Analyse des impacts de la reconnaissance faciale - Quelques éléments de méthode

Claude Castelluccia, Daniel Le Métayer

Analyse des impacts de la reconnaissance faciale
Quelques éléments de méthode

Claude Castelluccia, Daniel Le Métayer
Inria

20/11/2019

Résumé

Des progrès techniques importants ont été réalisés ces dernières années dans le domaine du traitement d'images, en particulier en reconnaissance faciale. Les déploiements et expérimentations de ce type de systèmes sont de plus en plus nombreux. Les applications concernent aussi bien le domaine régalien, notamment la sécurité publique, que les activités commerciales, comme le marketing ou le paiement. Cependant, les avis divergent sur l'usage de ces systèmes, notamment dans l'espace public. Constatant l'absence de consensus à propos d'une technologie qui peut avoir un impact significatif sur la société, de nombreuses organisations ont alerté l'opinion et demandé un débat public sur le sujet. Nous pensons qu'un tel débat est en effet nécessaire. Cependant, pour qu'il puisse être véritablement productif, il faut pouvoir confronter les arguments de manière rigoureuse en évitant, autant que faire se peut, les aprioris, et en distinguant les faits établis des suppositions ou des opinions.

L'objet du présent document est précisément de contribuer à poser les termes du débat sur des bases solides. Il ne s'agit donc pas ici de prendre position sur la reconnaissance faciale en général ni de fournir une revue exhaustive de ses applications mais de proposer des éléments de méthode, illustrés par quelques exemples.

Les applications de la reconnaissance faciale étant très variées, il est essentiel, afin d'éviter les amalgames ou les confusions, d'analyser précisément les impacts potentiels de chaque système en prenant en compte toutes ses caractéristiques ainsi que le contexte de son déploiement. Cependant, l'analyse au cas par cas ne doit pas faire perdre de vue les impacts plus « systémiques » d'une possible généralisation de la reconnaissance faciale dans notre société. Ces impacts globaux, même s'ils peuvent relever du plus long terme et être plus difficiles à évaluer, doivent aussi être analysés et mis au débat car ils peuvent justifier, selon certains, un rejet en bloc de la reconnaissance faciale.

Dans ce document, nous proposons d'abord un rapide tour d'horizon des applications de la reconnaissance faciale avant de détailler les raisons qui en font un sujet particulièrement sensible en insistant en particulier sur les risques liés à une possible généralisation de son usage. Nous présentons ensuite une démarche incrémentale, comparative et rigoureuse pour analyser les impacts d'un système de reconnaissance faciale.

- Cette démarche est incrémentale dans le sens où elle conduit à analyser successivement les impacts liés (1) à la finalité du système, (2) aux moyens choisis pour accomplir cette finalité, (3) à la l'utilisation de la reconnaissance faciale pour réaliser ces moyens et enfin (4) à la mise en œuvre particulière de la reconnaissance faciale dans le système.
- Elle est comparative dans le sens où elle préconise une évaluation des bénéfices et des risques en comparaison avec d'autres options possibles, à chaque étape. En d'autres termes, le débat ne doit pas être fermé, réduit à une alternative : accepter ou refuser le système proposé.
- Enfin, elle est rigoureuse dans le sens où elle exige de déterminer précisément le statut de chaque argument : hypothèse déjà corroborée par des mesures expérimentales ou des études reconnues par la communauté scientifique, hypothèses qui ne sont pas validées par des études suffisantes mais qui pourraient l'être et hypothèses qui relèvent de positions subjectives ou politiques qui ne sont pas susceptibles d'évaluation expérimentale.

Nous insistons aussi sur l'importance de *l'accountability*, redevabilité, ou obligation de rendre compte, qui est essentielle en matière de reconnaissance faciale. En effet, dès lors que des images sont captées, enregistrées et potentiellement analysées, aucune méthode ne sera en mesure de garantir de façon absolue que le système ne pourra pas être utilisé à mauvais escient ou produire des effets inattendus. Il est donc primordial de mettre en place des mesures techniques, juridiques et organisationnelles obligeant les opérateurs du système à rendre compte de leur utilisation. Pour être effectives, de telles mesures doivent pouvoir être contrôlées par un organe indépendant compétent et capable de fournir à toutes les parties prenantes une visibilité et des assurances sur l'utilisation des systèmes.

Dans les cas où des expérimentations préalables en situation réelle sont jugées nécessaires, celles-ci doivent également être soumises à une étude d'impact. De plus, pour être d'une véritable utilité, elles doivent respecter un protocole rigoureux. Il convient notamment de définir précisément les objectifs de l'expérimentation, les conditions dans lesquelles elle sera conduite, les hypothèses de l'étude, les critères d'évaluation des résultats et sa nécessité pour statuer ensuite sur le déploiement opérationnel du système.

Pour conclure, nous insistons sur le fait qu'il est nécessaire de faire progresser l'état de l'art pour améliorer la confiance que l'on peut placer dans les dispositifs de reconnaissance faciale et proposons plusieurs actions concrètes dans ce sens.

Nous espérons que les éléments proposés ici pourront être utiles à deux niveaux de discussion :

1. D'une part, dans le débat général qu'il est nécessaire de mettre en place sur le déploiement de la reconnaissance faciale dans nos sociétés. Ce débat doit considérer tous les impacts potentiels de cette technologie et doit être mené de manière ouverte, sans exclure l'éventualité d'un rejet global ou d'une acceptation soumise à certaines restrictions ou conditions.
2. D'autre part, l'analyse, au cas par cas, de chaque projet de déploiement (dans l'hypothèse où le débat précédent ne conduirait pas à un rejet global).

1. Introduction

Des progrès techniques importants ont été réalisés ces dernières années dans le domaine du traitement d'images, en particulier en reconnaissance faciale. Les déploiements et expérimentations de ce type de systèmes sont de plus en plus nombreux. Les applications concernent aussi bien le domaine régalien, notamment la sécurité publique, que les activités commerciales, comme le marketing ou le paiement. Parmi les exemples d'applications qui défraient la chronique, le concept de « ville sécurisée » fait l'objet de déploiements expérimentaux ou opérationnels dans de nombreux pays. Ces systèmes peuvent mobiliser la reconnaissance faciale pour identifier et suivre des personnes recherchées ou surveillées, identifier des comportements suspects ou dangereux, ou encore retrouver des personnes égarées.

De manière schématique, la reconnaissance faciale consiste à établir un lien de proximité entre deux images représentant des visages. Elle peut se décliner de différentes manières, notamment l'*authentification* – c'est à dire la vérification d'identité, l'*identification* – c'est à dire établissement de l'identité, ou encore le *traçage* – c'est à dire le suivi d'un visage sur plusieurs images vidéo. Bien entendu les avis divergent sur l'usage de ces technologies, en particulier dans l'espace public. Certains, comme le maire de Nice, s'offusquent de ne pas pouvoir utiliser des solutions qui permettraient d'identifier les individus fichés et d'éviter, voire de prévenir, des attaques terroristes[1]:

> *« Je dispose du logiciel qui permettrait dès demain matin d'appliquer la reconnaissance faciale et d'identifier des individus fichés où qu'ils se trouvent dans la ville… Pourquoi se l'interdire ? Est-ce qu'on veut prendre le risque de voir des gens mourir au nom des libertés individuelles, alors qu'on a les technologies qui permettraient de l'éviter ? »*

Dans le même esprit, James O'Neill, commissaire de police à New York, met en avant l'utilité de la reconnaissance faciale pour la recherche de suspects, en concluant que se priver des technologies du 21e siècle pour protéger une ville du 21e siècle serait commettre une injustice envers les citoyens que la police est censée protéger[2].

D'autres, comme la CNIL, dénoncent cette logique de surveillance de masse et s'inquiètent des risques démesurés sur les libertés individuelles que posent ces technologies[3] :

> *« Mais ces dispositifs, qui s'articulent parfois avec des technologies de big data, soulèvent des enjeux importants pour les droits et libertés individuelles des citoyens. Le sentiment de surveillance renforcée, l'exploitation accrue, automatisée et potentiellement à grande échelle de données personnelles, pour certaines sensibles (données biométriques), la restriction de la liberté d'aller et de venir anonymement, et le caractère prédictif de ses technologies sont autant de problématiques essentielles pour le bon fonctionnement de notre société démocratique. »*

Plusieurs villes états-uniennes ont décidé, à l'instar de San Francisco, de bannir les usages de la reconnaissance faciale par leurs services municipaux, notamment par leurs forces de police. De son côté, le comité d'éthique d'Axon a recommandé de ne pas doter les caméras-piétons des services de police de

[1] Comment des villes « hyper connectées » contrôlent l'espace public, Le Monde, 19 décembre. 2018, https://www.lemonde.fr/economie/article/2018/12/19/au-nom-de-la-smart-city-des-villes-sous-surveillance_5399527_3234.html.

[2] How facial recognition make you safer, James O'Neill, New York Times, 9 juin 2019. https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html.

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

fonctions de reconnaissance faciale [4]. D'autres voix s'élèvent pour demander l'arrêt total des déploiements de ces techniques[5]. On se trouve donc aujourd'hui dans une situation contrastée avec d'un côté des fournisseurs de technologie de reconnaissance faciale toujours plus performantes qui parviennent souvent à convaincre les décideurs politiques (et les citoyens) de leur efficacité pour améliorer la sécurité publique et de l'autre des autorités de régulation, des associations de citoyens ou des chercheurs qui tirent la sonnette d'alarme.

Constatant l'absence de consensus à propos d'une technologie qui peut avoir un impact significatif sur la société, de nombreuses organisations, aussi bien publiques (CNIL, AINow, etc.) ou associatives (ACLU, EFF, La Quadrature du Net, etc.) que privées (Google, Microsoft, etc.) ont alerté l'opinion et demandé un débat public sur le sujet. Par exemple, la CNIL [6] « appelle *d'urgence à un débat démocratique sur cette problématique, et à ce que le législateur puis le pouvoir réglementaire se saisissent de ces questions afin que soient définis les encadrements appropriés, en recherchant le juste équilibre entre les impératifs de sécurisation, notamment des espaces publics, et la préservation des droits et libertés de chacun* ».

Nous pensons qu'un tel débat est en effet nécessaire. Cependant, pour qu'il puisse être véritablement productif, il faut pouvoir confronter les arguments de manière rigoureuse en évitant, autant que faire se peut, les aprioris, et en distinguant les faits établis des suppositions ou des opinions. Il nous semble en effet que les arguments en la matière mêlent souvent différents niveaux de discours – certains visent par exemple la reconnaissance faciale en général, d'autres des contextes d'application ou des systèmes particuliers – et ne font pas toujours le départ entre les éléments objectifs et ce qui relève de positions subjectives ou politiques.

Les applications de la reconnaissance faciale étant très variées, il est essentiel, afin d'éviter les amalgames ou les confusions, d'analyser précisément les impacts potentiels de chaque système. Pour ce faire, il faut prendre en compte non seulement les caractéristiques techniques du système mais aussi son encadrement et le contexte de son déploiement. Par exemple, l'utilisation de la reconnaissance faciale pour une application d'identité numérique, comme ALICEM, introduit des risques qui sont, par nature, très différents de ceux qui résultent d'un système visant à sécuriser l'espace public, comme celui qui a été expérimenté à Nice. Ces applications n'ont pas les mêmes finalités, n'utilisent pas les mêmes formes de reconnaissance faciale et leurs mises en œuvre sont très différentes. Par ailleurs, une application de reconnaissance faciale ne doit pas être envisagée comme un pur objet technique mais comme un système socio-technique, dont il importe également de considérer les dimensions économiques, sociales et psychologiques[7]. Il convient aussi de noter que l'analyse au cas par cas, qui devrait être un préalable à tout déploiement, ne doit pas faire perdre de vue les impacts plus « systémiques » d'une possible généralisation de la reconnaissance faciale dans notre société. Ces impacts globaux, même s'ils relèvent souvent du plus long terme et sont plus difficiles à évaluer, doivent aussi être analysés et mis au débat car ils pourraient justifier, selon certains, un rejet en bloc de la reconnaissance faciale.

[4] First report of the Axon AI & Policing Technology Ethics Board, juin 2019.
[5] Facial recognition is the perfect tool for oppression, W. Hartzog, E. Selligner, Medium.com, http://cyberlaw.stanford.edu/publications/facial-recognition-perfect-tool-oppression.
[6] https://www.cnil.fr/fr/la-cnil-appelle-la-tenue-dun-debat-democratique-sur-les-nouveaux-usages-des-cameras-video.
[7] Il importe par exemple de distinguer la perception des risques ou de l'amélioration de la sécurité apportée par un dispositif de la réalité de ces risques et de l'effet réel du dispositif. Voir, par exemple, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2508019.

