AVIS N°8

ENJEUX ÉTHIQUES DES TECHNOLOGIES DE RECONNAISSANCE FACIALE, POSTURALE ET COMPORTEMENTALE

COMITÉ NATIONAL PILOTE
D'ÉTHIQUE DU NUMÉRIQUE

sous l'égide du
COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE
POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ

AVIS N°8

ENJEUX ÉTHIQUES DES TECHNOLOGIES DE RECONNAISSANCE FACIALE, POSTURALE ET COMPORTEMENTALE

AVIS ADOPTÉ LE 20 NOVEMBRE 2023
À L'UNANIMITÉ DES MEMBRES PRÉSENTS
LORS DE L'ASSEMBLÉE PLÉNIÈRE DU
COMITÉ NATIONAL PILOTE D'ÉTHIQUE DU NUMÉRIQUE

Comment citer cet avis :
Enjeux éthiques des technologies de reconnaissance faciale, posturale et comportementale.
Avis 8 du Comité national pilote d'éthique du numérique.
20 novembre 2023.

SOMMAIRE

LISTE DES ENCADRÉS

AVANT-PROPOS

Cet avis porte sur les enjeux éthiques des dispositifs intégrant des technologies de reconnaissance faciale, posturale et comportementale. Comme l'explique le rapport de la CNIL paru en 2019 sur le sujet[1], le recours à la biométrie en général, et aux technologies de reconnaissance faciale, posturale et comportementale, en particulier, ouvre nombre d'opportunités d'applications. Certaines d'entre elles sont potentiellement bénéfiques pour l'ensemble de la société tandis que d'autres suscitent des inquiétudes fort légitimes pour les libertés publiques. Du fait du caractère ambivalent de ces technologies, il n'est ni possible, ni souhaitable d'émettre un avis tranché sur leur emploi. En revanche, il convient d'évaluer avec précision et rigueur pour chaque cas d'usage l'adéquation des technologies déployées avec le gain escompté, et d'anticiper les conséquences de leur déploiement à court, moyen et long terme sur la société. Cet avis porte sur la réflexion éthique à mobiliser dans chaque cas spécifique. Il vise à éclairer et non à juger. Il ne condamne pas et ne cherche pas à faire l'apologie de l'emploi de telle ou telle approche. Il procède sans a priori et s'adresse à tous les acteurs concernés à divers titres par leur mise en œuvre. Cela inclut les concepteurs et les chercheurs à l'origine des évolutions de ces technologies, les ingénieurs impliqués dans leur mise en œuvre, les entreprises qui fabriquent les dispositifs, les commercialisent et conçoivent des usages, des produits ou des services associés, les décideurs qui mettent ces dispositifs au service d'une politique, le législateur et les représentants institutionnels qui ont la responsabilité de veiller au cadre de leur déploiement, enfin les exploitants et les personnes exposées, qui en tirent les éventuels bénéfices, et qui en subissent aussi les effets. Son but est d'aider les différentes parties prenantes à se forger une opinion précise et adaptée à chaque situation, en se fondant sur des arguments tangibles et sur une démarche rigoureuse.

[1] CNIL - Reconnaissance faciale, pour un débat à la hauteur des enjeux, 2019. https://www.cnil.fr/sites/cnil/files/atoms/files/reconnaissance_faciale.pdf

1. INTRODUCTION

Les technologies de reconnaissance faciale, posturale et comportementale connaissent une accélération notable depuis une décennie autant dans leur conception que dans leur utilisation, en particulier pour des finalités de surveillance, mais pas uniquement. Les systèmes équipés de ces technologies algorithmiques permettent de détecter automatiquement des personnes, des gestes ou des comportements : ils visent à identifier, authentifier ou catégoriser automatiquement les personnes ou leurs agissements tant dans la sphère publique que privée, et ce en temps réel ou différé. Certains systèmes sont potentiellement bénéfiques pour l'ensemble de la société; d'autres font craindre le pire pour les libertés publiques, ce qui suscite des positions très tranchées, des controverses et des dilemmes qu'il convient d'objectiver.

