement de données personnelles est légal, il faut partir de sa finalité, du but poursuivi. Ce n'est qu'à l'aune d'une finalité précise que l'on peut apprécier si les données sont pertinentes, proportionnées, si les durées de conservation sont appropriées, si la sécurité est adaptée, etc. **Dès lors, s'il peut exister des cas légitimes et légaux d'usage de la reconnaissance faciale, ils ne doivent pas conduire à penser que tout serait souhaitable ou possible**.

II - Les impacts de la reconnaissance faciale : quels sont les risques de cette technologie ?

Les risques effectivement soulevés par cette technologie doivent être précisément évalués, afin de les gérer efficacement, voire de refuser certains usages. Si le RGPD et la loi « Informatique et Libertés » sont des textes « technologiquement neutres », leur application concrète ne peut rester indifférente à l'importance de ces risques, de ceux partagés avec les autres techniques biométriques à ceux, tels que le recul de l'anonymat dans l'espace public, plus spécifiques à la reconnaissance faciale.

1. Des données particulièrement sensibles, faisant l'objet d'une protection particulière

Les données biométriques sont des données « sensibles » au sens de la législation en matière de protection des données, au même titre que, par exemple, les données relatives à la santé ou à la vie sexuelle, aux opinions politiques et aux convictions religieuses ou encore les données génétiques. **Il s'agit là d'un choix, nouveau, du législateur européen** : alors qu'auparavant les traitements de données biométriques n'étaient pas classés comme sensibles, le RGPD et la directive « police justice » ont modifié leur statut pour tirer toutes les conséquences des risques soulevés par leur traitement.

Elles sont en effet, tout comme les autres données sensibles, **relatives à l'intimité de la vie privée des personnes**. Elles présentent 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 pas attribuée par un tiers ni même 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. Contrairement à un mot de passe ou un identifiant, elle ne peut dès lors être modifiée en cas de compromission (perte, intrusion dans le système, etc.) : elle est **non révocable**. Tout détournement ou mauvais usage de cette donnée fait ainsi peser des risques substantiels sur la personne dont elle émane : privation de ses accès à des services ou à des lieux, usurpation de son identité à des fins d'escroquerie, voire criminelles, etc.

La reconnaissance faciale, tout comme les autres techniques biométriques, n'est donc jamais un traitement tout à fait anodin. Même un usage légitime et bien cadré peut, en cas de cyberattaque, de compromission ou d'erreur, entraîner des conséquences particulièrement graves. Dans ce contexte, la question de la **sécurisation des données biométriques** est essentielle et doit être une priorité impérieuse dans la conception de tout projet de cette nature. Le stockage des données biométriques sur un support individuel détenu par l'utilisateur, à la main de ce dernier, doit toujours être privilégié aux solutions de stockage en base centrale, afin de minimiser les risques encourus. Ce n'est qu'en cas d'absolue nécessité, en l'absence de toute alternative, qu'un stockage centralisé peut être envisagé, sous réserve de strictes mesures de sécurité.

C'est pour ces raisons que les traitements biométriques, dont la reconnaissance faciale, font l'objet d'un encadrement juridique strict, resserré par les récents textes européens. Dans le RGPD, le principe est l'interdiction de tels traitements. Ils ne peuvent être mis en œuvre, par exception, que dans certains cas particuliers (avec le consentement exprès des personnes, pour protéger leurs intérêts vitaux ou sur la base d'un intérêt public important) et selon des modalités adaptées à ces risques. La logique est la même dans la directive « police-justice », qui ne permet le traitement de telles données qu'en cas de nécessité absolue. La loi française du 20 juin 2018, modifiant la loi « Informatique et Libertés », s'est inscrite dans la continuité des textes européens. En l'absence de consentement, un opérateur, public ou privé, ne peut mettre en œuvre un traitement biométrique que s'il n'y est pas préalablement autorisé par une loi ou, au minimum, par un décret.

