http://observatoireethiquepublique.com/

Reconnaissance faciale : pour un régime juridique à la hauteur des enjeux éthiques[1]

Note #26
Mai 2022

Raphaël MAUREL

Secrétaire Général de l'OEP
Directeur du département éthique des affaires

EN BREF

Un rapport sénatorial du 10 mai 2022 a ouvert une nouvelle perspective en matière d'utilisation des technologies numériques en France. Intitulé **« La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance »**, il préconise l'autorisation d'expérimentations de la reconnaissance faciale dans l'espace public. Bien que les propositions démontrent un souci d'encadrement rigoureux de l'expérimentation, plusieurs angles morts, de nature éthique et juridique, apparaissent à la lecture de ce rapport qui servira probablement de base à une future loi sur le sujet. À titre principal, cette note invite à débattre sérieusement de la question de la nécessité de développer la reconnaissance faciale. Subsidiairement, elle propose de clarifier le régime juridique envisagé en adoptant un régime d'interdiction soumis à dérogations selon un principe de stricte nécessité.

[1] Les propos tenus et propositions formulées dans cette note n'engagent pas collectivement l'Observatoire de l'éthique publique et sont propres à son auteur.

Le rapport sénatorial sur « La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », qui sert de base à cette réflexion[2], a proposé **l'inéluctable : l'expérimentation de la reconnaissance biométrique en France**.

La **« reconnaissance faciale », qui relève des techniques biométriques, recouvre des réalités différentes.** Celles-ci vont du déverrouillage d'ordiphone à la reconnaissance d'une personne recherchée par les forces de police dans une foule, en passant par l'ouverture de comptes bancaires. Si on peut définir la reconnaissance faciale comme « une technique informatique et probabiliste qui permet de reconnaître automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier »[3], il reste que les enjeux qu'elle soulève sont particulièrement diversifiés selon l'usage qui en est fait. À cet égard, deux usages possibles de la reconnaissance faciale, qui demeure un **outil probabiliste comprenant une marge d'erreur**, sont principalement distingués. D'une part, **l'authentification d'une personne** unique, par comparaison d'un visage avec un autre préenregistré, afin d'établir une concordance et de vérifier que la personne est bien celle qu'elle prétend être. D'autre part, **l'identification d'une personne**, qui vise à détecter la présence d'un individu précis au sein d'un groupe, d'un lieu ou base de données. L'identification ouvre la voie vers la **catégorisation des personnes** et soulève des problématiques spécifiques, et plus générales, en termes de libertés fondamentales.

Le sujet est d'actualité et le « *débat est crucial. En effet, au-delà des aspects techniques du débat, des choix politiques doivent être faits afin de façonner ce à quoi ressemblera notre société demain : face à la puissance de cette technologie, comment concilier la protection des droits et libertés fondamentaux avec les questions de sécurité, les considérations*

[2] Sénat, « La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », Rapport d'information n° 627 (2021-2022) de MM. Marc-Philippe DAUBRESSE, Arnaud de BELENET et Jérôme DURAIN, fait au nom de la commission des lois, déposé le 10 mai 2022.
[3] CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux », CNIL, 15 novembre 2019, p. 3.

économiques et la compétitivité technologique ? »[4]. Alors que de tels dispositifs sont déjà utilisés dans plusieurs pays, comme en Italie, aux États-Unis ou en Chine, la question de leur implantation en France était donc latente. Des expérimentations auprès de personnes volontaires ont déjà eu lieu dans l'hexagone, à l'instar de celle menée lors du carnaval de Nice en 2019[5]. De nombreux dispositifs seraient prêts à être utilisés dès l'autorisation acquise[6] ; mais le consentement des personnes filmées demeure une limite, en l'état du droit principalement issu du RGPD (Règlement général sur la protection des données). À l'heure où l'Union européenne prépare une harmonisation *a minima* des droits nationaux à ce propos[7], **la perspective des Jeux Olympiques de Paris en 2024**, où « *les tensions en matière de sécurité et de gestion de flux seront accrues* » **accélère indubitablement le processus en France**, comme le révèle le rapport.

On peut néanmoins, à titre liminaire, regretter la **terminologie** employée par les auteurs du rapport. Alors que celui-ci annonce « écarter le risque d'une société de surveillance », il préconise finalement l'inverse, en proposant justement d'expérimenter la reconnaissance faciale dont la technologie relève indubitablement des techniques de surveillance des sociétés. Cette contradiction sémantique, qui conduit à suggérer l'inverse de ce que l'on promeut, n'est pas inconnue des travaux parlementaires, mais peut être contestée**.** Par transparence, honnêteté et bonne foi, il faut nommer les choses par leur nom : **le rapport se positionne à titre principal pour une expérimentation de la reconnaissance biométrique dans l'espace public**, et non pour éviter tout risque de dérive vers une société de surveillance – dans ce dernier cas, l'interdiction aurait certainement été la seule conclusion du rapport. Une éthique de la fonction législative inviterait, dès lors, les porteurs d'un futur texte sur ce thème à **ne pas évoquer, en intitulé, la levée d'un risque que l'on ne peut pas totalement écarter** si l'expérimentation est actée.