La CNIL a récemment publié une note sur la reconnaissance faciale qui présente quelques éléments techniques, juridiques et éthiques qui doivent être pris en compte dans ce débat[8]. Cette note précise en particulier le cadre juridique dans lequel les expérimentations et le déploiement d'applications utilisant la reconnaissance faciale doivent être réalisés. Le présent document est complémentaire à la note de la CNIL dans le sens où il propose une démarche systématique pour l'analyse des impacts des applications de reconnaissance faciale. Notre objectif est essentiellement de contribuer à poser les termes du débat sur des bases solides. Il ne s'agit donc pas ici de prendre position sur la reconnaissance faciale en général ni de fournir une revue exhaustive de ses applications mais de proposer des éléments de méthode, illustrés par quelques exemples. Les exemples[9] choisis ici concernent principalement l'usage de la reconnaissance faciale dans le cadre de services publics, mais la démarche que nous proposons est générale et s'applique aussi bien aux déploiements réalisés par des acteurs privés.

Nous espérons que les éléments proposés dans ce document pourront être utiles à deux niveaux de discussion :

1. D'une part, dans le débat général qu'il est nécessaire de mettre en place sur le déploiement de la reconnaissance faciale dans nos sociétés. Ce débat doit considérer tous les impacts potentiels de cette technologie et doit être mené de manière ouverte, sans exclure l'éventualité d'un rejet global ou d'une acceptation soumise à certaines restrictions ou conditions.
2. D'autre part, pour l'analyse, au cas par cas, de chaque projet de déploiement (dans l'hypothèse où le débat précédent ne conduirait pas à un rejet global de la reconnaissance faciale).

Avant de présenter ces éléments de méthode dans la partie 3, nous résumons dans la partie 2 les principaux types de reconnaissance faciale et les enjeux liés à leurs déploiements. Nous concluons avec une mise en perspective et quelques propositions concrètes dans la partie 4. Le lecteur intéressé pourra aussi trouver dans l'annexe 1 une classification des modalités d'application de la reconnaissance faciale et dans l'annexe 2 un exemple montrant comment les matrices d'éthique peuvent être utilisées pour synthétiser les impacts identifiés lors de l'analyse.

[8] https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux.

[9] Même si les exemples que nous considérons dans cette note s'inspirent de certains développements récents, ils ne correspondent pas forcément à des systèmes réels (dont les choix techniques ne sont pas toujours connus). Ces exemples doivent donc être considérés comme des systèmes hypothétiques fournis à titre d'illustration.

2. La reconnaissance faciale : de quoi parle-t-on ?

L'expression « reconnaissance faciale » est très générique et englobe des situations extrêmement variées. Il nous paraît utile d'en présenter un rapide tour d'horizon (partie 2.1) avant de détailler les raisons qui font de la reconnaissance faciale un sujet particulièrement sensible (partie 2.2) en insistant en particulier aux risques liés à une possible généralisation de son usage (partie 2.3).

2.1 Les différents types de reconnaissance faciale

La reconnaissance faciale est en fait un type parmi d'autres d'analyse d'images. Des systèmes qui ne relèvent pas de la reconnaissance faciale stricto sensu peuvent avoir pour but d'inférer, à partir de visages ou de traits physiques, des informations biographiques (âge, genre, etc.), des émotions, des profils psychologiques, ou encore des comportements (bagarres, agressions, etc.). Il existe également des méthodes consistant à identifier des personnes à partir d'éléments vestimentaires. Dans ce rapport, nous nous intéressons plus particulièrement aux techniques de reconnaissance faciale, c'est à dire aux applications qui, schématiquement, consistent à établir un lien de proximité entre deux images représentant des visages. Cependant, la démarche que nous proposons peut être appliquée aux autres types de systèmes, notamment pour analyser les questions spécifiques posées par les techniques d'analyse de comportement.

La reconnaissance faciale utilise des algorithmes qui analysent les visages présents sur des photographies ou des vidéos pour en extraire un ensemble de traits distinctifs. Ces attributs physiques, comme la distance entre les yeux ou la forme du menton, sont ensuite codés sous forme de représentations mathématiques, communément appelées « gabarits ». Les gabarits, qui ne contiennent que les caractéristiques importantes des visages, sont soit stockés, soit comparés à ceux qui sont contenus dans une base de données.

On peut distinguer différents types de reconnaissance faciale selon les deux paramètres que sont le nombre de personnes concernées[10] dans les images captées « in vivo » (X) et le nombre de personnes concernées dans la base de données (Y), ce qu'on peut dénoter par (X,Y):

- Authentification (1:1) : il s'agit dans ce cas de vérifier une identité. C'est ce que fait par exemple le possesseur d'un téléphone mobile offrant la fonctionnalité de reconnaissance faciale pour procéder au déverrouillage : la photographie de son visage est comparée à celle qui est enregistrée sur l'appareil.
- Identification (1:N) : on se focalise alors sur une personne dont on cherche l'identité dans une base de données. Il peut s'agir d'un suspect dont on souhaite comparer la photographie avec celles qui sont contenues dans une base de données de personnes recherchées. On peut aussi généraliser à une recherche non ciblée (M:N), comme l'analyse systématique d'images de vidéosurveillance pour tenter de repérer des visages contenus dans une base de personnes recherchées. Une autre déclinaison, plus extrême, serait l'association d'une identité à chaque visage apparaissant sur des images, par exemple via des lunettes de réalité augmentée (le nombre de personnes concernées dans la base serait alors l'ensemble de la population).
- Traçage (1:0) : on peut aussi appliquer la reconnaissance faciale pour comparer plusieurs images captées in vivo, par exemple pour suivre les déplacements d'un pickpocket ou d'un

[10] C'est à dire dont les visages sont comparés.

agresseur sur des images de vidéosurveillance. Dans ce cas, il n'est pas nécessaire de disposer d'une base de données de photographies.

Par ailleurs, la reconnaissance faciale peut être utilisée soit en « temps réel », c'est à dire lors de la capture des images[11], soit a posteriori[12]. La seconde utilisation correspond au scenario où les images d'un système de vidéosurveillance sont exploitées à la suite d'un délit pour identifier les potentiels auteurs. Cette distinction a notamment surgi aux États-Unis après que plusieurs villes ont décidé de bannir l'usage de toute forme de reconnaissance faciale par les services municipaux, notamment la police : certains ont appelé à faire la distinction entre ces deux formes d'utilisation et à permettre la seconde pour ne pas priver la police d'outils efficaces [13]. Le lecteur intéressé pourra trouver dans l'annexe 1 une catégorisation plus complète montrant la diversité des modalités d'application de reconnaissance faciale.

Les risques induits par les différentes utilisations sont bien entendu variables et plus ou moins acceptables. Par exemple, les systèmes qui utilisent des bases de données internes introduisent généralement des risques supplémentaires (notamment des risques de fuite). De même, les risques croissent avec le nombre de personnes concernées (dans la base de données et dans les images captées in vivo). Certaines applications peuvent donc être plus acceptables que d'autres. Par exemple, Wojciech Wiewiórowski, le contrôleur européen de la protection des données, distingue le recours à la reconnaissance faciale pour l'authentification, notamment aux contrôles aux frontières, qui lui semble raisonnable, de son utilisation à des fins d'identification ou de recherche dans l'espace public, qui lui paraît beaucoup plus discutable[14].

2.2 Pourquoi la reconnaissance faciale pose-t-elle des questions spécifiques ?

Les inquiétudes soulevées par le développement de la reconnaissance faciale tiennent à une combinaison de caractéristiques qui font de ces systèmes des menaces particulières pour les libertés publiques :

- Il s'agit d'une technique biométrique, qui exploite des traits du corps humain qu'une personne ne peut pas changer, tout du moins pas facilement, à la différence d'autres attributs numériques qui peuvent être aussi utilisés pour la tracer (identifiants de téléphones mobiles, cookies, etc.). Le caractère sensible des données biométriques est d'ailleurs reconnu par le droit. Par exemple, le Règlement général sur la protection des données (RGPD)[15] interdit le traitement de données biométriques à des fins d'identification sauf si une des dix exceptions listées dans l'article 9(2) peut être évoquée. De plus, la Chartre des droits fondamentaux de l'Union européenne, qui consacre le respect de la vie privée et la protection des données personnelles dans ses articles 7 et 8, spécifie que « toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général » (article 52).

[11] On appelle parfois cette utilisation « surveillance faciale » : Here's a way forward on Facial Recognition, oct. 31 2019, https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html.
[12] On appelle parfois cette utilisation « identification faciale ».
[13] https://www.nytimes.com/2019/10/31/opinion/facial-recognition-regulation.html. https://edition.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.
[14] https://edps.europa.eu/node/5551.
[15] https://www.cnil.fr/fr/reglement-europeen-protection-donnees.

- Contrairement à d'autres traits biométriques, comme les empreintes digitales ou génétiques, les photographies du visage peuvent être saisies à l'insu d'une personne, à distance, sans contact et de manière très économique. De fait, elles le sont de plus en plus fréquemment, notamment via la multitude de caméras de vidéosurveillance qui sont déployées dans la plupart des pays. Le visage est aussi la partie du corps la plus visible, la plus difficile à masquer.
- Le consentement, qui peut être une base légale de collecte de données personnelles, est très difficile à mettre en œuvre pour la reconnaissance faciale dans l'espace public[16]. Les affichettes informant de la présence de caméras de vidéosurveillance sont inopérantes comme mode d'information et ne permettent pas d'effectuer un choix libre et éclairé puisque le refus du consentement ne peut se traduire que par l'évitement de la zone concernée.
- Contrairement à d'autres traits biométriques, qui exigent de passer par une phase spécifique dite d'enrôlement, c'est à dire de saisie initiale de l'information, les photographies de visages sont déjà disponibles à grande échelle : beaucoup d'acteurs publics ou privés peuvent disposer d'une grande quantité d'images qui ont pu être collectées pour d'autres finalités ou qui sont accessibles via internet[17]. À titre d'exemple, la moitié des citoyens états-uniens adultes figurent dans des bases de données de photographies accessibles par le FBI, notamment celles des permis de conduire[18]. En France, tout citoyen demandant une carte d'identité est désormais enregistré, avec sa photographie, dans le fichier des Titres électroniques sécurisés (TES).
- Malgré les grands progrès qui ont été réalisés ces dernières années, notamment grâce au développement de l'apprentissage profond et à la possibilité d'exploiter de grosses bases de données d'images, les techniques de reconnaissance faciale restent très imparfaites. Selon les paramétrages choisis et le contexte de prise de vue, elles peuvent présenter des taux de faux positifs (personnes reconnues à tort) et/ou de faux négatifs (personnes non reconnues à tort) très importants et variables selon les catégories de population. Ainsi, certains systèmes fonctionnent de manière plus satisfaisante sur des personnes à la peau blanche que sur des personnes à la peau foncée, sur des hommes que sur des femmes ou encore sur des quadragénaires que sur des adolescents. Ces biais conduisent à des discriminations envers certaines populations qui sont désormais bien documentées[19].

Cet ensemble de caractéristiques a amené Woodrow Hartzog, professeur de droit à l'université de Samford (USA), à qualifier la reconnaissance faciale de « mécanisme de surveillance le plus dangereux

[16] Des solutions existent pour certaines applications et services: https://www.theregister.co.uk/2019/06/10/microsoft_windows_photos_facial_recognition_consent/.

[17] Voir par exemple : https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html, https://www.vice.com/en_us/article/a3x4mp/microsoft-deleted-a-facial-recognition-database-but-its-not-dead, ou https://megapixels.cc/datasets/megaface/.

[18] The perpetual line-up. Unregulated police face recognition in America, Georgetown Law Center on Privacy & Technology, octobre 2016. https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf.

[19] Gender shades : intersectional accuracy disparities in commercial gender classification, J. Buolamwini, G. Gebru, Machine Learning Research,No 81, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. AI Now Report 2018, https://ainowinstitute.org/AI_Now_2018_Report.pdf. AI experts question Amazon's facial-recognition technology, New York Times, 3 avril 2019, https://www.nytimes.com/2019/04/03/technology/amazon-facial-recognition-technology.html. Amazon's face recognition falsely matched 28 members of congress with mugshots, ACLU, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

qui ait été inventé »[20]. De son côté, l'association britannique Liberty voit en elle l' « arsenic dans l'eau de la démocratie »[21]. Ces inquiétudes n'ont pas empêché les initiatives de se multiplier, souvent dans un certain flou juridique (voire de manière illégale), alimentées par les présentations attrayantes des promoteurs de la reconnaissance faciale. Les arguments promotionnels les plus utilisés sont l'amélioration de la sécurité publique, notamment par la possibilité d'analyser les images de vidéosurveillance, le gain de temps, par exemple pour les contrôles aux frontières, et la simplification de la vie des citoyens, par exemple en leur permettant d'entrer dans un local sans avoir à montrer un badge ou de sortir d'un magasin avec leurs achats sans avoir à passer par une caisse. Ce recours croissant aux dispositifs de reconnaissance faciale fait naître une crainte diffuse, plus profonde, celle d'une généralisation de cette technologie qui pourrait devenir inéluctable et comporterait des conséquences majeures sur nos sociétés.