2. Une technologie sans contact et potentiellement omniprésente

À la différence d'autres données faisant l'objet de traitements biométriques, **les données de reconnaissance faciale sont, potentiellement, disponibles partout.** Les visages des personnes sont en effet collectés et enregistrés dans une multitude de bases de données largement disponibles, qui gardent ainsi des traces de passage des individus, dans le temps et dans l'espace, et qui constituent une source potentielle de comparaison pour tout système de reconnaissance faciale. Plus généralement, toute photographie peut potentiellement devenir une donnée biométrique au prix d'un traitement technique plus ou moins aisé.

Cette dissémination des données utilisées par les dispositifs de reconnaissance intervient en outre dans un contexte d'exposition de soi permanente sur les réseaux sociaux et, plus généralement, de porosité entre les usages domestiques, privés et publics de ces données. On mesure ainsi le nombre de données techniquement accessibles et potentiellement mobilisables dans le cadre d'une identification par reconnaissance faciale. C'est une spécificité majeure de la reconnaissance faciale.

Par ailleurs, la reconnaissance faciale peut constituer une **réelle technologie « sans contact »,** certains dispositifs faisant disparaître totalement la machine du champ visuel de l'utilisateur. Elle **permet le traitement de données à distance et à l'insu des personnes.** Ce n'est pas le cas de tous les usages (déverrouillage d'ordiphone, et plus généralement la plupart des usages d'authentification), mais elle peut permettre le suivi en temps réel des déplacements de chacun, sans interaction avec la personne et donc sans qu'elle en ait même conscience. Techniquement, la reconnaissance faciale permet ainsi ce que nulle autre technologie ne permet actuellement ni n'a jamais permis, à savoir reconnaître une personne n'ayant entrepris aucune démarche particulière, ni à l'occasion d'un l'enrôlement ni à l'occasion de la comparaison, voire identifier nominativement une telle personne, sans que le porteur du dispositif ait jamais entretenu la moindre relation avec elle.

À l'heure où sont mises en avant les technologies « sans couture », la « fluidité des services », il faut rappeler que certaines frictions sont utiles. Elles constituent en effet **des points d'accroche pour les personnes, des rappels à la réalité et aux conséquences de leurs interactions avec les outils numériques**. Elles peuvent en outre constituer l'occasion pour les personnes de faire valoir leurs droits.

3. Un potentiel de surveillance inédit, pouvant mettre en cause des choix de société

Les systèmes de reconnaissance faciale peuvent s'interfacer aisément avec de nombreux dispositifs vidéo. Or, **de très nombreux dispositifs de captation d'images sont dorénavant intégrés dans notre quotidien** : caméras de vidéosurveillance ou de vidéoprotection, ordiphones, écrans publicitaires, etc. Tous ces objets peuvent ainsi potentiellement devenir des supports d'une surveillance, au sens générique du terme (régalienne ou privée), sans précédent. On ne peut exclure que ces dispositifs de captation d'images, supports potentiels de tout système de reconnaissance faciale, soient en outre couplés à d'autres types de technologies, par exemple la captation du son, amplifiant encore davantage le degré de surveillance des personnes et des lieux. Ce tournant technologique se double d'un **changement de paradigme de la surveillance**, déjà constaté en de nombreux domaines : **le passage d'une surveillance ciblée de certains individus à la possibilité d'une surveillance de tous aux fins d'en identifier certains**. Le remplacement des contrôles humains de vérification de l'identité des personnes par des contrôles réalisés par des traitements algorithmiques, modifie, par lui-même, le potentiel de surveillance. Le changement de nature de la surveillance, devenant indifférenciée, peut, plus encore, se matérialiser dans l'utilisation de la reconnaissance faciale dans l'espace public via des caméras de vidéoprotection. L'identification d'une personne sur la voie publique passe en effet par le traitement biométrique de l'ensemble des personnes circulant dans l'espace public surveillé – il faut générer les gabarits de tous pour, par comparaison, retrouver la personne recherchée.