[4] Th. Christakis, K. Bannelier, Cl. Castelluccia, D. Le Metayer, « Mapping the use of facial recognition in public space in Europe, Part 1. A quest for clarity: unpicking the "catch-all" term », May 2022, p. 4 (traduction personnelle).
[5] L'expérience, menée auprès de plusieurs centaines de personnes consentantes qui avaient préalablement fourni leur photographie, se savaient filmés et avaient accepté d'être soumises à une technologie de reconnaissance faciale, a permis d'identifier avec précision des figurants supposés représenter des personnes « fichées S ».
[6] V. par exemple Le Continent Média, « Reconnaissance faciale : les expérimentations se multiplient avant les J.O de Paris », 9 septembre 2020.
[7] Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, 21 avril 2021 (COM/2021/206 final).

Le rapport du 10 mai servira de levier pour **l'ouverture d'une porte qui ne se refermera plus**. Si la reconnaissance biométrique devait faire l'objet d'un projet ou d'une proposition de loi visant à en proposer l'expérimentation au cours de la prochaine législature, il y a en effet très peu de doutes quant au fait que **son usage se trouverait peu à peu généralisé**. Il est dès lors essentiel de poser les bonnes questions, sur les plans éthiques et juridiques, dès maintenant.

Une insuffisante prise en compte des enjeux éthiques

Le rapport du 10 mai est le fruit d'un dense et long travail d'auditions, d'expertises et de réflexion. Il ne peut que relever que « *les conséquences de la reconnaissance faciale en matière de sauvegarde des libertés publiques constituent une source de préoccupation unanimement partagée* ». Qu'il s'agisse d'atteintes aux droits à la vie privée et à la protection des données personnelles ou d'atteintes encore plus profondes, comme la génération spontanée de **comportements d'autocensure** du simple fait de la conscience de l'existence de la reconnaissance faciale, les dangers sont bien identifiés, quand bien même le risque d'une société de surveillance serait effectivement écarté – ce qui n'est pas évident à la lecture du rapport. Pourtant, ce dernier conclut que « *[s]ans être exhaustif, la liberté d'aller et venir, de réunion, d'association, de culte ou d'expression sont autant de libertés dont la portée pourrait être restreinte du fait d'un usage illégitime ou disproportionné de la reconnaissance faciale* ». La sémantique a ici son importance : alors même que l'existence de comportements d'autocensure dans ces contextes a été clairement mentionnée, les rapporteurs induisent, *a contrario,* qu'un usage légitime ou proportionné de la reconnaissance faciale ne restreindrait aucune de ces libertés.

C'est sur cette base argumentative – à notre sens erronée – que s'est bâtie une **réflexion qui fait l'impasse un enjeu éthique majeur** : il faut avant tout se poser la question de **l'utilité** de cette technologie. Par ailleurs, il est impératif à la fois de **ne pas concevoir**

l'expérimentation comme un préalable à l'inscription de la reconnaissance faciale dans la loi, et de ne pas chercher à **favoriser artificiellement l'acceptabilité de ces dispositifs**.

Poser la question de l'opportunité d'ouvrir la brèche

Peut-on posséder une technologie sans l'utiliser[8] ? Telle est la question à laquelle on propose de ne pas répondre d'emblée par la négative, à l'inverse de l'esprit qui semble avoir guidé les rapporteurs du Sénat.

La reconnaissance faciale peut servir à authentifier, à identifier et à catégoriser les individus dans une société. Alors que l'efficacité de ces dispositifs, en termes de sécurité publique, n'est pour l'instant pas démontrée[9] et que la sobriété numérique devient déjà un sujet écologique majeur [10], la question éminemment éthique de l'utilité de leur développement n'est en effet guère posée. Ce silence est d'autant plus assourdissant que dès lors que la reconnaissance biométrique permet la catégorisation des individus, la terrifiante dérive vers une société de la notation sociale à la chinoise, dont le rapport prescrit l'évitement, devient de l'ordre du possible. Autrement dit, face aux risques identifiés pour nos sociétés et nos libertés, **la question de l'utilité de la reconnaissance faciale devrait être au fondement de toute réflexion** sur une éventuelle démarche législative. C'est bien là, au cœur de l'éthique du numérique, que devrait se positionner le débat, si d'avance il devait vraiment être ouvert.