Le Comité national pilote d'éthique du numérique (CNPEN) souhaite par cet avis apporter des éléments pour éclairer ces débats en explorant les questionnements éthiques que les technologies intégrées aux systèmes de reconnaissance faciale, posturale et comportementale soulèvent. La profusion et l'accumulation de leurs applications exigent de s'interroger collectivement sur le bien-fondé, les désagréments, voire les dangers potentiels de chacune d'entre elles, dans son contexte d'usage. La reconnaissance faciale, posturale et comportementale est à la source de bien des commodités. Ainsi, la propose-t-on de plus en plus communément pour s'authentifier dans de nombreux services, par exemple pour accéder à son compte bancaire à distance ou actionner son téléphone portable, ou encore pour franchir une frontière ou pour limiter le nombre de présentations de ses pièces d'identité dans un aéroport. Elle est présentée comme une valeur ajoutée à un service ou à un usage sans pour autant que soient toujours précisées les limites, les conséquences ou les conditions de son usage.

Il arrive parfois qu'elle soit utilisée à l'insu des personnes ou de façon plus ou moins contrainte, sous la forme d'une surveillance, d'un suivi biométrique individuel ou collectif dans des espaces publics, privés ou de transit. Elle peut aussi conduire à un traçage très intrusif des individus par la détection, le suivi ou le contrôle d'un accès en faisant parfois appel à la reconnaissance des émotions ou à des données biométriques spécifiques. Ceci tout autant pour des finalités qui peuvent être le respect d'une loi, d'un règlement privé, un objectif d'intérêt général, que des finalités définies par des opérateurs privés pour d'autres types de services. Il reste que les conditions de conception et d'usage sont rarement explicites, ce qui contribue à réactiver les craintes de voir émerger au sein de la société un dispositif panoptique qui, à l'instar du « regard sans visage » de Michel Foucault, transformerait « tout le corps social en un champ de perception».[1]

Les technologies automatisées de reconnaissance faciale, comportementale et posturale sont devenues diffuses dans notre environnement et de plus en plus souvent présentées comme étant une solution dans un contexte international qui tend à en généraliser ou en normaliser l'usage.

[1] M. Foucault - *Surveiller et punir. Naissance de la prison. Gallimard,* 1975.

Dans la perspective des Jeux olympiques de 2024, il est par exemple proposé d'utiliser ces technologies pour détecter les mouvements de foule, afin d'anticiper les engorgements et leurs conséquences funestes et, par là, renforcer la sécurité collective. Ce dispositif diffère fondamentalement des technologies de reconnaissance faciale qui ont précédemment été utilisées en 2021 pour contrôler les athlètes, les bénévoles et le personnel des stades et des installations des Jeux olympiques et paralympiques de Tokyo[2].

Ces technologies sont de plus en plus utilisées dans le domaine de la sécurité, pour le contrôle aux frontières depuis la mise en place d'équipements de contrôle automatisés tel que le système PARAFE en 2017. Elles sont parfois associées aux systèmes vidéo pré-existants dans les villes, dans les transports (gares, métro, aéroports), dans les espaces de loisirs ou commerciaux ou encore dans les écoles. Les forces de police y ont recours pour résoudre des situations ou des incidents spécifiques (vols, accidents, repérage d'une personne). Certaines collectivités ont conduit des expérimentations pour contrôler l'accès à des événements ou à des écoles. Ce fut le cas dans la ville de Nice, lors de son carnaval en 2019. Les projets de déploiement de ces technologies dans l'espace public visent deux finalités distinctes, bien que non exclusives : une finalité préventive (police administrative), pour prévenir les infractions ou essayer d'intervenir au moment où elles sont commises, et une finalité répressive (police judiciaire), pour appréhender les auteurs de ces infractions et apporter des éléments de preuve à l'enquête.
Dans le domaine de la santé, grâce aux avancées de l'apprentissage profond, l'analyse des émotions ou du comportement permet de détecter certaines maladies, tel le syndrome de DiGeorge[3] ou la réaction à la douleur afin d'ajuster les traitements. Dans le secteur commercial, ces technologies facilitent le suivi des consommateurs ainsi que l'accès des clients à des services sur internet. À titre d'illustration, l'expérimentation MONA conduite par VINCI AIRPORT à l'aéroport Lyon-Saint Exupéry propose un parcours biométrique aux voyageurs : à condition qu'ils acceptent de créer un compte, des portails à reconnaissance faciale placés sur les différents points de contrôle leur évitent de présenter plusieurs fois leurs documents d'identité. Ils peuvent aussi recevoir des informations personnalisées et contextualisées à portée commerciale. Cette expérimentation associe dans un même socle technologique un suivi biométrique et une solution de marketing relationnel.