Les cas d'usages les plus poussés de la reconnaissance faciale présentent donc un risque évident d'atteinte à **l'anonymat dans l'espace public**. L'espace public, physique ou numérique, est un lieu où s'exercent de nombreuses libertés individuelles et publiques : droit à la vie privée et à la protection des données personnelles, mais également liberté d'expression et de réunion, droit de manifester, liberté de conscience, libre exercice des cultes, etc. Cet anonymat est protégé par le droit en vigueur : il n'existe aucune règle obligeant chacun à être identifié ou à s'identifier à chaque seconde où il circule dans l'espace public. S'il existe certains interdits de ce point de vue (interdiction de dissimuler son visage) ou certaines obligations (port de badge dans certains lieux ou obligation de se soumettre aux contrôles, vérifications et relevés d'identité, par exemple), ces dispositifs sont

précisément encadrés par la loi et ne remettent aucunement en cause toute possibilité d'anonymat dans les espaces publics. Les atteintes à cet anonymat, par les pouvoirs publics ou par des organismes privés, est ainsi susceptible de remettre en cause certains de nos principes fondamentaux et doivent dès lors faire l'objet d'une réflexion approfondie.

Par ailleurs, des retours d'expérience, à l'étranger notamment, témoignent de ce que le besoin d'anonymat dans l'espace public peut conduire à rendre suspects, en présence d'un dispositif de reconnaissance faciale, des comportements anodins. Le port d'une capuche, de lunettes de soleil ou d'une casquette, le fait de regarder son téléphone ou par terre, peuvent avoir un impact sur l'efficacité de ces dispositifs, et servir, par eux-mêmes, de fondement à des soupçons.

L'ensemble de ces impacts doit être mûrement soupesé, car ce sont les termes du contrat social que certaines évolutions technologiques peuvent redéfinir à bas bruit.

4. Des technologies faillibles et coûteuses, appelant un bilan complet et lucide

Comme tout traitement biométrique, la reconnaissance faciale repose sur des estimations statistiques de correspondance entre les éléments comparés. Elle est donc intrinsèquement faillible. La réponse offerte par un système de comparaison biométrique n'est jamais binaire (oui ou non) ; elle est une probabilité de correspondance. En outre, les gabarits biométriques calculés sont toujours différents selon les conditions dans lesquelles ils sont calculés (luminosité, angle, qualité d'image, résolution du visage, etc.). Tout dispositif se caractérise ainsi par des performances variables en fonction, d'une part, des objectifs qui lui sont assignés et, d'autre part, des conditions de collecte des visages comparés.

La reconnaissance faciale, comme d'autres techniques de même nature, comporte ainsi nécessairement des « faux positifs » (une personne est reconnue à tort) et des « faux négatifs » (le dispositif ne reconnaît pas une personne qui devrait l'être). Selon la qualité et le paramétrage du dispositif, les taux de faux positifs et de faux négatifs peuvent varier. Qui plus est, ces réglages peuvent conduire à des effets de vases communicants dont il faut être conscient : si l'on privilégie, par exemple dans une finalité sécuritaire forte (lutte contre le terrorisme), la réduction des « faux négatifs », le nombre de « faux positifs », c'est-à-dire de personnes susceptibles d'être identifiées comme suspectes à tort (avec les inconvénients que cela génère), peut s'accroître. **Cette variation des performances peut ainsi avoir des conséquences très importantes pour les personnes mal reconnues par le dispositif,** qui posent des questions d'ordre pratique à prendre au sérieux pour la définition des cas d'usage et des mesures à mettre en œuvre en conséquence. Le choix des opérateurs dans le paramétrage de ces systèmes revêt ainsi une importance cruciale.

En outre, **cette technologie comporte actuellement des biais importants** : des expérimentations menées en France et dans le monde ont par exemple démontré que les taux d'erreur commis par les algorithmes de reconnaissance faciale pouvaient varier avec le sexe ou la couleur de peau. Même si des travaux, et notamment l'auto-configuration des algorithmes, peuvent être mis en œuvre pour réduire ces biais, la nature même du traitement biométrique, quel que soit le degré de maturité de la technologie, implique que des biais continueront nécessairement d'être observés.

Ces **limites techniques indépassables**, qui peuvent contredire les promesses et la fascination à l'égard d'une technologie parfois présentée ou ressentie à tort comme infaillible, doivent être prises en compte dans les choix d'investissement, au sens budgétaire comme sociétal, qui doivent nécessairement être consentis pour recourir ou non à la reconnaissance faciale.