2.3 Risques liés à une possible généralisation de l'usage de la reconnaissance faciale

Toute analyse de risques sur l'opportunité d'utiliser un système de reconnaissance faciale particulier doit aussi intégrer une réflexion plus globale de l'effet du déploiement de cette technologie sur nos sociétés. Occulter cette étape reviendrait à céder au déterminisme technologique ambiant en tenant pour acquis que le développement de la reconnaissance faciale serait inéluctable[22]. Cette étape préalable est d'autant plus nécessaire que, même si on tente d'encadrer l'usage de ces systèmes par des moyens techniques et juridiques, la possibilité d'étendre ultérieurement leur utilisation ne pourra jamais être écartée totalement. Ces extensions peuvent avoir lieu de multiples manières, par exemple en utilisant des données collectées sur des réseaux sociaux[23] ou des bases de données constituées à l'origine pour des finalités différentes, comme on l'a vu plus haut avec le FBI, ou encore en élargissant les finalités autorisées pour une base de données, comme on l'a constaté avec le fichier national des empreintes génétiques (FNAEG) qui a été étendu par une demi-douzaine de lois successives[24] ou avec le fichier des titres électroniques sécurisés (TES) et celui du traitement des antécédents judiciaires (TAJ)[25]. L'extension peut aussi consister à ajouter de nouvelles fonctionnalités à un système existant, par exemple en généralisant la reconnaissance faciale utilisée pour le contrôle des passeports aux paiements

[20] Facial recognition is the perfect tool for oppression, W. Hartzog, E. Selligner, Medium.com, http://cyberlaw.stanford.edu/publications/facial-recognition-perfect-tool-oppression.

[21] https://www.theguardian.com/technology/2019/jun/07/facial-recognition-technology-liberty-says-england-wales-police-use-should-be-banned.

[22] À titre d'illustration, le mot « inéluctable » apparaît deux fois à ce sujet dans la Note No14 de l'Office parlementaire d'évaluation des choix scientifiques et technologiques consacrée à la reconnaissance faciale (juillet 2019) ; http://www2.assemblee-nationale.fr/content/download/82754/922439/version/1/file/Note+Scientifique+-+Reconnaissance+Faciale+-+VF+19072019.pdf.

[23] De nombreux cas ont été révélés. Voir par exemple : https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html, https://www.vice.com/en_us/article/a3x4mp/microsoft-deleted-a-facial-recognition-database-but-its-not-dead, ou https://megapixels.cc/datasets/megaface/. En France, un article du projet de loi de finances a également été adopté récemment pas l'Assemblée nationale, en dépit de l'avis de la CNIL : il a pour but de permettre aux services fiscaux et douaniers de collecter des données sur les réseaux sociaux pour détecter certaines fraudes: https://www.lemonde.fr/pixels/article/2019/11/06/la-surveillance-des-reseaux-sociaux-contre-la-fraude-fiscale-passe-un-cap-a-l-assemblee_6018284_4408996.html.

[24] https://www.cnil.fr/fr/donnees-genetiques-les-reserves-de-la-cnil-sur-lamendement-portant-sur-lelargissement-du-fnaeg.

[25] https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/.

dans tout un aéroport, puis dans toute la ville[26], ou en intégrant la détection de comportements suspects à un système de vidéosurveillance. On peut se demander si ces extensions seront forcément acceptées des populations mais l'expérience montre que, quand elles sont réalisées de manière très progressive et présentées à chaque fois comme des évolutions naturelles, elles ne rencontrent pas d'opposition majeure. Comme la grenouille de la fable, la société se laisse peu à peu engourdir pour finir ébouillantée. Certains pensent même que les promoteurs de ces techniques appliquent délibérément cette stratégie en multipliant les usages d'agrément, apparemment anodins, ou facilitant la vie des consommateurs, comme le déverrouillage d'un téléphone mobile ou le paiement au supermarché, pour accoutumer la population à ces techniques et rendre naturel, voire inévitable, le passage progressif à des usages plus massifs. Enfin, de manière générale, quand les humains ont à mettre en balance des avantages immédiats et identifiables, si mineurs fussent-ils, et des préjudices possiblement graves, mais incertaines et vagues, force est de constater que les seconds pèsent généralement peu.

Si on admet l'hypothèse qu'aucun obstacle technique, juridique ou social ne pourrait s'opposer à la tendance, déjà constatée, à la généralisation du recours à la reconnaissance faciale, il est important d'analyser les conséquences possibles d'une telle généralisation sur la société. On peut notamment se poser les questions suivantes :

1. Quelles sont les effets possibles sur la société d'une généralisation du recours à la reconnaissance faciale (sans jugement de valeur à ce stade) ?
2. Ces effets sont-ils désirables ou pas ?
3. Peut-on prévenir ou réduire les effets négatifs et favoriser ou amplifier les effets positifs ?
4. Au vu des réponses aux questions précédentes, faut-il bannir l'usage des technologies de reconnaissance faciale (de façon sélective ou générale) ?
5. Dans l'hypothèse où elle peut être utilisée, quels grands principes doit-on appliquer au développement et au déploiement de la reconnaissance faciale ? Quelles mesures techniques, juridiques et/ou organisationnelles, peut-on mettre en place pour limiter les risques d'extension incontrôlée ?

À cet égard, il est important de prendre en compte le fait qu'un grand nombre de caméras de vidéosurveillance sont déjà déployées dans l'espace public. A l'heure actuelle, ces images sont visualisées, soit en direct par les agents des centres de supervision[27], soit a posteriori par des enquêteurs. L'analyse des impacts de la reconnaissance faciale dans ce contexte doit donc comparer la situation actuelle (supervision et reconnaissance par des agents humains) à une mise en œuvre reposant sur la reconnaissance automatique. Les avantages et les inconvénients de chaque option doivent être pesés, en considérant les mesures de protection qui peuvent être envisagées dans les deux cas et sans négliger les risques liés à la situation actuelle. En effet, plusieurs études ont montré les dérives graves auxquelles donnent lieu la supervision par des opérateurs humains[28]. Le remplacement de certaines tâches par des traitements automatiques pourrait éventuellement permettre de limiter ces dérives, ou tout au moins de les rendre plus traçables, si des mesures de protection suffisantes sont mises en œuvre. Inversement, si une étude d'impact conduit à la conclusion que tout usage de ces images de vidéosurveillance représente un risque disproportionné, que les analyses soient réalisées par des opérateurs humains ou des systèmes

[26] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/how-tsas-facial-recognition-plan-will-go-far.
[27] Par exemple pour coordonner les équipages sur le terrain ou pour le suivi en temps réel des grandes manifestations dans le cas du Centre de Supervision Urbain de Nice : https://www.nice.fr/fr/securite/le-centre-de-supervision-urbain.
[28] Face Off, https://www.eff.org/wp/law-enforcement-use-face-recognition.

de reconnaissance faciale, alors c'est le dispositif de vidéosurveillance lui-même qu'il faudrait remettre en cause.

La tentation de la surveillance n'est pas l'apanage exclusif des institutions. Il ne faut pas négliger la surveillance interpersonnelle, parfois appelée « sousveillance »[29]. Ainsi, selon l'anthropologue Judith Donath[30], le fait de se promener masqué ou le visage couvert sur la voie publique est déjà mal accepté, il crée un sentiment d'insécurité, ce qui a amené certains pays à légiférer en la matière. Selon elle, il pourrait en être de même demain avec le fait de croiser une personne qu'on ne pourrait rattacher à une identité ou un profil, par exemple à travers des lunettes de réalité augmentée. On pourrait ainsi évoluer dans une ville comme dans un village où chacun aurait une forme de connaissance de chacun, où on ne rencontrerait jamais de parfait « étranger ». Il s'agirait assurément d'une évolution majeure dans notre manière de concevoir l'espace public avec de multiples conséquences sur les relations sociales. Certaines pourraient être considérées comme positives, comme le fait de se sentir plus en sécurité, voire de nouer plus facilement connaissance avec des personnes qu'on n'a jamais rencontrées, sur la base de goûts ou d'amis communs révélés par les profils. D'autres seraient négatives, comme l'impossibilité de se déplacer anonymement, le risque de stigmatisation selon les informations contenues dans les profils (condamnations pénales, pays d'origine, religion, préférences sexuelles, etc.), les nouvelles formes d'insécurité auxquelles ces profils pourraient donner lieu, le risque de conformisme induit par cette transparence totale, etc.

[29] http://wearcam.org/acmmm2004sousveillance/mann.pdf.
[30] How facial recognition could tear us apart, Judith Donah, entretien Medium, https://onezero.medium.com/how-facial-recognition-tech-could-tear-us-apart-c4486c1ee9c4.

3. Analyse d'impact incrémentale

Après avoir évoqué les risques liés à l'usage de la reconnaissance faciale en général, nous présentons maintenant quelques éléments de méthode pour aborder l'analyse d'impact d'un système particulier. Nous fournissons d'abord une vue d'ensemble de notre démarche (partie 3.1) avant d'en décrire plus précisément chaque étape et de les illustrer à travers quelques exemples (partie 3.2).

3.1 Une démarche en quatre étapes

La démarche que nous proposons présente comme caractéristiques principales le fait d'être est d'être incrémentale, comparative et rigoureuse.

Démarche incrémentale : il nous paraît utile, pour mieux séparer les enjeux, de distinguer quatre niveaux d'analyse :

1. **La finalité**

   L'objectif de cette phase est d'analyser et de questionner la finalité déclarée du système, indépendamment des moyens utilisés pour l'accomplir et de l'utilisation de la reconnaissance faciale, avec un esprit critique, pour éventuellement la remettre en cause ou la préciser. Des exemples de finalités pourraient être « empêcher qu'un terroriste puisse commettre un attentat dans un train » ou « assurer que seules les personnes habilitées peuvent pénétrer dans un bâtiment ».

   Des exemples de questions essentielles à se poser à ce stade sont :
   - Est-ce que la finalité déclarée est licite ?
   - Quels sont les bénéfices attendus de la finalité et quels intérêts sert-elle (privés ou publics, état, citoyens, etc.) ?
   - Les bénéfices attendus sont-ils d'importance majeure ou relative ? Est-ce que la finalité est vraiment une priorité ?
   - Quels sont les impacts possibles, positifs ou négatifs, à court ou long terme, de la finalité pour toutes les parties prenantes[31], indépendamment des moyens adoptés pour l'accomplir ?
   - Les impacts sont-ils d'importance majeure ou mineure ?
   - En fonction de ces éléments, la finalité est-elle légitime ?

2. **Le moyen adopté pour accomplir la finalité**

   L'objectif de cette phase est d'analyser et de questionner le moyen adopté pour accomplir la finalité, toujours sans référence à une technologie particulière comme la reconnaissance faciale. Le moyen décrit la stratégie adoptée pour accomplir la finalité, indépendamment d'une mise en œuvre particulière, par un système informatique et/ou par des opérateurs humains. Par exemple, un moyen

[31] On entend par « parties prenantes » toutes les entités, personnes ou groupes de personnes, qui peuvent être affectées par un système, directement ou indirectement, de façon active (commanditaire, développeur, opérateur, utilisateur, etc.) ou passive (citoyen, passager, etc.). On peut aussi inclure l'État ou la société parmi les parties prenantes (voir annexe 2).

hypothétique pour accomplir la finalité « empêcher qu'un terroriste puisse commettre un attentat dans un train » pourrait être de « contrôler, lors de l'accès au quai, que (1) le visage du voyageur correspond à la photographie liée à un titre de transport valide, et (2) cette photographie ou l'identité du voyageur ne correspond pas à un terroriste figurant dans un fichier de police ».

Il s'agit soit de remettre en cause ces moyens, soit de les préciser, de les améliorer ou d'en proposer des alternatives. Dans l'exemple précédent, comme nous le détaillons dans la partie 3.2.2, on pourrait argumenter que le moyen proposé n'est pas approprié à la finalité déclarée car un contrôle d'accès n'est pas suffisant pour éviter des attentats terroristes.

Des exemples de questions essentielles à se poser à ce stade sont :

- Le moyen permet-il d'accomplir effectivement la finalité ? Quels sont les éléments de preuve qui en attestent ?
- Quels sont les impacts possibles, positifs ou négatifs, à court ou long terme, des moyens pour toutes les parties prenantes, indépendamment du fait que la reconnaissance faciale soit utilisée pour réaliser ce moyen ?
- Ces impacts sont-ils d'importance majeure ou mineure ?
- Quels pourraient-être des moyens alternatifs pour accomplir la finalité ?
- En fonction de ces éléments, le moyen est-il proportionné pour accomplir la finalité ?