Les quelques exemples d'applications des techniques de reconnaissance faciale, posturale et comportementale décrits ci-dessus montrent, tant par leur diversité que par la multitude de leurs conséquences potentielles, que l'on ne saurait circonscrire, par avance, les vertus ou les inconvénients intrinsèques de ces différentes technologies. Chaque situation d'usage demande une analyse préalable qui en cerne les enjeux, les conséquences prévisibles et les dérives potentielles. Avant d'être prescriptive, l'approche éthique nécessite une démarche réflexive. En l'occurrence, cette approche réflexive apparaît d'autant plus indispensable que les applications de la reconnaissance faciale, posturale et comportementale diffèrent les unes des autres. Certaines apparaissent bénéfiques, d'autres sont problématiques, et d'autres encore sont tout à la fois utiles et néfastes selon les modalités de leur mise en place ou de leur utilisation. Il importe également d'adopter une démarche prospective afin d'anticiper des détournements d'usage d'applications qui aujourd'hui apparaissent anodines.

Le présent avis insiste sur la méthodologie à mettre en œuvre pour conduire cette démarche réflexive. Elle s'inscrit dans la logique initiée par le rapport de la CNIL intitulé *Reconnaissance faciale : pour un débat à la hauteur des enjeux* paru en 2019[4]. Cette approche passe par la définition précise de ce que l'on entend par reconnaissance faciale, posturale et comportementale, par l'identification des problèmes que ces technologies sont censées résoudre, par une étude de la façon dont elles sont susceptibles de le faire et des risques induits, en particulier de leur détournement à des fins non anticipées. Et pour finir, par une évaluation expérimentale rigoureuse de leur efficacité.
Cet avis a engagé le Comité à approfondir la réflexion sur la démarche à mettre en œuvre et, surtout, sur les enjeux qui ne se limitent pas à la protection des données personnelles.

Outre ce chapitre introductif, le présent avis est constitué de quatre chapitres.
Le chapitre 2 veille à préciser et à décrire ce que l'on entend par reconnaissance faciale, posturale et comportementale, la typologie des acteurs impliqués dans la mise en œuvre de ces technologies et les définitions des termes associés.
Le chapitre 3 souligne les questions que soulève le déploiement d'un système intégrant de la reconnaissance faciale, posturale et comportementale, notamment, comment poser une réflexion pour en évaluer l'efficacité avec rigueur. Nous évoquerons les aspects épistémologiques de cette démarche qui doit se fonder sur des expérimentations scientifiques. Il s'agit aussi d'évaluer les bénéfices potentiels qui justifient le recours à ces technologies au regard de l'impact économique global. Enfin, il convient, surtout dans une démarche éthique, d'anticiper, autant que faire se peut, les modifications des comportements sociaux consécutives à l'utilisation de ces technologies, en particulier les stratégies d'évitement.
Le chapitre 4 aborde les différentes tensions et les dilemmes éthiques.
Enfin, le chapitre 5 formule des recommandations selon les acteurs impliqués. Celles-ci portent sur la finalité des systèmes de reconnaissance faciale, posturale et comportementale, qu'il faut distinguer de leur utilité, sur les notions classiques de proportionnalité et de transparence, sur les risques de biais et de discriminations, sur les aspects scientifiques et épistémologiques de l'évaluation de ces dispositifs, sur les conditions d'usage et enfin sur les aspects économiques et environnementaux.