Le **coût économique** des dispositifs de reconnaissance faciale doit à cet égard être très précisément documenté. Il pèse le plus souvent sur les collectivités territoriales ou sur les pouvoirs publics, dans un contexte global de rationalisation de la dépense publique, sans que le retour sur investissement soit toujours mesuré avec précision et méthode. Ces coûts (installation de dispositifs physiques, développement de puissances de calcul très importantes, installation de serveurs, capacité de stockage, coûts logiciels, coûts de maintenance et d'évolution, etc.) ne sauraient être minorés et les décisions prises à cet égard impliquent dès lors nécessairement l'affectation de nouvelles ressources ou la réaffectation de ressources allouées à d'autres dispositifs.

III - Expérimenter la reconnaissance faciale ? Dans un cadre précisé et avec méthode

Les pouvoirs publics semblent envisager le développement de la reconnaissance faciale par une démarche tout d'abord expérimentale. Trois exigences essentielles doivent guider l'exercice, pour garantir le respect des principes protégeant la vie privée des citoyens et leurs données personnelles, mais aussi la confiance qu'ils pourront nourrir dans les dispositifs éventuellement mis en œuvre.

1. Première exigence : tracer des lignes rouges, avant même tout usage expérimental

La reconnaissance faciale, qu'elle soit expérimentale ou non, doit respecter le cadre européen, RGPD et directive « police justice ». Dans ce cadre, tout n'est pas et ne sera pas permis en matière de reconnaissance faciale. Le but des expérimentations est, sans doute, de dessiner les frontières qui circonscrivent le champ du souhaitable (politiquement, socialement, etc.), comme celui du possible (technologiquement, financièrement, etc.). Pour autant, **des frontières préexistent à l'exercice**. Le débat, en lui-même salutaire, ne pourra pas se nourrir de tout type d'expérimentation.

La CNIL a déjà eu l'occasion de reconnaître la légitimité et la proportionnalité de certains usages. Par exemple, et sans préjudice de ses appréciations concernant certaines modalités de mise en œuvre (s'agissant notamment du caractère libre du consentement recueilli pour le dispositif ALICEM), elle a déjà admis, pour les dispositifs PARAFE ou ALICEM, le recours à la reconnaissance faciale en cas d'exigence d'un niveau particulièrement élevé d'authentification des personnes et sous réserve de leur maîtrise sur leurs données biométriques. Elle a aussi admis que, à l'occasion du carnaval de Nice, une technologie de reconnaissance faciale soit testée en conditions réelles sur un échantillon de volontaires, sans conséquence opérationnelle, pour le filtrage des accès à la zone du carnaval.

Elle a aussi déjà été conduite à dire que certains usages sont interdits dans notre société. Elle l'a ainsi signifié, récemment, pour la mise en œuvre de systèmes d'identification par reconnaissance faciale des enfants à des fins de contrôle d'accès à des établissements scolaires, dès lors que les objectifs de sécurisation et la fluidification des entrées dans de tels établissements peuvent être atteints par des moyens aussi efficaces et bien moins intrusifs en termes de vie privée et de libertés individuelles et compte tenu de la protection particulière dont doivent bénéficier les enfants.

D'autres projets pourront ainsi se heurter à ces exigences supérieures. Les principes de légitimité des objectifs poursuivis et de stricte nécessité de mise en œuvre de tels traitements biométriques sont en effet des exigences indépassables. La reconnaissance faciale ne peut légalement être utilisée, même à titre expérimental, si elle ne repose pas sur un impératif particulier d'assurer un haut niveau de fiabilité de l'authentification ou de l'identification des personnes concernées et sans démonstration de l'inadéquation d'autres moyens de sécurisation moins intrusifs.