3. L'usage de la technologie de reconnaissance faciale pour réaliser le moyen

L'objectif de cette phase est de questionner l'usage de la reconnaissance faciale pour réaliser le moyen proposé (sans référence à une mise en œuvre particulière de la technologie). Dans l'exemple du train évoqué plus haut, la reconnaissance faciale pourrait être intégrée dans un portique par lequel passent les voyageurs pour parvenir aux quais. Lorsque que le voyageur se présente au portique, une photographie est prise automatiquement et un visage en est extrait. Cette extraction est ensuite utilisée pour vérifier dans une base de données qu'il existe bien une réservation pour une personne qui possède ce visage et que celui-ci ne figure pas dans le fichier de police.

On fait à ce stade l'hypothèse que la reconnaissance faciale est mise en œuvre de manière « parfaite », notamment qu'elle est précise, exempte de biais et ne peut pas être compromise. Les questions abordées lors de cette phase sont donc de nature théorique plus qu'expérimentale : elles concernent les avantages et les risques intrinsèques de la reconnaissance faciale.

Des exemples de questions essentielles à se poser à ce stade sont :

- La reconnaissance faciale permet-elle de réaliser effectivement le moyen proposé ?
- Quels sont les impacts possibles, positifs ou négatifs, à court ou long terme, de la reconnaissance faciale pour toutes les parties prenantes ? Sont-ils d'importance majeure ou mineure ?
- Cette application de la reconnaissance faciale est-elle susceptible de donner lieu à des extensions ou des généralisations ? Quels en seraient les impacts ? Peut-on prévenir ou réduire les effets négatifs et favoriser ou amplifier les effets positifs ?
- Quelles technologies alternatives pourraient être mobilisées pour réaliser le moyen ?
- En fonction de ces éléments, l'usage de la reconnaissance faciale est-il proportionné pour réaliser le moyen ?

4. **La mise en œuvre d'une solution de la reconnaissance faciale dans un système particulier**

L'objectif de cette phase est de questionner la mise en œuvre du système de reconnaissance faciale en considérant les détails techniques des solutions et produits utilisés et le contexte de son déploiement. Les questions abordées dans cette phase sont donc de nature concrète : elles concernent les avantages et les risques de la solution choisie et de son déploiement.

Des exemples de questions essentielles à se poser à ce stade sont :

- Les spécifications techniques du système choisi sont-elles connues ?
- Les performances (fiabilité, sécurité, équité, etc.) du système déployé ont-elles été évaluées rigoureusement ?
- Le système est-il transparent et les résultats sont-ils explicables ?
- Les mesures de contrôle (*accountability*) sont-elles suffisantes ?
- Quels sont les impacts possibles, positifs ou négatifs, à court ou long terme, des faiblesses de la mise en œuvre du système pour toutes les parties prenantes ? Sont-ils d'importance majeure ou mineure ?
- Peut-on prévenir ou réduire les effets négatifs et favoriser ou amplifier les effets positifs ? Est-ce que des contre-mesures suffisantes ont été mises en place ?
- Quel est le coût financier du système (développement, déploiement, maintenance, etc.) ? Est-il acceptable au vu de la finalité ?
- D'autres choix de mise en œuvre pourraient-ils offrir un meilleur équilibre entre les risques et les bénéfices (à un coût acceptable) ?
- En fonction de ces éléments, la solution est-elle acceptable ?
- Sinon, est-ce que, en l'état de l'art, d'autres options de mise en œuvre de la reconnaissance faciale pourraient être acceptables ?

Ces quatre niveaux, qui constituent quatre étapes de la solution, sont représentés dans la figure 1. Chacun d'entre eux doit être décrit précisément et analysé en considérant aussi bien les bénéfices que les risques, à court et long terme, pour toutes les parties prenantes, et en premier lieu les personnes qui peuvent être affectées par le traitement[32]. Notons que, même si cette possibilité n'est pas représentée dans la figure, ce processus incrémental peut en réalité donner lieu à des itérations quand l'analyse amène à réviser certains choix, par exemple de moyen ou de mode d'utilisation de la reconnaissance faciale.

La figure 1 inclut également une cinquième étape, la réalisation d'une analyse d'impact sur la protection des données (AIPD), requise par le RGPD et par la Directive Police-Justice pour les applications qui traitent des données biométriques. Notons que, même s'il ne s'agit pas de son objectif premier, la démarche proposée dans cette note pourra servir à alimenter une AIPD dans le sens où elle comprend, comme une AIPD (article 35 du RGPD), une « description systématique des opérations de traitement envisagées et des finalités du traitement » et « une évaluation de la nécessité et de la proportionnalité des opérations de traitement en regard des finalités ». Cependant, la vocation de notre méthode est différente puisqu'il ne s'agit pas seulement d'« évaluer les risques pour les droits et libertés des personnes concernées » et d' « assurer la protection des données à caractère personnel » comme le

[32] Même si cette note fournit quelques éléments (voir partie 3.2), les méthodologies d'analyse utilisées pour chacune des quatre étapes devront être développées rigoureusement. Il conviendra, par exemple, d'identifier et d'évaluer les différents types de risques, ainsi que leur amplitude et leur probabilité d'occurrence, les personnes affectées par ces risques, etc. Des matrices d'éthique peuvent servir de support à cette évaluation (voir annexe 2).

prévoit le RGPD. Ainsi, nous proposons de mettre systématiquement en regard les bénéfices et les risques, aux quatre niveaux évoqués ici, et nous insistons sur les impacts globaux, positifs et négatifs, sur la société. Notre analyse va au-delà du traitement des données personnelles et considère également des questions d'ordre éthique, comme celles d'équité[33]. Nous préconisons également le questionnement, qui peut aller jusqu'à la remise en cause, de la finalité aussi bien que des moyens, de l'usage de la reconnaissance faciale ou de sa mise en œuvre. Inversement, nous ne nous étendons pas ici sur la dimension juridique, comme le fondement légal du traitement, qui devra être traitée spécifiquement dans le cadre d'une AIPD.

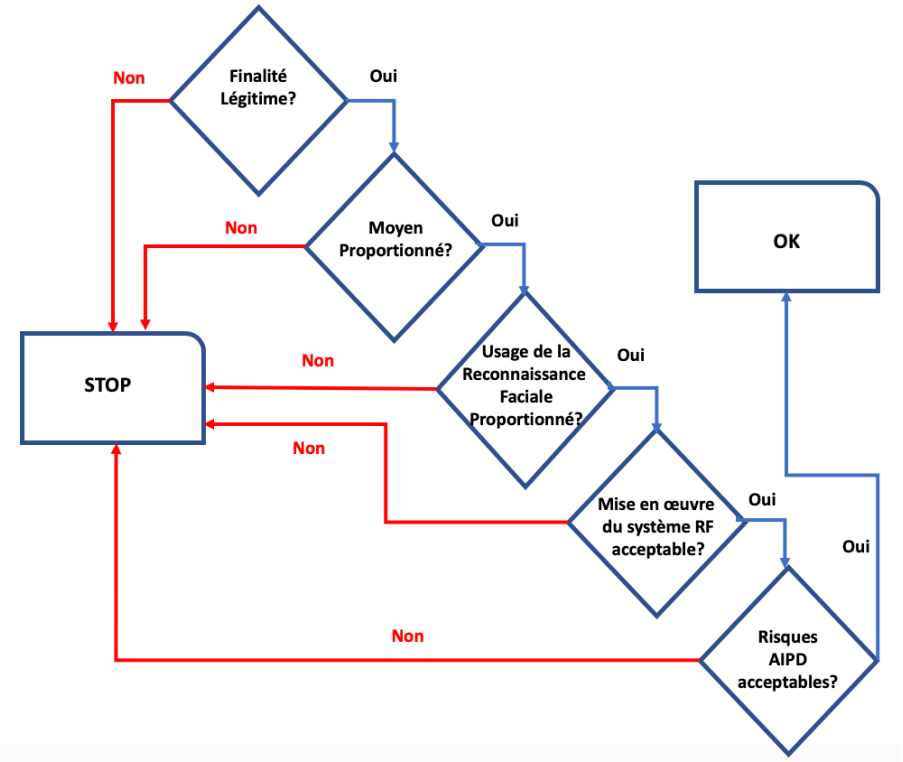

Figure 1. Méthodologie d'analyse des impacts (4 étapes + AIPD)

Le séquencement en quatre étapes favorise la réflexion en obligeant à clarifier les causes des impacts envisagés, positifs ou négatifs, et à caractériser ainsi la portée des différents arguments.

En effet, il peut se trouver des situations où la finalité elle-même est discutable : ce pourrait être le cas, par exemple, d'un projet visant à attribuer un niveau de confiance à tout citoyen, à l'instar du score social en cours de déploiement en Chine. Dans d'autres situations, la finalité peut être acceptable mais les moyens contestables, indépendamment de leur réalisation par la reconnaissance faciale : dans l'exemple évoqué plus haut, on peut contester le fait que la recherche des visages des passagers dans un

[33] Voir la matrice d'éthique présentée dans l'annexe 2.

fichier de réservations et un fichier de police soit un moyen effectif de réduire le risque d'attentat, puisqu'un terroriste peut se munir d'un titre de transport valide et ne figurer dans aucun fichier de police. Par ailleurs, ce moyen est inopérant vis à vis d'assaillants internes (employé de la société de chemins de fer, par exemple). Le bénéfice à espérer de tout système reposant sur une telle stratégie est donc faible. Dans d'autres cas, c'est l'usage de la reconnaissance faciale en tant que telle, indépendamment de ses performances actuelles ou futures, qui peut être contesté : ainsi, un avis récent de la CNIL, concernant une expérimentation de la reconnaissance faciale à l'entrée de deux lycées de la Région PACA est essentiellement motivé par le fait que « les objectifs de sécurisation et la fluidification des entrées dans ces lycées peuvent être atteints par des moyens bien moins intrusifs en termes de vie privée et de libertés individuelles, comme par exemple un contrôle par badge »[34]. La position de Woodrow Hartzog[35] porte aussi sur la reconnaissance faciale en tant que telle : selon lui, son caractère intrinsèquement invisible, ubiquitaire et opaque, plus le fait qu'il existe déjà de grandes quantités de photographies disponibles dans des bases diverses, est de nature à créer un sentiment de surveillance généralisée qui justifie qu'on l'interdise absolument. Finalement, certains impacts peuvent être dus aux caractéristiques de systèmes particuliers, comme le fait d'être trop imprécis ou biaisés, ou à leur contexte de déploiement. L'argument principal de la CNIL à l'encontre d'ALICEM est de cet ordre : il ne remet pas en cause l'usage de la reconnaissance faciale mais la validité du consentement des utilisateurs. Cet argument pourrait être contré par l'offre de solutions alternatives permettant d'obtenir le même niveau de sécurité[36], comme la CNIL le suggère elle-même.

En procédant de manière descendante, de la finalité à la mise en œuvre, chaque étape d'analyse peut être vue comme un test à passer avant d'envisager le niveau suivant. Ainsi, si la finalité est jugée inacceptable, il est inutile de considérer les moyens de l'accomplir. De même, si les moyens ne sont pas jugés effectifs, il est inutile de considérer leur réalisation par la reconnaissance faciale, et ainsi de suite.

Démarche comparative : une autre dimension essentielle de notre méthode est d'insister sur la nature comparative des arguments avancés : les bénéfices comme les risques doivent être évalués en comparaison avec d'autres hypothèses. La situation initiale (avant l'éventuel déploiement du système) sert généralement de point de repère implicite mais il convient d'envisager également, à chaque étape, d'autres options possibles : d'autres moyens pour accomplir la finalité, d'autres solutions que la reconnaissance faciale, et d'autres mises en œuvre que celle qui est proposée. La figure 2 présente, à titre d'illustration, une analyse comparative simplifiée de l'exemple fictif de contrôle d'accès aux trains évoqué plus haut. À chaque étape (moyen, usage de la reconnaissance faciale, mise en œuvre) différentes alternatives sont considérées et évaluées.

L'analyse peut aussi conduire à proposer des contremesures ou améliorations susceptibles de réduire les impacts négatifs ou d'augmenter les impacts positifs. En d'autres termes, le débat ne doit pas être fermé, réduit à une alternative : accepter ou refuser le système proposé. Au contraire, l'application de la méthode a pour but de susciter un esprit critique et de faire émerger tous les arguments et les suggestions d'alternatives.