[2] En effet, la loi du 19 mai 2023 relative aux Jeux olympiques et paralympiques de 2024 ne prévoit l'utilisation d'aucune technique de reconnaissance faciale, ni aucun système d'identification biométrique. En outre, des garanties ont été prévues pour encadrer cette utilisation, comme l'information préalable du public, l'évaluation du dispositif par les parlementaires et le contrôle de la CNIL.
[3] https://www.msdmanuals.com/fr/professional/immunologie-troubles-allergiques/d%C3% Agficits-immunitaires/syndrome-de-digeorge
[4] https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux

ENCADRÉ 1

LES JEUX OLYMPIQUES DE 2024 : L'ABSENCE DE TECHNIQUES DE RECONNAISSANCE FACIALE

Dans la perspective des Jeux olympiques et paralympiques qui se tiendront en France du 24 juillet au 8 septembre 2024, la Loi du 19 mai 2023, complétant celle du 26 mars 2018[a], prévoit des dérogations aux règles en vigueur et autorise certaines expérimentations.

L'étude d'impact du projet de loi met l'accent sur les spécificités et l'ampleur dudit événement pour justifier la nécessité d'adapter le droit aux contraintes propres à son organisation, dans le respect du principe de proportionnalité. L'article 10 prévoit ainsi, à titre expérimental, que les images collectées au moyen d'un système de vidéoprotection ou de caméras installées sur des aéronefs pourront faire l'objet de traitements algorithmiques afin de détecter et signaler certains événements. Il ressort de l'étude d'impact[b] que la mise en œuvre de solutions utilisant des techniques d'intelligence artificielle est strictement encadrée : les traitements visent une finalité unique, assurer la sécurité de manifestations sportives, récréatives ou culturelles, ou de lieux publics, lesquels sont particulièrement exposés à des risques d'actes de terrorisme (marchés de Noël, concerts, transports). Ces traitements portent sur un vivier d'images limité pour détecter des événements prédéterminés susceptibles de présenter ou de révéler l'un de ces risques et de les signaler en vue d'améliorer les conditions d'intervention des services compétents. En outre, ces algorithmes ne fonctionnent qu'en temps réel et non en temps différé sur des images conservées et excluent l'utilisation de données biométriques ainsi que tout recours à des dispositifs d'identification biométrique ou de reconnaissance faciale.

Les traitements algorithmiques pourront porter sur la détection d'objets (armes, colis abandonnés) ou de situations à risque (mouvements de foule, personnes au sol), mais ne permettront pas d'identifier les individus concernés. Enfin, ces traitements ne pourront procéder à aucun rapprochement, interconnexion ou mise en relation automatisée avec d'autres traitements de données à caractère personnel.

Cette disposition a été vivement contestée mais le Conseil constitutionnel, constatant l'absence de techniques de reconnaissance faciale et de systèmes d'identification biométrique, a considéré que le recours à des traitements algorithmiques était entouré de garanties suffisantes[c]. En validant la loi du 19 mai 2023, le juge constitutionnel a estimé que ces dispositions ne méconnaissaient ni la liberté d'aller et venir, ni le droit de manifester, ni la liberté d'opinion, ni le droit au respect de la vie privée. Il n'a pas davantage suivi les requérants qui estimaient que la loi portait atteinte au principe d'égalité (au prétexte que les critères des traitements algorithmiques n'excluraient pas toute discrimination), ni qu'elle violait la dignité de la personne humaine en permettant, toujours selon les requérants, le traitement des images par des algorithmes sans intervention d'un être humain.

En effet, il ressort des dispositions de la loi que les traitements algorithmiques employés doivent permettre de vérifier l'objectivité des critères et la nature des données traitées ainsi que comporter des mesures de contrôle humain et un système de gestion des risques pour prévenir et corriger la survenue de biais ou de mauvaises utilisations.

Enfin, s'agissant de la pérennisation éventuelle du dispositif expérimental, il appartiendra au législateur de tirer les conséquences de l'évaluation de ce dispositif et, en tenant compte du droit au respect de la vie privée, d'examiner son efficacité dans la prévention des atteintes à l'ordre public. À la lumière de ces éléments, la conformité du dispositif à la Constitution pourra le cas échéant de nouveau être examinée[d].

[a] LOI n° 2018-202 du 26 mars 2018 relative à l'organisation des Jeux olympiques de 2024.

[b] https://www.legifrance.gouv.fr/contenu/Media/files/autour-de-la-loi/legislatif-et-reglementaire/etudes-d-impact-des-lois/ei_art_39_2022/ei_-spox2233026l_cm_22.12.2022.pdf.