La proportionnalité des moyens déployés au regard d'objectifs jugés légitimes constitue également une exigence indépassable. À cet égard, la reconnaissance faciale à la volée, qui repose sur une captation indifférenciée des visages dans un espace déterminé, appelle une vigilance toute particulière. Compte tenu de son ampleur et du degré de surveillance qu'il induit, ce type d'usage appelle une analyse approfondie, dans chaque contexte d'utilisation et objectif par objectif, afin d'apprécier l'adéquation ou non de tels dispositifs d'identification. La protection des droits des enfants et des autres personnes vulnérables est également une condition impérieuse.

L'élaboration d'un encadrement expérimental de la reconnaissance faciale, si elle est décidée, devra être l'occasion de fixer, avec l'avis de la CNIL dans son rôle de conseil aux pouvoirs publics, ces lignes rouges au-delà desquelles aucun usage, même expérimental, ne peut être admis.

2. Deuxième exigence : placer le respect des personnes au cœur de la démarche

Le droit à la protection des données et à la vie privée sont des droits fondamentaux. Leurs déclinaisons opérationnelles sont multiples : droit à l'information, droit d'opposition, droit de rectification, droit à ne pas faire l'objet d'une décision entièrement automatisée, etc. À l'ère numérique, la CNIL constate tous les jours le souhait croissant des personnes de savoir qui traite leurs données et comment, afin de « garder la main » sur la destinée de leurs données. Compte tenu des impacts majeurs sur les personnes des dispositifs de reconnaissance faciale, **le respect de leurs droits prend une dimension particulière. Il doit être central dans la démarche.**

Ainsi, leur **consentement** devra être recueilli pour chaque dispositif le permettant, tout particulièrement dans le cadre d'expérimentations. Le **contrôle** des données, par des supports possédés par les individus et leur en assurant la maîtrise, doit être privilégié. La **transparence** à l'égard des personnes devra être assurée en toutes circonstances, par la fourniture d'informations claires, compréhensibles et aisément accessibles. Leurs **droits** de retrait du dispositif, d'accès aux informations qui les concernent et de recours à une intervention humaine en cas de contrôle automatique devront être garantis. La **sécurité** de leurs données biométriques, relatives à l'intimité des personnes et dont toute compromission peut avoir des conséquences graves sur leur vie quotidienne, doit constituer une condition impérieuse de leur traitement.

Au-delà des droits juridiquement reconnus, les personnes devront être, en tant que telles, mises au cœur de tout système de reconnaissance faciale. **Les expérimentations ne sauraient éthiquement avoir pour objet ou pour effet d'accoutumer les personnes à des techniques de surveillance intrusive**, en ayant pour but plus ou moins explicite de préparer le terrain à un déploiement plus poussé. Il ne saurait s'agir, à ce stade, de rendre « acceptables » des dispositifs nuisant à l'autonomie des personnes ou portant atteinte à leurs droits fondamentaux. L'acceptabilité ne peut devenir un objectif qu'ultérieurement, pour des dispositifs reconnus comme parfaitement légitimes et licites.

3. Troisième exigence : adopter une démarche sincèrement expérimentale

Compte tenu des enjeux soulevés par la reconnaissance faciale, il est impérieux de se prémunir de tout effet cliquet lié à la mise en œuvre de certains dispositifs. De ce point de vue, une démarche expérimentale est sans doute préférable à la préparation d'un cadre d'emblée pérenne, qui figerait un certain nombre de cas d'usage autorisés de manière générale en France. Néanmoins, le déploiement de ces systèmes doit alors suivre une véritable démarche expérimentale.

Cela implique notamment une limitation dans le temps et dans l'espace de tels dispositifs, une identification exacte des objectifs poursuivis par ces expérimentations et de leurs critères de réussite. La définition précise de leurs modalités d'évaluation, qui doit être rigoureuse, contradictoire, pluridisciplinaire et menée dans des délais raisonnables, ainsi que la détermination des autorités chargées de celle-ci, constituent des dimensions essentielles. La comparaison avec d'autres dispositifs techniques pouvant répondre aux mêmes besoins permettra en outre une meilleure évaluation des systèmes de reconnaissance faciale.