Démarche rigoureuse : un dernier point important, d'ordre méthodologique, concerne les éléments de preuve qui doivent être apportés pour soutenir les hypothèses avancées concernant les impacts

[34] Lycées : la CNIL précise sa position, 29 octobre 2019, https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.
[35] Facial recognition is the perfect tool for oppression, W. Hartzog, E. Selligner, Medium.com, http://cyberlaw.stanford.edu/publications/facial-recognition-perfect-tool-oppression.
[36] Pour la création de l'identité numérique de niveau de garantie élevé (au sens du règlement e-IDAS).

potentiels. Trop souvent, les discussions en matière de reconnaissance faciale reposent sur des aprioris positifs ou négatifs, notamment à propos de son efficacité supposée et des risques auxquels elle peut donner lieu. Il importe donc, pour chaque hypothèse, de déterminer précisément son statut. On pourra distinguer au moins trois types de situations : des hypothèses déjà corroborées par des mesures expérimentales ou des études scientifiques sérieuses (comme celles qui concernent les risques de biais dans les algorithmes[37]) ; des hypothèses qui ne sont pas validées par des études suffisantes mais qui pourraient l'être (comme celles qui concernent les bénéfices de la reconnaissance faciale dans le domaine policier[38]), ce qui pourrait exiger dans certains cas des déploiements expérimentaux ; et des hypothèses qui relèvent de positions subjectives ou politiques (comme la position selon laquelle le développement de la reconnaissance faciale ne doit pas être trop contraint de façon à ne pas nuire à la capacité d'innovation des industriels français du domaine, ou, inversement, l'idée qu'il faudrait s'opposer à tout déploiement, même expérimental, car il répondrait forcément à un plan dissimulé de surveillance policière) et ne sont pas susceptibles d'évaluation expérimentale. Par ailleurs, quand des expérimentations sont conduites pour valider des hypothèses, celles-ci doivent être réalisées de manière indépendante, en respectant un protocole précis. Nous revenons sur cette question cruciale dans la partie 4.

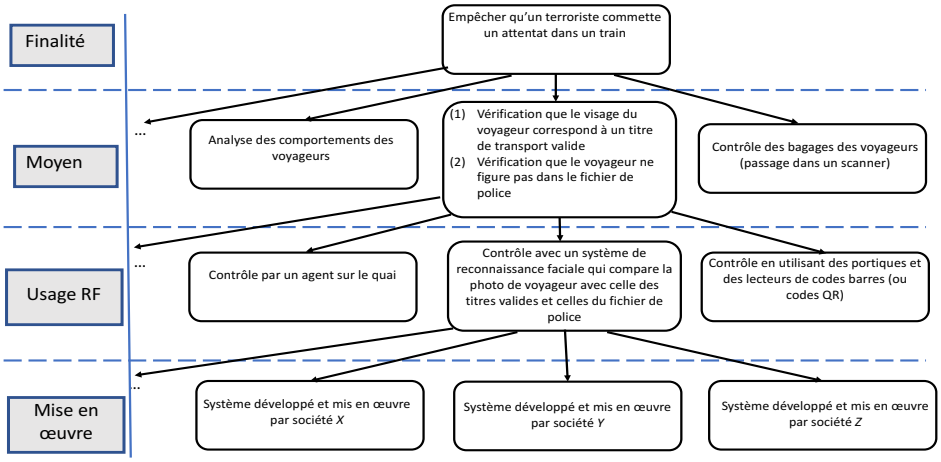

Figure 2. Analyse comparative d'une application

[37] J. Angwin, J. Larson, S. Mattu, L. Kirchner, «Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks», ProPublica, 23 May 2016 ; https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
A. W. Flores, K. Bechtel, C. T. Lowenkamp, «False positives, false negatives, and false analyses: A rejoinder to "Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks"», Fed. Prob. 80, 38 (2016).

[38] Face off. The lawless growth of facial recognition in UK policing, Big Brother Watch, https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. How facial recognition make you safer, James O'Neill, New York Times, 9 juin 2019, https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html.

3.2 Présentation détaillée

Pour chacun des quatre niveaux d'analyse de notre méthode, il est nécessaire de :

1. Caractériser précisément le système au niveau en question (finalité, moyen, usage de la reconnaissance faciale et mise en œuvre).
2. Réaliser l'inventaire de tous les enjeux (impacts positifs et négatifs, personnes affectées, etc.).
3. Analyser ces enjeux (appréciation de la gravité et de la vraisemblance des impacts, de leur caractère temporaire ou permanent, réversible ou irréversible, etc.).
4. Envisager des alternatives ou des améliorations du système pour répondre aux enjeux identifiés.

Pour faciliter le travail d'inventaire et d'analyse des enjeux, il peut être utile de recourir aux matrices d'éthique proposées initialement par Ben Mepham dans le domaine de la bioéthique[39] et qui ont été utilisées ensuite dans d'autres domaines comme l'alimentation ou l'énergie. Les matrices d'éthique permettent de représenter de manière concise les enjeux pour toutes les parties prenantes : leurs lignes représentent les catégories de parties prenantes et leurs colonnes les impacts potentiels. Nous en présentons un exemple dans la figure 5 en annexe 2 de ce document. Les impacts sont souvent regroupés en trois catégories, respectivement *bien-être* (santé, conditions de vie, etc.), *autonomie* (liberté, dignité, etc.) et *équité* ou *justice,* mais d'autres choix sont possibles. On pourrait notamment distinguer la protection des données personnelles et de la vie privée comme un enjeu séparé dans l'optique de la préparation d'une analyse d'impact sur la protection des données (AIPD) dans le cadre du RGPD[40] ou de la Directive Police-Justice[41]. Une telle étude d'impact est en effet exigée par ces textes (intégrés en France dans la loi Informatique et Libertés) pour le traitement de données sensibles, comme les données biométriques. Nous ne détaillons pas l'AIPD dans ce document car elle a déjà donné lieu à de nombreuses publications. La CNIL a notamment mis à disposition plusieurs guides et un outil pour aider les responsables de traitement dans cette tâche[42]. Comme évoqué dans la partie 3.1, l'étude d'impact générale décrite dans ce document pourra alors servir d'étape préparatoire à une AIPD.

D'un point de vue opérationnel, l'analyse d'impact devrait être menée de façon collaborative en impliquant toutes les parties prenantes, par exemple en suivant des procédures établies en matière de démocratie participative (convention citoyenne, conférence de consensus, concertation, etc.). Les rôles des parties prenantes, du maître d'œuvre et des experts techniques peuvent varier selon le périmètre retenu (par exemple, projet spécifique ou débat plus large sur la reconnaissance faciale), les niveaux d'analyse et les étapes. Par exemple, la participation des parties prenantes est essentielle dans les étapes 2 et 3 (inventaire et analyse des enjeux, à tous les niveaux) ainsi que, dans une certaine mesure, dans les étapes 4 (propositions d'alternatives ou d'améliorations). L'expertise technique est indispensable pour la caractérisation précise de l'usage de la reconnaissance faciale et la spécification détaillée du système ainsi que pour la suggestion ou l'évaluation d'alternatives. Le maître d'œuvre, quant à lui, doit justifier la solution proposée, notamment la finalité, le moyen et l'usage de la reconnaissance faciale pour réaliser ce moyen.

[39] Voir, par exemple : The ethical matrix – A tool for ethical assessments for biotechnology, E.-M. Forsberg, Golbal Bioethics, Vol. 17, 2004 ; ou Ethical matrix, Food Ethics Council, https://www.foodethicscouncil.org /uploads/publications/Ethical_Matrix_1.pdf.
[40] https://www.cnil.fr/fr/reglement-europeen-protection-donnees.
[41] https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t.
[42] https://www.cnil.fr/fr/nouveautes-sur-le-pia-guides-outil-piaf-etude-de-cas.

Dans les parties suivantes, nous présentons successivement les quatre niveaux d'analyse de notre méthode : finalité (partie 3.2.1), moyen (partie 3.2.2), usage de la reconnaissance faciale (partie 3.2.3) et mise en œuvre (partie 3.2.4).

3.2.1 Finalité

La finalité est l'objectif ultime, la justification du déploiement envisagé : sa définition conditionne donc toute la suite de l'analyse. Même si elle est de nature plus politique ou économique que technique, elle doit être définie de la manière la plus précise possible de façon à permettre l'inventaire et l'analyse des enjeux. Par exemple, si on considère une solution d'identité numérique sécurisée, il est important de savoir si son utilisation aura un caractère obligatoire ou pas pour l'accès à certains sites et, le cas échéant, quels sont ces sites. Pour prendre deux hypothèses extrêmes, les enjeux seront très différents si la solution est un moyen d'authentification facultatif pour l'accès à certains sites régaliens comme celui des impôts, ou si elle est destinée à devenir obligatoire pour un grand nombre de sites, publics ou privés. Dans le second cas, elle serait en effet susceptible de remettre en cause la notion d'anonymat sur internet. De la même façon, la légitimité d'un système d'analyse d'images de vidéosurveillance à des fins de recherche de personnes pourra dépendre de la qualification précise de la notion de « personne recherchée » (terroriste ou criminel en cavale, enfant fugueur, adulte disparu, etc.). Certains projets pourront également paraître d'emblée illicites ou contestables, politiquement ou juridiquement : on peut imaginer que ce serait le cas par exemple d'une initiative visant à empêcher certaines personnes de participer à des manifestations publiques ou à identifier les manifestants. Par ailleurs, même si une finalité est légitime, elle peut être plus ou moins critique et comporter des impacts variés, à court ou long terme, pour différentes catégories de population.

3.2.2 Moyen adopté pour accomplir la finalité

Le moyen décrit la stratégie adoptée pour accomplir la finalité, indépendamment d'une mise en œuvre particulière, par un système informatique et/ou par des opérateurs humains.

Dans l'exemple de l'introduction, le moyen était défini comme « contrôler, lors de l'accès au quai, que (1) le visage du voyageur correspond à la photographie liée à un titre de transport valide, et (2) cette photographie ou l'identité du voyageur ne correspond pas à un terroriste figurant dans un fichier de police ». La première question à se poser est celle de l'effectivité du moyen proposé pour accomplir la finalité et d'éventuels éléments de preuve (études, expérimentations, etc.) qui pourraient en attester. Pour bien séparer les problèmes, on suppose à ce stade que le moyen est parfaitement mis en œuvre. Dans l'exemple considéré ici, on peut contester le moyen proposé car il est inopérant vis à vis des attaques internes (émanant d'un employé ou sous-traitant malveillant) ou, de manière générale, des menaces provenant de personnes inconnues des services de police. Deux options sont possibles à ce stade de l'analyse : soit le moyen n'est pas susceptible d'être révisé, il est alors considéré comme ineffectif et le projet est rejeté ; soit le moyen peut être précisé ou renforcé.

Dans le cas du système ALICEM, la finalité consiste à prouver son identité et le moyen consiste à montrer quelque chose que l'on possède (en l'occurrence son passeport) et quelque chose que l'on est (en l'occurrence, son visage). Il s'agit là d'une authentification multi-facteurs bien connue dans le domaine de la sécurité. Selon le niveau de garantie désiré, on demande parfois un troisième facteur

(montrer que l'on connaît quelque chose, par exemple un mot de passe). La spécificité d'ALICEM ne réside donc pas tant dans le moyen que dans l'utilisation de la reconnaissance faciale pour le réaliser.

Après avoir analysé l'effectivité du moyen proposé, il faut répertorier les impacts possibles de ce moyen sur toutes les parties prenantes et sur la société dans son ensemble (notamment sur le fonctionnement démocratique). Dans l'exemple de contrôle d'accès aux quais de gare, on peut distinguer par exemple les impacts sur voyageurs, les employés de la société de chemins de fer, la compagnie elle-même, les citoyens en général (ou la société), l'État et également les fournisseurs de la technologie. Si on considère, à titre d'illustration, les voyageurs, on peut identifier, dans la catégorie des impacts positifs possibles : un sentiment accru de sécurité (justifié ou pas) et dans les impacts négatifs, une restriction de la liberté de circuler anonymement et un sentiment de surveillance. S'agissant des risques de dérives liées au moyen, il est important de préciser notamment le nombre de personnes figurant dans le fichier de police utilisé, les critères selon lesquels une personne y est intégrée, la manière dont son utilisation est contrôlée, et le type d'autorisation, judiciaire ou administrative, à laquelle cette utilisation est subordonnée. Le lecteur intéressé pourra trouver dans l'annexe 2 une liste plus complète d'impacts possibles pour différentes catégories de parties prenantes.

S'agissant des alternatives possibles au moyen proposé, on peut imaginer, pour l'exemple précédent, le passage des bagages des voyageurs au scanner et des portiques de sécurité pour les passagers (comme dans les aéroports) sans vérification de titre de transport nominatif. Il s'agit alors de comparer les deux solutions, aussi bien du point de vue de leurs impacts positifs (notamment en termes d'effectivité) que dans leurs impacts négatifs. Dans le cas présent, on pourrait argumenter que cette alternative permettrait de mieux accomplir les finalités tout en préservant la liberté de circuler anonymement. Cependant, elle pourrait provoquer des attentes plus longues à l'embarquement. Dans une analyse réelle, ces arguments devraient être étayés par des résultats ou des études expérimentales permettant de comparer les options de la manière la plus rigoureuse possible. Nous ne le ferons pas ici, notre propos n'étant pas d'investiguer ces différentes options en détail mais de fournir les lignes directrices de la démarche. Par ailleurs, la légitimité du moyen et la pertinence des alternatives dépendent évidemment de la finalité elle-même. L'objection évoquée ci-dessus à propos du moyen ne tiendrait pas pour un projet qui aurait pour but, par exemple, de restreindre l'accès à un local sensible à quelques collaborateurs habilités. Dans ce cas, le fichier des personnes concernées serait circonscrit à un nombre limité d'employés.