[c] Décision n°2023-850 DC du 17 mai 2023 - Loi relative aux Jeux olympiques et paralympiques de 2024.

[d] Notons que ces conclusions du Conseil constitutionnel ne font pas l'unanimité des juristes : voir Céline Castets-Renard, "Caméras augmentées" : un danger pour les libertés lors des Jeux Olympiques et Paralympiques (et au-delà) ? Recueil Dalloz n°22 2023 pp.1138-1141.

2. ASPECTS TECHNIQUES ET VOCABULAIRE

2.1 LES COMPOSANTES DU SYSTÈME

2.1.1 COMPOSANTES MATÉRIELLES

Un système numérique de reconnaissance faciale, posturale ou comportementale repose tout d'abord sur **un ou plusieurs capteur(s)** dont le rôle est de recueillir des signaux physiques sur la scène ou l'environnement dans lequel il(s) est (sont) placé(s). Un capteur peut être une caméra dans le domaine visible ou infrarouge (pour le recueil de signaux la nuit), un radar (pour le recueil de signaux relatifs à la position et à la vitesse de déplacement d'objets), un microphone, un capteur à ultrasons. Plusieurs capteurs peuvent être associés, par exemple une caméra et un microphone (recueil de vidéos sonorisées). Ils peuvent également être mis en réseau par des dispositifs de communication afin de couvrir un environnement large, par exemple l'ensemble d'une ville.

Un capteur peut être fixe, par exemple une caméra montée sur un mât disposé à un carrefour ou à l'angle d'un distributeur automatique de billets. Il peut être mobile, et cela de plusieurs façons : il peut effectuer un balayage de l'environnement à partir d'un point d'ancrage fixe, par exemple une caméra pivotant sur un mât dans des limites angulaires données ; il peut être monté sur un dispositif mobile, par exemple un drone ou un autre aéronef, ou bien un téléphone portable.

Un capteur peut recueillir des signaux de manière instantanée (photographie), ou pendant un certain créneau temporel, voire de manière permanente (vidéo).

Dans certains cas d'usage, il n'y a pas de capteurs spécifiquement mis en œuvre pour la reconnaissance : celle-ci est effectuée directement à partir de la mise en correspondance de données numériques préexistantes, comme la reconnaissance de personnes sur des photographies publiées sur les réseaux sociaux numériques.

Noter enfin que dans cet avis nous ne considérerons pas les dispositifs fondés sur des capteurs qui sont portés au contact du corps d'une personne (pour la détection d'armes par exemple) ou qui recueillent des signaux concernant l'intérieur du corps (par exemple des capteurs d'échographie).

2.1.2 COMPOSANTES LOGICIELLES

Les signaux recueillis par les capteurs sont traités par des logiciels embarqués sur les capteurs ou déportés sur un autre support. Dans ce dernier cas, les signaux sont transmis depuis le capteur par un moyen de communication (liaison de données). Pour un objectif de reconnaissance automatisée ou d'aide à la reconnaissance, les traitements logiciels consistent à interpréter les signaux recueillis par le capteur, c'est-à-dire à leur donner un sens pertinent pour la finalité concernée. Le résultat du traitement sera ainsi « oui » ou « non » (une personne est reconnue ou non), le nom ou l'identifiant d'une personne, le suivi d'une personne ou d'un objet mobile, la qualification d'un comportement (« court », « dépose un objet »), etc.