Le cadre juridique doit ainsi garantir la sincérité des expérimentations conduites, dont l'issue ne saurait être préjugée. Il doit pour cela consacrer une méthode expérimentale rigoureuse, inspirée du cadre juridique plus général en la matière et du « guide méthodologique » récemment élaboré par le Conseil d'État, afin de tirer tout le parti possible d'une telle démarche tout en faisant montre de la prudence nécessaire face aux risques posés par la reconnaissance faciale.

Cette prudence n'a pas pour objet de brider l'innovation technologique. Au contraire, **une véritable démarche expérimentale permettra de tester et de parfaire des solutions techniques respectueuses du cadre juridique**, lorsqu'elles se présenteront, et intégrant directement les contraintes liées à ces règles.

IV - Quel rôle pour la CNIL dans la régulation de la reconnaissance faciale ?

Les principes de protection des libertés, de la vie privée et des données personnelles ont été portés au niveau européen par le RGPD et la directive « police justice » en 2016. Ces principes cristallisent un pacte républicain sur le numérique rappelé à l'article 1er de la loi « Informatique et Libertés » : « *L'informatique doit être au service de chaque citoyen. […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

Le sens de ce pacte n'est pas, en l'occurrence, d'opposer de manière stérile la protection des données, d'une part, et les objectifs, légitimes, poursuivis par certains projets de reconnaissance faciale (sécurité, fourniture d'une identité numérique, etc.), d'autre part. Il est d'inviter à rechercher une voie permettant de concilier ces deux séries d'exigences, dans une optique de long terme et en s'attachant aux enjeux éthiques de toute transformation numérique.

Les choix politiques sont du ressort du Gouvernement et du Parlement. Quels que soient ces choix, l**a CNIL jouera son rôle de garante indépendante de ces grands principes, dans sa double mission de conseil aux pouvoirs publics et, autant que nécessaire, de contrôle du respect de la loi**.

Pour ce faire, elle devra s'assurer, à chaque étape, du respect des règles particulières établies par le cadre juridique actuel pour le traitement de données biométriques, qui s'imposent dès lors à tout dispositif de reconnaissance faciale : des dérogations strictes au principe d'interdiction du traitement de telles données, le caractère libre et éclairé du consentement des personnes participant à un dispositif biométrique, la réalisation d'une analyse d'impact préalable à la mise en œuvre d'un tel traitement afin d'en limiter les risques, le nécessaire encadrement par des textes (selon les cas, décret en Conseil d'État, pris après avis de la CNIL, ou loi) des dispositifs ne reposant pas sur le consentement des personnes, etc.

Si un dispositif expérimental ad hoc devait voir le jour en matière de reconnaissance faciale, **la CNIL conseillera les pouvoirs publics en amont sur tout cadre d'expérimentation** (périmètre, méthode, règles de fond, etc.) et devrait nécessairement être consultée sur tout projet de texte législatif ou réglementaire qui serait adopté pour permettre ou faciliter d'éventuelles expérimentations.

Elle pourrait également être consultée au préalable et systématiquement sur les cas concrets d'expérimentation envisagés, afin de s'assurer de la conformité des projets de systèmes de reconnaissance faciale au cadre juridique expérimental ainsi établi et d'appeler l'attention sur les éléments devant faire l'objet, du point de la vue de la protection des données à caractère personnel, d'une évaluation particulière. À l'appui d'une telle consultation, la CNIL devrait disposer des analyses d'impact élaborées avant la mise en œuvre de chaque traitement. Elle devrait en tout état de cause **être rendue destinataire de bilans périodiques**, d'étape et au terme de l'expérimentation, afin d'être en mesure de contribuer à l'exercice d'évaluation de ces dispositifs. Elle pourra naturellement, à tout moment, exercer toutes ses prérogatives lui permettant, d'initiative ou sur saisine des personnes concernées, de **contrôler le respect effectif du cadre juridique et, au besoin, d'imposer les correctifs nécessaires,** voire l'arrêt des dispositifs illégaux.

Dans l'exercice de l'ensemble de ses missions, la CNIL conservera sa totale indépendance. Elle ne peut dès lors être partie prenante de l'organisation effective des expérimentations en matière de reconnaissance ou de leur pilotage. Elle pourra ainsi jouer pleinement le rôle de régulateur qui est le sien.