3.2.3 Reconnaissance faciale pour réaliser le moyen

Le troisième niveau est celui où on prend en compte le recours à la technologie de reconnaissance faciale. L'objectif à ce stade est de décrire comment la reconnaissance faciale est utilisée sans entrer dans le détail de sa mise en œuvre qui est analysée au quatrième niveau. Si on poursuit l'exemple utilisé plus haut, on peut préciser par exemple que le voyageur qui se présente au portique est automatiquement photographié, qu'une image de son visage est extraite par le système et que celle-ci est comparée d'une part avec la base de réservation de la société de chemins de fer et d'autre part avec le fichier de police. Le voyageur ne peut franchir le portique que s'il figure dans la première base et n'apparaît pas dans la seconde.

Puisque la manière dont la reconnaissance faciale est mise en œuvre n'est pas encore introduite, on fait pour l'instant l'hypothèse que cette mise en œuvre est « parfaite », notamment qu'elle est précise, exempte de biais et ne peut pas être compromise. Les questions abordées à ce stade sont donc de nature

théorique plus qu'expérimentale : elles concernent les avantages et les risques intrinsèques de la reconnaissance faciale.

Comme pour le niveau précédent, la première question à se poser est celle de l'effectivité : il s'agit maintenant de l'effectivité de la reconnaissance faciale pour réaliser le moyen proposé. Dans l'exemple proposé, cette effectivité semble pouvoir être admise. S'agissant des risques, il est important de considérer aussi à ce stade les possibles dérives ou extensions successives auquel le traitement pourrait donner lieu. Ce risque, qui relève plus du moyen ou du long terme, est souvent évoqué par les opposants à la reconnaissance faciale. Ces extensions, déjà évoquées dans la partie 2.3, peuvent concerner aussi bien les bases de données utilisées, les finalités autorisées que les contextes d'utilisation des systèmes. On peut même se demander parfois s'il ne s'agit pas d'une stratégie délibérée des promoteurs de la reconnaissance faciale, consistant à l'utiliser d'abord dans des contextes où les finalités paraissent légitimes pour les banaliser et étendre ensuite progressivement leur usage. L'argument de la « pente glissante » doit donc être considéré sérieusement, même s'il convient de l'analyser concrètement, dans chaque cas particulier, pour éviter de verser dans le sophisme[43]. Pour ce qui concerne l'exemple de contrôle d'accès aux quais de gare, on pourrait argumenter qu'il existe un risque important de généralisation à tous les modes de transport (métro, tram, bus, etc.) et donc de perte totale de la liberté de circuler anonymement. Au-delà des transports, on pourrait aussi imaginer une généralisation à tous les lieux fermés où se rassemblent des personnes (salles de cinéma, de spectacle, centres commerciaux, etc.) : si ces systèmes sont jugés efficaces, pourquoi protéger seulement les moyens de transport ? Sinon, où fixer la limite et quels garde-fous prévoir pour assurer que celle-ci ne sera pas franchie à la première occasion ? Dans d'autres cas, ce sont les fichiers eux-mêmes qui pourraient être ultérieurement étendus ou croisés avec d'autres fichiers. Les précédents en la matière sont suffisamment abondants[44] pour montrer que ce genre de dérive ne relève pas du fantasme sans qu'il soit nécessaire de recourir à l'argument d'un éventuel changement de régime. Ce risque « systémique » et les conséquences de la surveillance de masse sur la liberté d'expression et la vie démocratique ont été largement documentés et analysés[45].

Il convient aussi de se poser la question de la nécessité et de la proportionnalité de l'utilisation de la reconnaissance faciale. La réponse à ces questions peut dépendre de nombreux facteurs, notamment du périmètre d'application : comme l'indique l'ICO, l'autorité britannique en matière de protection des données personnelles, un système de reconnaissance faciale ciblé, limité dans le temps et dans l'espace, et destiné à surveiller des suspects connus sera probablement plus justifiable qu'un déploiement à grande échelle, indiscriminé et permanent[46].

[43] Comme le souligne le philosophe Ruwen Ogien, ce type d'argument n'est « pas valide si l'on ne donne pas les raisons pour lesquelles on serait pour ainsi dire obligé de passer de la première étape, que tout le monde pourrait accepter, à la dernière, que tout le monde devrait refuser. » http://www.constructif.fr/bibliotheque/2010-6/retour-a-l-ethique-ou-panique-morale.html?item_id=3040.

[44] Le fichier national des empreintes génétiques (FNAEG), déjà cité, en fournit un exemple éloquent : créé en 1998, pour centraliser les empreintes des personnes condamnées pour des délits d'une extrême gravité (meurtre ou assassinat d'un mineur précédé ou accompagné d'un viol, de tortures ou d'actes de barbarie, etc.), il a été étendu successivement, jusqu'à inclure près de trois millions de profils génétiques en 2018. Voir aussi la note 25 pour les fichiers TES et TAJ.

[45] Chilling Effects: Online Surveillance and Wikipedia Use, Jon Penney, Berkeley Technology Law Journal, vol. 31, No1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645##. Under surveillance: examining Facebook's spiral of silence effects in the wake of NSA Internet Monitoring, Journalism & Mass Communication Quartely, Vol. 93(2), 2016. https://journals.sagepub.com/doi/abs/10.1177/1077699016630255.

[46] https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

Pour ce qui concerne les alternatives possibles à la reconnaissance faciale pour réaliser le moyen proposé dans l'exemple des trains, on pourrait imaginer un contrôle visuel effectué par des employés de la société de chemins de fer. Selon le type de fichier utilisé, ce contrôle pourrait consister en une recherche de la photographie de la personne à partir de son identité (pour la base des réservations), ou une comparaison directe avec quelques photographies de personnes recherchées. On pourrait aussi imaginer la lecture d'un code barre ou code QR qui donnerait accès à la photographie associée à la réservation. Dans tous les cas, l'inconvénient principal serait un embarquement moins fluide, et un coût probablement plus élevé. L'existence d'alternatives moins attentatoires à la vie privée peut être un élément déterminant pour juger l'usage de la reconnaissance faciale disproportionné, comme en témoigne l'avis de la CNIL concernant des expérimentations dans des lycées de Nice et Marseille. Celle-ci a jugé en l'espèce que « les objectifs de sécurisation et la fluidification des entrées dans ces lycées peuvent être atteints par des moyens bien moins intrusifs en termes de vie privée et de libertés individuelles, comme par exemple un contrôle par badge »[47]. De manière générale, comme le suggère l'EDPS[48], les usages à des fins d'authentification (c'est à dire reconnaissance faciale (1,1) selon la classification présentée dans la partie 2.1) seront souvent plus proportionnés que l'identification ou la recherche (reconnaissance faciale (1,N) ou (M,N) selon la classification de la partie 2.1). De fait, dans le cas d'ALICEM, les principales réserves de la CNIL n'ont pas porté sur l'usage de la reconnaissance faciale en tant que telle, mais plus, comme on le verra ci-dessous, sur les conditions de sa mise en œuvre.

3.2.4 Mise en œuvre de la reconnaissance faciale dans un système particulier

Le quatrième niveau prend en compte la mise en œuvre de la technologie de reconnaissance faciale. En particulier, il intègre les caractéristiques (et les imperfections) des technologies utilisées, les divers paramètres de configuration, les données, les acteurs, l'environnement de déploiement, etc. Il faut à ce stade procéder à l'évaluation du système dans sa globalité, en tenant compte des contre-mesures mises en place, des mécanismes de contrôle et de transparence, ainsi que des conditions socio-économiques de son déploiement.

L'intérêt de distinguer les questions liées à l'usage de la reconnaissance faciale de celles qui concernent une mise en œuvre particulière est de mieux séparer les enjeux, en séparant les problèmes de fond posés par l'usage de cette technologie et ceux qui sont liés à l'état de l'art à un moment donné. Ainsi, l'analyse pourra, dans certains cas, conclure que l'usage de la reconnaissance faciale serait acceptable si celle-ci pouvait satisfaire un ensemble d'exigences essentielles (en matière de performances, de fiabilité, de sécurité, d'équité, etc.) mais que les solutions existantes ne sont pas encore mûres ou que celle qui est proposée n'est pas satisfaisante.

Cette phase nécessite tout d'abord de définir précisément le système, c'est à dire son contexte de déploiement, les spécifications techniques de la solution adoptée, les divers paramètres de configuration, les données utilisées, les acteurs impliqués et leurs rôles, etc. Il faut ensuite procéder à l'évaluation des propriétés « intrinsèques » du système, notamment[49]:

[47] Lycées : la CNIL précise sa position, 29 octobre 2019, https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position.
[48] https://edps.europa.eu/node/5551.
[49] Pour plus d'information, voir https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)624261.

- Ses *performances et sa fiabilité*, en mesurant, par exemple, les taux de faux positifs (le système de reconnaissance faciale « reconnaît » des personnes à tort) et faux négatifs (le système ne « reconnaît » pas certaines personnes à tort).
- Sa *sécurité* en analysant les propriétés de confidentialité, d'intégrité et de disponibilité du système. On tentera notamment d'apporter des réponses à des questions comme : les performances du système peuvent-elles être altérées par un acteur malicieux ? Est-il possible de tromper le système de reconnaissance faciale ? Est-il possible d'accéder au système de paramétrage, aux modèles ou données utilisées ? Cette phase nécessite de faire des hypothèses sur les différents adversaires potentiels (sources de risques), notamment en termes d'objectifs, de capacités et de stratégies[50].
- Les *garanties sur les données* utilisées (par exemple, les données d'entraînement) et sur la protection de la vie privée des utilisateurs.
- L'*équité* et l'absence de biais du système, en évaluant, par exemple, les taux d'erreurs pour différents groupes (ethniques, démographiques, etc.) de population.
- Le respect des *droits des utilisateurs,* définis par le RGPD et la Directive Police-Justice, par exemple en termes d'information, d'accès aux données, de rectification, etc.

Il conviendra ensuite d'évaluer les propriétés « extrinsèques » telles que :

- La *transparence* du système : est-ce que les algorithmes, modèles et données utilisées sont disponibles (publiquement ou accessibles de façon restreinte, par des experts indépendants) ?
- L'« *explicabilité* » du système : est-ce que le comportement et les résultats du système sont compréhensibles et explicables aux usagers, en particulier en cas de faux positifs ou de faux négatifs ?

Finalement, il est nécessaire d'analyser les mécanismes de « *contrôle* » (*accountability*) mis en place. Par exemple, on pourra se poser les questions suivantes : qui sont les acteurs impliqués et responsables du système ? Comment ces acteurs peuvent-ils « rendre compte » de leurs actions et à qui ? Quelles sont les mesures prévues pour assurer la supervision des traitements ? Impliquent-elles des tiers indépendants, des représentants des parties prenantes, notamment des citoyens ?

L'étude des propriétés d'un système est un exercice très complexe et chronophage. Il est important de noter que ces analyses dépendent souvent de multiples paramètres tels que l'algorithme utilisé, la taille et la qualité des données d'entraînement (dans le cas de systèmes qui utilisent des algorithmes d'apprentissage) ou encore le choix du seuil de confiance. Le seuil de confiance caractérise le niveau de confiance que le système associe à un évènement donné. Ainsi, un système pourra, par exemple, identifier une personne recherchée avec une probabilité de 70% et une autre avec une probabilité de 99,9%. Si cette probabilité est supérieure au seuil de confiance, une alerte sera émise, sinon l'évènement sera ignoré par le système. Par exemple, Amazon recommande d'utiliser un seuil de confiance de 99% pour les utilisations de son système *Rekognition* à des fins policières mais un seuil de confiance de 80% pour des applications moins critiques[51]. Intuitivement, un seuil de confiance élevé permet de signaler uniquement des évènements très probables (le taux de faux positifs sera faible), au risque de ne pas détecter un nombre important de suspects (le taux de vrais positifs sera faible aussi). On limite alors le

[50] Les divergences de points de vue découlent souvent d'une divergence sur les hypothèses, implicites ou explicites, concernant les sources de risque. Par exemple, les opposants aux déploiements de systèmes de vidéo-surveillance ou de reconnaissance faciale font souvent l'hypothèse que l'opérateur, par exemple la ville, n'est pas digne de confiance et pourra être tenté d'utiliser le système pour d'autres finalités, voire de le modifier pour permettre des dévoiements. La question du modèle d'adversaire à considérer dans une analyse de risques est donc essentielle et doit être débattue.

[51] https://aws.amazon.com/blogs/aws/thoughts-on-machine-learning-accuracy/.

risque de fausse identification, au prix de l'efficacité de détection du système. Inversement, un seuil de confiance bas permet d'identifier la plupart des personnes recherchées, au prix d'un taux élevé de faux positifs (personnes identifiées à tort). Il faut aussi noter que les performances d'un système dépendent souvent de l'environnement dans lequel celui-ci est déployé (caractéristiques des caméras, luminosité, angles des prises de vues, etc.). Une analyse rigoureuse devrait donc comprendre une phase de mesures sur le terrain.