Se poser à titre préalable la question de l'utilité de la reconnaissance faciale ne suffit pas : encore faut-il **s'autoriser à y répondre par la négative et à en tirer les conséquences**. Dans l'histoire de l'humanité, de nombreuses avancées technologiques ont soulevé des questionnements éthiques : les OGM, la bombe atomique en sont deux exemples topiques.

[8] B. Jarry-Lacombe, J.-M. Bergère, F. Euvé, H. Tardieu, *Pour un numérique au service du bien commun*, Odile Jacob, 2022, pp. 148 et suivantes.
[9] R. Chatila, L. Devillers, K. Dognin-Sauze, J.-G. Ganascia, M. Gornet, A. Pronesti, C. Tessier, « Pourquoi la reconnaissance faciale, posturale et comportementale soulève-t-elle des questionnements éthiques ? », *in* CNPEN, *Pour une éthique du numérique*, PUF, 2022, pp. 209 et suivantes.
[10] D'après l'ONG GreenIT, le numérique était responsable d'environ 4% des émissions totales de gaz à effet de serre (GES) en 2020.

Force est de constater que, malgré de denses débat, l'Homme ne s'est jamais abstenu d'utiliser une technologie qu'il a préalablement développé[11]. De nos jours, la question est également économique et concurrentielle. Comme l'a souligné le rapporteur Jérôme Durain lors de l'audition de Cédric O, ancien secrétaire d'État chargé de la transition numérique et des communications électroniques, « *[n]os industriels ressentent une forte tension entre une réglementation européenne contraignante et le risque que des dispositifs plus performants soient développés par leurs concurrents. Nous risquons aussi d'être débordés par la technologie, car, on le sait,* code is law ». Doit-on pour autant renoncer par avance et considérer que dès lors qu'une technologie **existe**, et **sera nécessairement utilisée**, de sorte qu'il conviendrait de **l'expérimenter plutôt que l'interdire**, après examen rapide – et fondamentalement biaisé – de l'opportunité de la déployer ? Probablement pas : ce serait nier l'existence de cultures juridiques distinctes, mais aussi le **libre-arbitre d'une société** capable de déterminer, malgré l'existence d'une technologie proposée par un acteur privé, les avantages et les risques de son utilisation. Or, l'éthique du numérique nous semble constituer un terreau particulièrement fertile à l'expérimentation de l'abstention d'agir : à la mondialisation numérique, des États doivent pouvoir opposer la sobriété numérique et un projet de société vertueuse, impliquant des alternatives à l'adoption systématiques des nouvelles technologiques. **Pour des raisons d'opportunité, de libertés comme de sobriété numérique, les pouvoirs publics doivent impérativement pouvoir se garder d'ouvrir la porte à la reconnaissance biométrique** dans l'espace public.

Consulter et respecter l'avis de la population

L'absence de réflexion éthique quant à l'opportunité d'utiliser la reconnaissance faciale s'accompagne de deux dangers : la tentation, identifiée par le rapport sénatorial, de faire de l'expérimentation un **préalable menant vers la pérennisation « automatique » des dispositifs** testés, et celle de ne pas mener un **nécessaire débat national** sur ce thème.

[11] *Idem*.

L'expérimentation ne doit pas faire jurisprudence

Il est logique que l'expérimentation précède l'adoption éventuelle de la reconnaissance biométrique dans le paysage français. Le rapport du 10 mai 2022 s'inscrit en ce sens dans la dynamique européenne sur la question, **une consultation publique sur l'utilisation de la reconnaissance faciale étant justement menée par l'*European Data Protection Board*** depuis le 12 mai 2022[12]. On le sait, *« le débat sur l'utilisation de la reconnaissance faciale ne fait que commencer »*[13]. Pourtant, la plupart des expérimentations conduisent à une adoption à court terme du dispositif expérimenté.

Aussi, **il est essentiel d'envisager l'expérimentation comme un véritable « test » et non comme un préalable** à l'intégration du dispositif dans le droit français. Les débats reproduits dans le rapport soulignent, à cet égard, la problématique de **l'accoutumance** provoquée par l'expérimentation, dont on sait par expérience qu'elle est généralement suivie d'une codification. Comme l'a relevé la CNIL, « *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* »[14]. Il convient donc de prendre dès à présent les mesures qui s'imposent pour garantir que l'expérimentation puisse conduire à un verdict positif, mais également **aboutir à des conclusions négatives et donc à une interdiction de la reconnaissance faciale**, dont l'utilité, l'efficacité et/ou le degré de protection des droits et libertés fondamentaux ne se seraient pas avérés satisfaisants.