Un exemple de système dont la mise en œuvre pourrait être contestée est l'application ALICEM déjà évoquée plus haut. ALICEM est une application pour téléphone mobile développée par le ministère de l'Intérieur et l'Agence nationale des titres sécurisés (ANTS) qui permet à tout particulier de prouver son identité sur internet de manière sécurisée. ALICEM utilise la reconnaissance faciale en « temps réel » pour prouver que la personne qui souhaite générer une identité sécurisée est bien la propriétaire du passeport utilisé (en comparant la photographie qui est stockée dans le passeport avec celles issues d'une vidéo que l'utilisateur doit prendre et envoyer à l'ANTS). L'hypothèse de sécurité est alors que seul le propriétaire du passeport peut réaliser la vidéo en temps réel. Or, des résultats récents sur la fabrication d'images truquées (« *deepfakes* ») ont démontré qu'il était possible, à l'aide d'un logiciel en libre accès, de générer automatiquement une telle vidéo en utilisant la méthode d'échange de visages (« *face swapping* »)[52]. Des expérimentations ont montré que les systèmes de reconnaissance acceptaient ces vidéos avec une probabilité supérieure à 84%. Un attaquant qui possèderait donc le passeport d'une victime pourrait générer une identité numérique sécurisée au nom de la victime, ce qui remet en cause la sécurité et l'intérêt de cette application. Une autre faiblesse d'ALICEM concerne l'envoi de la vidéo au serveur de l'ANTS alors que la comparaison pourrait probablement être réalisée par l'application elle-même sur le téléphone. Par ailleurs, il est à noter que la reconnaissance faciale est uniquement mobilisée lors de la phase d'activation du compte de l'utilisateur. Par la suite, l'utilisateur peut simplement utiliser l'identité numérique créée lors de cette phase d'activation, via l'application ALICEM, pour s'authentifier auprès des sites auxquels il souhaite accéder. La sécurité du système dépend donc de la sécurité du code de l'application et de celle du téléphone, notamment du système d'exploitation Android, hypothèses qui permettent d'émettre des doutes sur la sécurité globale d'ALICEM.

De manière plus générale, un système de reconnaissance faciale n'est pas un objet technique qui peut être analysé *in abstracto*, indépendamment du contexte socio-économique de son déploiement. Il s'agit plutôt de ce qu'on appelle en sociologie un système socio-technique. L'analyse de la mise en œuvre devra donc intégrer ces dimensions sociologiques (acteurs concernés, rôles et intérêts dans le système, relations de pouvoir, perception du remplacement d'activités humaines par des machines, incidences sur les relations humaines, etc.), économiques (coûts de développement, de déploiement, de maintenance, etc.) et stratégiques (dépendance envers certains acteurs industriels ou puissances étrangères, risques de cyber-attaques, etc.). Il faut ensuite évaluer ces éléments en fonction des finalités affichées et des solutions alternatives.

[52] https://arxiv.org/abs/1910.01933.

4. Conclusion

Récapitulatif des points essentiels :

- Importance d'une méthodologie rigoureuse et systématique d'analyse des impacts (positifs et négatifs) sur tous les groupes affectés, à court terme et à long terme, aussi bien spécifiques à l'application que systémiques (risques de généralisation)
- Démarche incrémentale : quatre niveaux d'analyse pour une séparation claire des enjeux
- Démarche comparative : imaginer et évaluer les alternatives
- Démarche rigoureuse : distinguer les opinions des faits corroborés par des études ou des résultats
- Nécessité d'une procédure délibérative avec toutes les parties prenantes
- Importance du contrôle par des tiers indépendants (selon le cas, experts, autorités de protection, représentants des parties prenantes) : certification des algorithmes, expérimentations supervisées par des scientifiques, procédures d'audits, etc.

Figure 3 Éléments de méthode

Dans cette note, nous avons montré la diversité des applications de la reconnaissance faciale et la variété des paramètres à prendre en compte pour les analyser : type de finalité (sécurité des personnes, gain de temps, confort, etc.), type d'usage de la technique (identification, vérification d'identité ou surveillance ; fonctionnement en temps réel ou a posteriori, temporaire ou permanent, dans un espace géographiquement limité ou plus large, reposant sur une base de données centralisée ou pas, etc.), contexte de déploiement (consentement des intéressés, rôle des intervenants humains, autorisation judiciaire, etc.). Nous avons proposé, pour aborder ces enjeux de la manière la plus rationnelle possible quelques éléments de méthode dont les points essentiels sont résumés dans la figure 3. Il ne s'agit pas ici de trancher ni de fournir des solutions clefs en mains pour résoudre ces questions difficiles qui doivent être soumises au débat public. La manière de mettre en place un tel débat (convention citoyenne, conférence de consensus, etc.) et les procédures à suivre en la matière sortent du cadre de cette étude[53].

Il faut souligner que, même si nous avons illustré ce document principalement à l'aide d'exemples d'application dans les services publics, une attention similaire devrait être portée aux utilisations de la reconnaissance faciale par des acteurs privés. Les risques peuvent être aussi très importants en la matière et les bénéfices moindres pour les citoyens ou les consommateurs[54]. À défaut, on pourrait se trouver dans des situations paradoxales comme celle évoqué par Sidney Fussel à propos de la ville de San Francisco où les forces de polices se verraient interdire l'analyse de vidéos pour rechercher un suspect

[53] De nombreux travaux ont été effectués en la matière et les retours d'expérience sont riches et variés. Un exemple récent, et toujours en cours, en France est la convention citoyenne pour le climat qui réunit 150 français tirés au sort : https://www.conventioncitoyennepourleclimat.fr/2019/10/01/les-150-citoyens-nes-a-la-loupe/. Pour un tour d'horizon plus général, mais aussi plus ancien, on pourra consulter notamment l'ouvrage de M. Callon, P. Lascoumes et Y. Barthe, Agir dans un monde incertain, Essai sur la démocratie technique, Le Seuil, Points, 2001.

[54] Voir par exemple : https://www.nytimes.com/2019/11/08/realestate/are-my-neighbors-spying-on-me.html.

après une fusillade alors qu'un commerçant de la ville serait libre de faire la même chose pour analyser le comportement de ses clients.

Il convient de noter également que nous ne nous sommes pas placés ici sur le terrain juridique : les systèmes de reconnaissance faciale, parce qu'ils traitent des données personnelles, et même sensibles, relèvent évidemment du RGPD ou de la Directive Police-Justice, mais les questions qu'ils soulèvent dépassent le cadre du droit positif et de la protection de la vie privée : comme le souligne Wojciech Wiewiórowski, le contrôleur européen de la protection des données, « se focaliser sur les enjeux de vie privée serait une erreur. Il s'agit fondamentalement d'une question éthique pour une société démocratique. »[55].

Une dimension sur laquelle il nous paraît important de revenir est celle de *l'accountability*[56], redevabilité, ou obligation de rendre compte, qui est essentielle pour toute technologie pouvant être utilisée à des fins de surveillance. En effet, il n'est pas rare, même dans des pays démocratiques, qu'une technologie déployée initialement à des fins de lutte contre le terrorisme ou la criminalité, soit finalement étendue à la surveillance d'autres catégories de personnes, comme des journalistes ou des militants[57]. La reconnaissance faciale n'échappe pas à ce risque. En effet, dès lors que des images sont captées, enregistrées et potentiellement analysées, aucune méthode ne sera en mesure de garantir de façon absolue que le système ne pourra pas être utilisé à mauvais escient[58], se révéler moins performant que prévu, voire erroné ou, de manière générale, produire des effets inattendus. Il est donc primordial de mettre en place des mesures obligeant les opérateurs du système à rendre compte de leur utilisation, notamment en définissant précisément les règles de gestion des bases de données d'images (procédure d'introduction d'une personne dans la base, recoupements avec d'autres bases de données, possibilité de contestation, sécurisation de la base, etc.), en apportant des garanties sur la qualité des algorithmes utilisés (performances, absence de biais, etc.), et en enregistrant de manière sécurisée toutes les utilisations des données, les finalités de ces usages, les autorisations obtenues pour y procéder, etc. Pour être effectives de telles mesures doivent pouvoir être contrôlées par un organe indépendant compétent et capable de fournir à toutes les parties prenantes (y compris des organisations de citoyens) une visibilité et des garanties sur l'utilisation des systèmes. Le non-respect de leurs obligations par les opérateurs de systèmes de reconnaissance faciale (ou leurs agents) devrait être sanctionné de manière dissuasive.

Cette note concerne essentiellement les phases de développement et de déploiement d'applications utilisant la reconnaissance faciale. Dans certains cas, des expérimentations préalables en situation réelle peuvent s'avérer nécessaires, notamment pour évaluer les performances du système en regard des objectifs visés et des alternatives envisageables. Il est important de rappeler que de telles expérimentations doivent également être soumises à une étude d'impact[59]. De plus, pour être d'une

[55] https://edps.europa.eu/node/5551.

[56] Notons que nous utilisons ici le terme « *accountability* » dans le sens général de « obligation de rendre compte », moins restrictif que celui adopté dans le RGPD. Le RGPD définit le terme par le fait que le responsable du traitement est responsable du respect des principes relatifs au traitement des données à caractère personne tels que définis dans son article 5. Voir en particulier : Strong Accountability: Beyond Vague Promises. Denis Butin, Marcos Chicote, Daniel Le Métayer, in Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges, Springer, 2014. https://hal.inria.fr/hal-00917350/file/cpdp2013-bcm-strong_accountability_v4.pdf.

[57] https://www.nytimes.com/2019/11/09/technology/nso-group-spyware-india.html.

[58] De nombreux exemples d'abus ont été constatés, comme celui du FBI révélé par l'ACLU : https://www.aclu.org/news/privacy-technology/the-fbi-is-tracking-our-faces-in-secret-were-suing/.

[59] Cette étude d'impact tiendra compte des conditions spécifiques de l'expérimentation, notamment des possibilités d'un consentement effectif des personnes concernées, du nombre de personnes impliquées, de sa durée et de l'importance des résultats attendus.

véritable utilité, elles doivent respecter un protocole rigoureux et être limitées dans le temps. Il convient notamment de définir précisément les objectifs de l'expérimentation, les conditions dans lesquelles elle sera conduite, les hypothèses de l'étude, les critères d'évaluation des résultats et aussi leur nécessité pour statuer ensuite sur le déploiement opérationnel du système. Idéalement, ces expérimentations devraient aussi impliquer des scientifiques de disciplines différentes, notamment des informaticiens et des sociologues, et être validées par un tiers indépendant. Comme le rappelle la CNIL, « le cadre juridique doit aussi garantir la sincérité des expérimentations conduites, dont l'issue ne saurait être préjugée »[60]. À cet égard, on peut citer en parfait contre-exemple l'expérimentation menée lors du carnaval de Nice de février 2019[61]. De manière générale, il est important que de telles expérimentations ne soient pas biaisées, et entreprises dans le seul but d'« entraîner l'adhésion de la population française », selon les termes utilisés dans un rapport du CREOGN[62] ou pour répondre aux défis d'« innovation technologique » et d' « appropriation citoyenne » selon les termes utilisés récemment par des parlementaires[63].

Pour conclure, nous souhaitons insister sur le fait qu'il est nécessaire de faire progresser l'état de l'art pour améliorer la confiance que l'on peut placer dans les dispositifs de reconnaissance faciale. Plusieurs actions concrètes nous paraissent urgentes à ce stade :

- La définition d'un référentiel pour conduire des analyses d'impact des systèmes de reconnaissance faciale. Nous espérons, par cette note, avoir contribué à l'élaboration d'un tel référentiel mais celui-ci devrait être défini par une autorité compétente, à la manière de ce qu'a proposé la CNIL pour réaliser des études d'impact en matière de protection des données personnelles[64] ou le gouvernement canadien pour réaliser des « évaluations de l'incidence algorithmique »[65].
- La définition de normes ou de méthodologies de test, de validation et de certification des systèmes de reconnaissance faciale. Ces normes devraient apporter des garanties vérifiables par des tiers indépendants, sur les qualités attendues de ces systèmes, notamment en termes de précision et d'absence de biais. Il est nécessaire à cet effet de définir des schémas d'évaluation standard à l'instar de ce qui a été fait dans certains schémas d'évaluation de sûreté ou de sécurité informatique.
- La définition d'un protocole d'expérimentation de systèmes de reconnaissance faciale en environnement réel. Comme on l'a évoqué plus haut, des études en laboratoire sont parfois insuffisantes et des expérimentations en situation réelle peuvent être nécessaires pour valider certaines hypothèses. Cependant, il n'existe pas actuellement de protocole de référence en la matière.

Les experts ont un rôle important à jouer pour dans ces actions mais leur rôle ne doit pas se cantonner à la définition de normes techniques. En se gardant de préempter les débats démocratiques qui devraient précéder le déploiement de tels systèmes, ils doivent y prendre leur place. Comme l'a souligné le Président de la République lors de son intervention au *Global Forum on Artificial Intelligence for Humanity* le 30 octobre 2019, évoquant les choix éthiques cruciaux auxquels nos sociétés sont

[60] https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux
[61] https://www.documentcloud.org/documents/6350838-Bilan-Reconnaissance-Faciale.html
[62] https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Reconnaissance-faciale-et-controles-preventifs-sur-la-voie-publique-l-enjeu-de-l-acceptabilite
[63] https://www.lemonde.fr/idees/article/2019/10/24/pour-une-reconnaissance-faciale-ethique_6016693_3232.html
[64] https://www.cnil.fr/fr/nouveautes-sur-le-pia-guides-outil-piaf-etude-de-cas, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-fr.pdf
[65] https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592

aujourd'hui confrontées, notamment en matière d'intelligence artificielle, « c'est là que le dialogue entre les décideurs politiques, les juristes et les scientifiques est absolument critique ».

Remerciements
Les auteurs tiennent à remercier leurs relecteurs, notamment Clément Hénin et Vincent Roca, pour leurs remarques constructives sur une version antérieure de ce document.

Annexe 1 : exemples d'application de la reconnaissance faciale

La reconnaissance faciale est un terme générique qui inclut l'identification faciale et l'authentification faciale[66].

- L'identification faciale consiste à établir l'identité d'un utilisateur, c'est à dire retrouver cette identité à partir d'une ou plusieurs photographies de son visage. Lors de l'identification, une photographie de l'utilisateur est prise[67]. Un gabarit de son visage en est extrait et il est utilisé pour chercher, dans une liste contenant N entrées, l'identité qui correspond à ce visage. Il s'agit donc d'une opération de type (1:N) dans le sens où la photographie d'une personne est comparée avec N autres photographies. On fait l'hypothèse ici que le lien entre le visage et l'identité a été réalisé préalablement pour constituer la liste.
- L'authentification faciale (1:1) est la phase qui permet à l'utilisateur d'apporter la preuve de son identité. Lors de l'authentification faciale, une photographie de l'utilisateur est prise, un gabarit de son visage en est extrait et il est utilisé pour vérifier, par comparaison, qu'il correspond bien à celui qui est associé à son identité. Il s'agit donc d'une opération de type (1:1) dans le sens où la photographie d'une personne est comparée avec une autre photographie (supposée être de la même personne).

La sécurité d'une identification ou authentification faciale est plus ou moins forte selon les performances de l'algorithme de comparaison des images et la qualité des photographies. Elle dépend aussi fortement de la garantie que le visage de la photographie prise appartient bien à la personne que l'on cherche à identifier ou authentifier. Dans le cas d'un portique devant une école ou d'une photographie prise par un policier, cette garantie est relativement élevée. Dans le cas d'un selfie pris par l'utilisateur avec son téléphone, cette garantie est faible car l'utilisateur peut utiliser la photographie de quelqu'un d'autre. Il faudra alors utiliser des mécanismes supplémentaires, comme par exemple des tests de vivacité.

Les applications qui utilisent la reconnaissance faciale peuvent être catégorisées en considérant (1) les entrées qui sont fournies par l'utilisateur au moment du traitement (par exemple via un badge ou un passeport), (2) les entrées captées par le système (typiquement une vidéo ou des photographies), (3) les données stockées dans une base centralisée, (4) le mode opératoire (en temps réel ou a posteriori) et (5) les sorties du système. La figure 4 présente quelques exemples d'applications classées selon ces critères :

- Un système d'authentification sécurisé en ligne, du type d'ALICEM, permet à un utilisateur de générer une identité numérique sécurisée à distance. L'identification est effectuée par la présentation du passeport[68]. Le système extrait l'information présente sur le passeport (identité et une photographie du détenteur) et demande à l'utilisateur de prendre une vidéo de son visage. Les informations sont envoyées à un serveur qui compare le visage de la personne sur la vidéo et la photographie du passeport. En cas de succès, l'utilisateur est authentifié. Ce système ne requiert pas de base d'images centralisée.
- Le système de contrôle d'accès à un train, décrit dans la partie 3.1, est un système qui permet d'identifier et authentifier un voyageur à des fins d'autorisation. La reconnaissance faciale est

[66] Par ailleurs, comme nous le verrons plus tard, la reconnaissance faciale peut être aussi utilisée pour suivre une personne, sans nécessairement l'identifier. Le visage est alors utilisé comme un « index ».
[67] En pratique, on peut en réalité saisir plusieurs photographies, via une caméra vidéo par exemple.
[68] Il ne s'agit donc pas ici d'identification faciale.

utilisée pour identifier la personne. Le système capte une ou plusieurs photographies du visage de la personne qui se présente au portique d'accès et recherche si ce visage apparaît dans la base de données des voyageurs enregistrés. Une fois la personne identifiée, le système vérifie qu'elle est autorisée à prendre ce train (c'est à dire qu'elle possède un titre de transport et n'apparaît pas dans la liste des personnes recherchées). Le système fonctionne en temps réel.

- Un système de contrôle d'accès peut aussi combiner l'utilisation d'un badge, ou plus généralement d'un « *token* »[69], et de la reconnaissance faciale. Dans ce scenario, le badge est utilisé pour identifier l'utilisateur et la reconnaissance faciale pour l'authentifier. Il s'agit donc d'un système d'authentification faciale. Plus précisément, les photographies captées par le système sont comparées à celles qui sont associées à la référence du badge de l'utilisateur dans une base centralisée.
- Un système d'identification, comme celui qui pourrait être utilisé par la police, lorsqu'elle arrête une personne qui ne veut pas décliner son identité, utilise la reconnaissance faciale à des fins d'identification. Le système capte des photographies de la personne à identifier et les compare avec celles présentes dans sa base de données interne (par exemple base de données des personnes recherchées). Cette identification peut avoir lieu en temps réel ou a posteriori. Si une entrée est trouvée, l'identité associée à ce visage dans la base de données est retournée.
- Un système de recherche de personnes (enfants perdus, criminels,) dans un espace public capte des images en temps-réel et vérifie si les visages qui apparaissent sur ces images correspondent à des personnes recherchées. Techniquement, cela consiste à comparer les visages captés avec ceux qui figurent dans une base de données centralisée (la base des personnes recherchées). La reconnaissance faciale est utilisée à des fins d'identification.
- Un système de suivi ou de traçage utilise plusieurs visages cibles (par exemple les visages de suspects à suivre) et recherche ces visages dans d'autres images enregistrées, par exemple issues d'un système de vidéo-surveillance, ou captées en temps réel. La reconnaissance faciale est utilisée ici à des fins de comparaison, l'objectif n'étant pas d'identifier une personne, mais de la retrouver sur plusieurs photographies.

Application	***Entrées Captées***	***Entrées Fournies***	***Données stockées dans une base centralisée***	***Sorties***	***Mode opératoire : T : Temps Réel P : A posteriori***
Authentification Sécurisée en ligne – Alicem (Authentification faciale)	Une vidéo ou une photo	Identité et une photo	0	Echec (identité non vérifiée) ou identifiant numérique (identité vérifiée)	T
Accès au quai de gare (Identification faciale)	Une vidéo ou une photo	0	N paires (identité ; visage)	0 (non autorisé) 1 (autorisé)	T

[69] Objet possédé par la personne, qui peut prendre des formes variées : badge, carte, téléphone mobile, etc.

Contrôle d'accès avec badge (Authentification faciale)	Une vidéo ou M photos	Identifiant extrait du badge	N paires (identité ; visage)	0 (identité non vérifiée) 1 (identité vérifiée)	T
Identification par la police (Identification faciale)	Une vidéo ou M photos	0	N paires (identité ; visage)	0 ou identité	T ou P
Recherche de personnes (perdues ou criminelles) dans espace public (Identification faciale)	Une vidéo ou M photos	0	N paires (identité ; visage)	0 ou liste d'identités	T ou P
Suivi d'une personne (Reconnaissance faciale pour traçage)	Une vidéo ou M photos	Une vidéo ou M photos	0	N Images	T ou P

Figure 4. Exemples d'utilisation de la reconnaissance faciale

Annexe 2 : les matrice d'éthique

Les quatre étapes d'analyse décrites dans ce document permettent d'identifier des impacts, positifs et négatifs, qui doivent ensuite être synthétisés et évalués. Les matrices d'éthique peuvent constituer un instrument utile pour guider l'analyse et réaliser cette synthèse. Leurs lignes représentent les parties prenantes et leurs colonnes les enjeux ou types d'impacts à considérer. Les impacts sont souvent regroupés en trois catégories, respectivement *bien-être* (santé, conditions de vie, etc.), *autonomie* (liberté, dignité, etc.) et *équité* ou *justice*. D'autres choix sont cependant possibles en fonction du contexte et des valeurs ou des familles d'éthique auxquelles les parties prenantes souhaitent se référer.

À titre d'exemple, la figure 5 représente une possible matrice d'éthique résultant de l'analyse du cas d'étude évoqué dans ce document en considérant la finalité « empêcher qu'un terroriste puisse commettre un attentat dans un train » et le moyen : « contrôler, lors de l'accès au quai, que (1) le visage du voyageur correspond à la photographie liée à un titre de transport valide, et (2) cette photographie ou l'identité du voyageur ne correspond pas à un terroriste figurant dans un fichier de police ». La figure 5 n'a bien entendu aucune vocation à l'exhaustivité, l'objectif ici étant essentiellement d'illustrer l'usage des matrices d'éthique. Dans chaque colonne les éléments notés « + » représentent des impacts positifs et les éléments notés « - » des impacts négatifs.

Soulignons que les matrices d'éthique n'associent pas de niveaux de vraisemblance ou de gravité aux impacts identifiés. C'est ainsi par exemple qu'on peut trouver dans la colonne bien-être un impact positif sur les voyageurs si la procédure d'embarquement est fluidifiée et un impact négatif en cas de dysfonctionnement ; de la même façon, des contrôles renforcés peuvent produire chez certains un sentiment de sécurité et chez d'autres un sentiment d'insécurité. C'est dans la dernière phase, la délibération, que les degrés de vraisemblance et les priorités entre les impacts doivent être débattus, dans un processus qui devrait impliquer toutes les parties prenantes.

Impacts / **Groupes Affectés**	**Bien-être**	**Autonomie**	**Équité**
Voyageurs	+ Procédure d'embarquement fluide + Sentiment de sécurité + Amélioration effective de la sécurité - Sentiment d'insécurité - Absence de réelle amélioration de la sécurité (moyen inadapté à la finalité) - Passagers arrêtés à tort (faux positifs ou fichiers inexacts) - Conséquences possibles de violations de données à	- Restriction de la liberté de circuler anonymement - Sentiment de surveillance - Conséquences possibles de violations de données à caractère personnel	- Traitement inéquitable des personnes mal reconnues par le système

	caractère personnel, usurpation d'identité, etc.		
Employés de la Société de Chemins de Fer	+ Affectation à des tâches plus gratifiantes - Risque de réduction d'effectifs	- Dépendance vis à vis d'un système opaque (interactions difficiles avec les voyageurs en cas de dysfonctionnement)	
Société de Chemins de Fer	+ Affectation des agents à des tâches plus gratifiantes + Meilleure satisfaction des clients - Coût du système (achat et phase opérationnelle) possiblement prohibitif en regard des services rendus - Insatisfaction des clients en cas de dysfonctionnement (faux positifs ou fichiers inexacts) - Risque de piratage	- Dépendance vis à vis du fournisseur de technologie	+ Meilleure capacité à faire face à la concurrence
Citoyens, société	+ Sentiment de sécurité + Amélioration effective de la sécurité - Sentiment d'insécurité - Absence de réelle amélioration de la sécurité (moyen inadapté à la finalité)	- Restriction de la liberté de circuler anonymement - Sentiment de surveillance - Crainte de voir cette surveillance se généraliser à tous les lieux accessibles au public avec des conséquences sur la liberté d'expression, les comportements (conformisme) et, finalement, la démocratie.	- Crainte de traitement inéquitable des personnes mal reconnues par le système, notamment de minorités ethniques
État	+ Satisfaction des citoyens (sentiment de plus grande sécurité) + Amélioration effective de la sécurité - Insatisfaction des citoyens (sentiment d'insécurité) - Absence de réelle amélioration de la sécurité	- Risque de surveillance par un état tiers (si le système est piraté)	

	(moyen inadapté à la finalité)		
Fournisseurs de technologie de reconnaissance faciale	+Intérêt économique lié au déploiement de systèmes de reconnaissance faciale		+ Meilleure capacité à faire face à la concurrence (a contrario, handicap en cas d'interdiction de déploiement)

Figure 5 Matrice d'éthique