Ces éléments doivent se traduire, concrètement, par une attention particulière portée au caractère éphémère de l'expérimentation. Les éventuels **dispositifs installés doivent ainsi pouvoir être désinstallés** et **l'ensemble des données collectées pouvoir être détruit, sans**

[12] Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, soumises aux commentaires publics le 12 mai 2022.
[13] B. Jarry-Lacombe, J.-M. Bergère, F. Euvé, H. Tardieu, *Pour un numérique au service du bien commun*, Odile Jacob, 2022, p. 77.
[14] « Reconnaissance faciale : pour un débat à la hauteur des enjeux », CNIL, 15 novembre 2019. L'extrait est reproduit dans le rapport du 10 mai 2022.

possibilité de réutilisation ni de transfert, par des personnes privées ou publiques, de quelconque manière que ce soit.

Consulter la population par une Convention citoyenne

Le rapport du 10 mai 2022 pose la question de **l'acceptabilité, par la population française, de la reconnaissance biométrique**. Nonobstant les développements qui précèdent concernant le raisonnement qui élude l'enjeu majeur de l'utilité de cette technologie, la première proposition du rapport étonne : « *[r]éaliser une enquête nationale visant à évaluer la perception de la reconnaissance biométrique par les Français, à cerner les cas d'usages auxquels ils se montrent plus ou moins favorables et à identifier les ressorts d'une meilleure acceptabilité de cette technologie* ». Parmi les trois composantes de cette proposition, les deux premières paraissent adaptées. Comme le relève le même rapport, « *[i]l existe encore peu de sondages sur le sujet, et ceux qui sont disponibles ne permettent pas d'obtenir des certitudes quant à l'état de l'opinion sur cette technologie* » : on parle d'environ 50% de Français favorables à la reconnaissance faciale dans certains cas, et donc du même nombre de Français défavorables**. Une évaluation précise de l'état de l'opinion publique est donc nécessaire** et on peut se satisfaire que la toute première étape consiste à y pourvoir.

Néanmoins, l'idée selon laquelle ces données devraient être utilisées pour « *identifier les ressorts d'une meilleure acceptabilité* » de la reconnaissance facile induit, d'emblée, un objectif politique voire les prémices d'un programme d'action dont on ne peut se satisfaire. Face aux risques que soulève cette technologie, **l'objectif d'une telle enquête ne devrait pas résider dans la construction d'argumentaires** permettant de convaincre l'opinion publique de la nécessité – non encore démontrée – de la reconnaissance biométrique, mais **d'évaluer le besoin social** d'y recourir. L'institution d'une « **Convention citoyenne pour un usage éthique des technologies numériques** » dans notre société et d'un grand débat national paraît, à cet égard, une perspective souhaitable, dans la mesure où les propositions issues de cette Convention pourraient être intégrées aux débats législatifs.

Un régime juridique à construire en toute transparence

Une lecture formaliste du rapport laisse d'abord penser que le futur régime choisi est celui de **l'interdiction de la reconnaissance biométrique**. Cependant, la réalité est bien plus complexe, à tel point qu'on peut finalement y voir, de manière contre-intuitive, la proposition d'un rigoureux régime d'autorisation. La proposition principale du rapport réside en effet dans **l'expérimentation d'un régime d'autorisation soumis à contrôle *a priori* et *a posteriori*.** Nous suggérons de revenir sur ce choix, et, subsidiairement, proposons plusieurs points de vigilance. Il apparaît notamment pertinent de **centraliser les moyens de contrôle** des éventuelles autorisations ou dérogations accordées, et d'approfondir la question de la **gestion des données** issues de la reconnaissance faciale.

Les prémices d'un régime complexe et peu intelligible

Le rapport du 10 mai 2022 laisse, il est vrai, transparaître l'existence d'un régime d'interdiction de principe de certaines formes de reconnaissance biométrique. À cet égard, il préconise clairement **l'interdiction de la notation sociale**, de la **catégorisation d'individus en fonction de leur origine ethnique, sexe, orientation sexuelle** (sauf dans le cadre de la recherche scientifique et sous réserve de garanties à déterminer), et de **l'analyse d'émotions** (sauf à des fins de santé ou de recherche scientifique et sous réserve de garanties là aussi). Ces trois « lignes rouges », appelées des vœux de la CNIL[15], sont complétées par une quatrième, moins claire, et d'emblée soumise à des exceptions potentiellement nombreuses malgré l'expression utilisée : « *[d]'une manière générale, **interdire l'utilisation de la reconnaissance biométrique à distance en temps réel dans l'espace public**, sauf exceptions très limitées* ». Bien que répondant globalement à l'une des

[15] CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », 15 novembre 2019, p. 8.

recommandations récentes de la Commission nationale consultative des droits de l'homme[16], Ces « *exceptions très limitées* » figurent en proposition n°22 :

> « *Proposition n° 22 : Créer un cadre juridique expérimental permettant, par exception et de manière strictement subsidiaire, le recours ciblé et limité dans le temps à des systèmes de reconnaissance biométrique sur la voie publique en temps réel sur la base d'une menace préalablement identifiée, à des fins de sécurisation des grands évènements et de site sensibles face à une menace terroriste, pour faire face à une menace imminente pour la sécurité nationale, et à des fins d'enquête judiciaire relatives à des infractions graves menaçant ou portant atteinte à l'intégrité physique des personnes* ».

Au-delà de la formulation et contrairement à la proposition restrictive de la CNCDH[17], de **nombreuses exceptions paraissent ainsi invocables**, dès lors que sont en jeu la sécurité d'une manifestation sportive, les abords de sites « sensibles », l'état d'urgence terroriste ou encore une enquête diligentée à la suite de violences commises sur une personne. Si l'on peut féliciter de certaines propositions, comme celle d'un contrôle humain systématique (proposition n°16) ou d'un recensement au niveau national des actes autorisant le déploiement des technologies de reconnaissance biométrique (proposition n°12), le rapport s'avère ainsi bien plus contrasté qu'annoncé. En particulier, il faut relever que la perspective de **la généralisation de la reconnaissance faciale est pleinement admise pour sécuriser l'accès à certains évènements** – on pense en premier lieux aux manifestations sportives ou culturelles. Si le rapport rappelle l'importance de fonder ces pratiques sur le consentement des personnes concernées, il paraît évident qu'il s'agira demain d'une **simple adhésion formelle à la reconnaissance faciale**, imposée *de facto* à toute personne souhaitant accéder à un évènement sportif. Le rapporteur Jérôme Durain va même plus loin en indiquant dans les débats que **les dispositifs d'authentification par reconnaissance biométrique pourraient également être rendus obligatoires** pour accéder

[16] CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, 7 avril 2022, A-2022-6, recommandations n°5 (« [l]a CNCDH recommande d'interdire tout type de notation sociale ("*social scoring*") mis en place par les administrations ou par toute entreprise, publique ou privée ») et n°6 (« [l]a CNCDH recommande d'interdire l'identification biométrique à distance des personnes dans l'espace public et les lieux accessibles au public, en admettant par exception son utilisation, dès lors que celle-ci est strictement nécessaire, adaptée et proportionnée pour la prévention d'une menace grave et imminente pour la vie ou la sécurité des personnes et celle des ouvrages, installations et établissements d'importance vitale »).

[17] *Idem.*

« *à des zones nécessitant une sécurisation exceptionnelle* », de manière certes dérogatoire. Cette idée redoutable, en ce qu'elle mène droit vers une société du contrôle que le rapport est censé éviter, figure en proposition n°17 : « *permettre, à titre expérimental, aux acteurs étatiques, dans l'organisation de grands évènements, d'organiser par exception un contrôle exclusivement biométrique de l'accès aux zones nécessitant une sécurisation exceptionnelle* ».

Même l'usage de **la reconnaissance faciale par des opérateurs privés est finalement admise**, selon la même logique : « *[i]nterdire tout usage privé des technologies de reconnaissance biométrique ne requérant pas le consentement des utilisateurs, à l'exception, dans quelques rares cas particuliers et dûment justifiés, de traitements pour contrôler l'accès aux lieux et aux outils de travail (accès à des zones ou à des produits nécessitant un niveau de protection particulièrement élevé)* » (proposition n°23). Autrement dit, le rapport préconise non pas un régime d'interdiction, mais une **banalisation encadrée du recours à la reconnaissance faciale pour authentifier, voire pour identifier des individus** dans divers contextes du quotidien. Il suffira donc, demain, à un employeur d'inclure une clause contractuelle relative au consentement général du salarié à la reconnaissance biométrique à l'entrée de l'entreprise pour satisfaire pleinement aux exigences suggérées par le rapport ; dans le cas d'un laboratoire pharmaceutique ou chimique, cette clause pourrait même s'avérer non nécessaire. On imagine alors aisément la généralisation possible de la reconnaissance faciale dans l'espace public comme privé, à rebours des objectifs annoncés par le rapport.

Le régime juridique esquissé par le rapport s'avère donc, de prime abord, **peu intelligible**, puisqu'à une interdiction censée être de principe succède **une dense série d'autorisations possibles, et même l'éventualité de rendre une partie du dispositif obligatoire**. Il est dès lors peu aisé de déterminer lequel, de l'interdiction ou de l'autorisation, est le principe.

Faire le choix de l'interdiction de la reconnaissance faciale d'identification dans l'espace public

Face aux apparents tiraillements du rapport, au nombre de dérogations prévues et à la complexité prévisible de leur interprétation, le travail législatif qui s'annonce devra **clarifier la doctrine française sur la question de la reconnaissance faciale**. À cet égard et compte tenu des considérations éthiques développées plus haut, deux options pourraient être retenues.

Le choix du silence de la loi

La première possibilité est de **conclure au nécessaire silence de la loi**. En l'absence d'autorisation de la reconnaissance faciale dans l'espace public, qu'elle vise à authentifier ou à identifier, le régime actuel, fondé sur une interdiction sauf dérogations particulièrement encadrées du fait de l'application du RGPD (Règlement général sur la protection des données), n'est critiqué que du fait de sa rigidité[18]. Comme le relève le rapport, certains détracteurs considèrent que « *la législation ne permet pas de distinguer la reconnaissance faciale* stricto sensu*, qui vise délibérément à identifier une personne physique, de l'analyse vidéo augmentée, qui peut procéder à l'analyse du visage à d'autres fins que l'identification* ». Autrement dit, **le moteur de la réforme suggérée n'est pas l'absence d'encadrement de la reconnaissance faciale, mais son actuelle interdiction de principe**. En l'absence de certitudes quant à l'opportunité, du point de vue de l'éthique du numérique, d'autoriser ces technologies, **la meilleure des solutions pourrait être l'abstention parlementaire d'agir**.

Cela n'empêcherait pas l'utilisation ponctuelle et limitée, dans le cadre du RGPD, de la reconnaissance faciale à des fins d'authentification.

[18] Voir le rapport sénatorial du 10 mai 2022.

Pour un régime d'interdiction soumis à rares exceptions

Si le législateur estimait nécessaire de se saisir du sujet et de proposer une réforme, il devrait **clarifier le régime proposé en optant pour une interdiction qui serait véritablement de principe**. Il est en effet possible de limiter au strict minimum les cas d'usage de la reconnaissance biométrique dans l'espace public, à la suite d'un débat sérieux sur les cas lesquelles celle-ci s'avère indispensable. Ce n'est que dans le cadre de cette réflexion fondée sur le principe de l'interdiction que peut avoir lieu un débat de fond sur les subtilités des usages qu'il serait pertinent non pas d'autoriser de manière générale, mais de permettre de manière dérogatoire. À cet égard, **les dérogations possibles devraient être en nombre limité et être exhaustivement énumérées par la loi**.

À cet effet, **le principe de « stricte nécessité » de la reconnaissance faciale**, comme critère dérogatoire possible, **gagnerait à remplacer celui de « l'inadéquation » d'autres moyens**. Dans sa communication de novembre 2019 qui a servi de base de travail au rapport sénatorial de 2022, la CNIL déclarait que « *[l]a 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*** »[19]. Or, le standard de l'inadéquation est moins exigeant que celui de la stricte nécessité, entendu comme **l'impossibilité de faire autrement**. Telle est la voie tracée par la Commission de la protection de la vie privée belge dès 2008 : « *[l]es systèmes biométriques ne devraient pas être utilisés seulement parce qu'ils sont pratiques, mais parce qu'ils constituent* ***le seul moyen pour permettre de réaliser la finalité initialement décrite*** »[20]. L'adoption d'une formulation similaire permettrait d'orienter clairement l'interprétation du régime juridique émergent par le juge, susceptible d'être amené à connaître de la légalité de l'utilisation d'un dispositif de reconnaissance faciale

[19] CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », 15 novembre 2019, p. 9.

[20] Commission de la protection de la vie privée belge, Avis d'initiative relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes, Avis n° 17 /2008 du 9 avril 2008, §72. Voir dans le même sens le §68 : « *[l]e responsable de traitement doit donc réaliser une comparaison des différents systèmes d'authentification et vérifier si le même résultat ne pourrait être obtenu avec un système moins intrusif pour la vie privée, telle que la reconnaissance visuelle (comparaison avec la photo d'une carte ou d'un badge)* ».

dans un contexte donné. Le terme « inadéquation » peut en effet être interprété de manière restrictive comme avec souplesse, et pourrait faire l'objet d'une interprétation neutralisante, ce qui s'avèrerait plus complexe si le standard de la « stricte » ou « impérieuse » nécessité était retenu. Pareille formulation ne ferait, par ailleurs, pas obstacle à certains usages légitimes tels que l'utilisation *a posteriori* de la reconnaissance faciale dans le cadre d'une enquête de police judiciaire.

L'utilisation de ces technologies par des **acteurs privés** pourrait enfin être interdite sans dérogation possible. Ce **verrou législatif**, dont on est bien conscient qu'il constituerait un engagement politique fort aux conséquences industrielles significatives, assurerait ainsi de manière optimale la préservation des libertés fondamentales actuellement garanties, sans pour autant contrevenir aux normes européennes actuelles et en développement. Des aménagements spécifiques pourraient être prévus pour les personnes privées gérant un service public, dans le respect du principe de stricte nécessité.

À défaut, créer un régime d'autorisation plus rigide

Le régime esquissé par le rapport du 10 mai prend soin retenir une division des autorités de contrôle, et un modèle de contrôle différencié selon les usages projetés. Si cette prévoyance apparaît pertinente, l'éclatement des autorités compétentes pourrait soulever des difficultés. Par ailleurs, la bonne gestion des données issues de l'expérimentation et, demain, de la pérennisation éventuelle du dispositif doit rester une priorité.

Assurer un contrôle a priori *par une autorité unique*

Dans les nombreux cas de dérogations prévus par le rapport, une **autorisation préalable** des usages de la reconnaissance biométrique a été jugée nécessaire. La mission sénatoriale souhaite ainsi que les usages soient autorisés *a priori*, selon deux modalités distinctes. En cas de **recours à la reconnaissance faciale par les forces de sécurité intérieure, l'autorisation relèverait soit d'un magistrat, soit du préfet,** selon que l'action requise

s'exerce dans le cadre d'une mission de police judiciaire ou de police administrative. Dans ces deux cas, qui peuvent relever de la reconnaissance *a priori* comme *a posteriori* sur la base d'images de vidéosurveillance, une **consultation préalable de la CNIL** serait nécessaire. En cas de déploiement **par un acteur privé** dans un lieu accessible au public, le rapport préconise que la **CNIL serait seule compétente** pour autoriser le déploiement *a priori*. Enfin, le rapport indique que « *le pouvoir de contrôle de la CNIL serait réaffirmé afin qu'elle exerce son rôle de gendarme de la reconnaissance biométrique, qu'elle mène des contrôles* a posteriori *du bon usage des dispositifs et des éventuels détournements de finalité en dehors de l'autorisation* ». Autrement dit, dans le futur dispositif, la CNIL est censée intervenir à tous les stades, *a priori* comme *a posteriori*. La nature de sa mission diverge cependant fortement selon un critère organique : **consultative** dans le cadre du contrôle *a priori* d'un usage par l'autorité publique, elle devient **décisoire** dans le cadre du contrôle *a priori* d'un usage par une personne privée et **contentieuse** dans le cadre du contrôle *a posteriori* de tous les usages.

Le souci de distinguer selon la nature de la mission de police administrative ou judiciaire en cause est louable. Cependant, ce système présente l'inconvénient de **diluer le contrôle *a priori* entre trois autorités distinctes**, rendant plus difficile une interprétation commune. Par ailleurs, confier au préfet la responsabilité d'autoriser l'usage d'une technologie de reconnaissance biométrique par une personne publique dans le cadre d'une mission de police administrative conduirait probablement à **générer de nombreux contentieux** devant la CNIL et le Conseil d'État, les risques de dérives étant importants. Au surplus, le temps juridictionnel nécessaire au traitement des contentieux nés de ce type de décisions préfectorales sera préjudiciable aux administrés, de sorte **que les éventuelles autorisations illégalement accordées par les préfectures conduiraient à l'accoutumance de la population** et à de nombreux comportements d'autocensure justement pointés par le rapport sénatorial. Il serait dès lors préférable que la **CNIL centralise l'ensemble des procédures** – à condition qu'elle bénéficie des moyens idoines.

Cette proposition de principe, qui peut s'avérer rigide en pratique, pourrait cependant être modulée s'agissant de l'utilisation de la reconnaissance faciale *a posteriori* dans le cadre

d'une mission de police judiciaire. La CNIL pourrait éventuellement, dans ce cas, conserver une fonction consultative, par l'intermédiaire d'une **procédure d'avis conforme**.

Garantir une conservation nationale des données

Un autre enjeu réside dans la **gestion des risques de détournement des données** issues de la reconnaissance faciale. Celui-ci dépasse la seule technologie de la reconnaissance biométrique, puisque les données de vidéosurveillance, voire les photographies d'usagers de réseaux sociaux du monde entier, peuvent être aisément captées par des sociétés en vue d'appliquer à grande échelle, à des fins de ciblage publicitaire ou de fourniture de services rémunérés, ces technologies de reconnaissance. Tel est notamment le cas de *Clearview AI,* société américaine se présentant comme un fournisseur de technologie de reconnaissance faciale pour les forces de l'ordre, condamnée récemment par l'Italie et Royaume-Uni pour avoir illégalement collecté et traité les données personnelles des Italiens sans base légale – en violation du RGDP[21]. La CNIL française a d'ailleurs mis en demeure, fin 2021, la société de cesser la réutilisation de photographies accessibles sur internet et de procéder à la suppression des données collectées sous deux mois [22]. Autrement dit et bien que le RGPD prévoie d'ores et déjà une protection minimale, **la sécurité des données collectées** par les futurs systèmes autorisés par la CNIL – et les autres autorités compétentes, le cas échéant – **doit constituer une priorité absolue**. Leur stockage **temporaire** et **limité aux stricts besoins** de l'autorité l'utilisant devrait notamment être réalisé dans des ***datacenters* européens voire Français**, sans l'intermédiaire de services extérieurs.

[21] V. par exemple L'Usine digitale, « Clearview AI condamné à une amende de 8,85 millions d'euros au Royaume-Uni », 23 mai 2022.
[22] CNIL, Décision n° MED-2021-134 du 26 novembre 2021 mettant en demeure la société CLEARVIEW AI.

7 PROPOSITIONS EN VUE D'UNE RÉFORME

Nous proposons à titre principal de réfléchir plus avant à l'opportunité d'engager la France sur la voie de la reconnaissance biométrique, en instaurant un débat national sur la question. À titre subsidiaire, nous recommandons de faire de l'interdiction le véritable principe, et d'encadrer plus rigoureusement les dérogations possibles.

1 Créer les conditions du débat public autour de l'opportunité de la reconnaissance faciale

Le travail parlementaire autour de la reconnaissance faciale devrait être précédé d'études approfondies, le cas échéant par l'entremise d'un financement public de recherches scientifiques, afin de déterminer la plus-value concrète, en termes d'opportunité et d'efficacité, de ces dispositifs. Les travaux préparatoires doivent prévoir clairement la possibilité de ne pas modifier la loi.

2 Instituer une Convention citoyenne pour un usage éthique des technologies numériques

Une telle Convention permettrait de réconcilier les citoyens avec le pouvoir législatif sur le thème de la reconnaissance faciale et d'autres technologies, et d'enrichir le débat public pour garantir que le régime adopté s'appuie sur une éthique du numérique, et non sur une volonté d'améliorer artificiellement l'acceptabilité de la reconnaissance faciale.

3 À titre expérimental, faire de l'interdiction le réel principe

Maintenir le principe de l'interdiction de la reconnaissance biométrique est un objectif réalisable de deux manières. Le Parlement pourrait d'abord s'abstenir de modifier le droit positif, en n'adoptant aucune réforme. Le droit de la reconnaissance faciale resterait dès lors encadré par le RGPD, qui permet peu de dérogations au principe de l'interdiction. Le législateur pourrait, subsidiairement, adopter le principe de l'interdiction en limitant les dérogations au strict nécessaire.

4 Adopter le principe dérogatoire de la « stricte nécessité » du dispositif

Dans l'hypothèse où le législateur se saisirait du sujet et opterait pour le principe de l'interdiction ou pour le principe de l'expérimentation, les dérogations ou autorisations ne devraient pouvoir survenir qu'en cas d'impossibilité d'aboutir au même résultat par un autre moyen, et non en cas de simple « inadéquation » d'un autre dispositif. Le standard de « l'inadéquation » pourrait en effet être interprété de manière restrictive.

5 Interdire l'utilisation privée de la reconnaissance faciale

Tant qu'un besoin social clair et non fondé sur des arguments économiques ne sera pas exprimé sur la question, la faculté dérogatoire de recourir à des technologies de reconnaissance faciale ne devrait pas être accordée aux personnes privées sans lien avec le service public. Cette interdiction devrait s'imposer sans dérogation possible lorsque la reconnaissance biométrique a une visée d'identification.

6 Centraliser les autorisations de recourir à la reconnaissance faciale

Si un prochain dispositif législatif devait aboutir à l'expérimentation, il serait souhaitable que la CNIL soit seule chargée de délivrer les autorisations d'utiliser la reconnaissance faciale, afin de limiter le nombre d'interlocuteurs et les risques d'interprétations divergentes. Une modulation visant à autoriser un magistrat, après avis conforme de la CNIL, à autoriser l'utilisation *a posteriori* d'un dispositif de reconnaissance faciale dans le cadre d'une enquête de police judiciaire pourrait être discutée.

7 Sécuriser les données issues de la reconnaissance biométriques

Garantir que les données issues de ces technologies ne seront conservées que pour une durée elle aussi strictement nécessaire, et au sein de centres de stockage des données (datas centers) situés en France.