L'interprétation des signaux nécessite des références, à partir desquelles on établit des mises en correspondance. Ainsi, pour indiquer qu'une personne est bien celle qui présente son passeport, on évalue la proximité de son image à la photographie qui figure sur le passeport. Cette évaluation passe par un calcul de similitude entre différents points remarquables de cette image (yeux, nez, oreilles, etc.) et ceux qui y correspondent sur la photographie du passeport.
Les références peuvent faire appel à des modèles décrits par un ensemble de caractéristiques – par exemple, dans le cas de descriptions de comportements, des modèles d'action comprenant l'action de « déposer un objet » elle-même constituée d'une séquence de sous-actions telles que « déplacement avec objet », « arrêt avec objet », « déplacement sans objet », auxquelles sont associés des paramètres de proximité, de vitesse, d'incertitude, etc[1].
Les références peuvent aussi être constituées de bases de données à partir desquelles le logiciel va calculer des corrélations entre les signaux recueillis et les éléments de ces bases, en fournissant comme résultats les éléments dont certaines caractéristiques sont statistiquement les plus « proches » de celles du signal recueilli. On peut alors faire appel à des algorithmes d'apprentissage machine pour exploiter des données et caractériser une classe d'exemples, par exemple une émotion.
Notons que l'apprentissage machine vise à acquérir des connaissances à partir d'expériences passées. Différentes approches existent (apprentissage par renforcement, regroupement conceptuel, apprentissage paresseux, apprentissage par l'action, etc.). Parmi elles, on recourt le plus souvent à l'apprentissage supervisé. Ce dernier part d'un flux d'exemples étiquetés, c'est à dire à chacun duquel est associée une catégorie. Il construit ensuite une fonction en mesure de retrouver l'étiquette de chaque exemple. Notons qu'il existe une grande multitude de techniques d'apprentissage supervisé : construction d'arbres de décisions, programmation logique inductive, machines à noyaux, apprentissage profond, etc. Leur choix dépend en grande partie de la nature des données.

[1] Rim Romdhane et al. "Activity Recognition and Uncertain Knowledge in Video Scenes". In: IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS). Krakow, Poland, Aug. 2013. url: https://hal.inria.fr/hal-01059602.

2.1.3 COMPOSANTES HUMAINES

Le dispositif de reconnaissance peut être entièrement automatisé, comme c'est le cas pour le système PARAFE[2] (Passage rapide aux frontières extérieures). Dans ce cas précis, des professionnels sont sur place pour superviser les opérations et intervenir si besoin. Le dispositif peut toutefois fonctionner sans composante humaine explicite, comme c'est par exemple le cas pour la reconnaissance de personnes sur les photographies publiées sur les réseaux sociaux numériques. Dans ce contexte, une personne déjà identifiée sera « reconnue » automatiquement sur d'autres photographies, sans que personne ne viennent confirmer ou infirmer la reconnaissance.

Le système peut aussi être conçu pour apporter une aide à des utilisateurs professionnels, par exemple en donnant l'alarme suite à la reconnaissance d'une personne, d'un comportement ou encore d'une situation. C'est alors aux opérateurs, associant le cas échéant les autorités compétentes, de confirmer ou non l'information fournie par le système et d'agir en conséquence. Le dispositif est constitué alors d'éléments matériels et logiciels associés à des opérateurs humains. Les domaines d'usage de tels systèmes sont par exemple la santé (aide à la détection de la douleur, confirmation de l'identité d'une personne avant une intervention chirurgicale), la sécurité (aide à la détection d'agressions ou de mouvements de foules problématiques), le domaine militaire (aide à l'appréciation d'une situation).

2.2 TYPOLOGIE DES ACTEURS IMPLIQUÉS

Par souci de précision, nous proposons une typologie des acteurs impliqués à différents égards dans la conception, la fabrication, la mise en œuvre et l'utilisation de dispositifs de reconnaissance faciale, posturale et comportementale. Celle-ci se fonde, avec quelques adaptations, sur les terminologies utilisées dans l'élaboration du projet de règlement européen sur l'intelligence artificielle.

1. Le **scientifique**, qui observe et analyse les effets des technologies de reconnaissance faciale, posturale ou comportementale. Il peut aussi s'agir du **concepteu**r ou **chercheur** à l'origine d'une méthode ou d'un système pour le traitement du signal ou de l'image.
2. L'**ingénieur** ou le **développeur**, qui travaille pour le compte d'un fabricant et qui développe des dispositifs intégrant des technologies de reconnaissance faciale, posturale ou comportementale.
3. Le **fabricant** qui, comme son nom l'indique, fabrique et vend des dispositifs intégrant des technologies de reconnaissance faciale, posturale ou comportementale.
4. Le **fournisseur** ou l'**intégrateur**, qui conçoit et commercialise des produits ou des services associés. Il peut acheter le produit au fabricant, ou en acquérir une licence, pour le mettre sur le marché dans son propre système. Il peut être un importateur ou un distributeur. Il peut également être le fournisseur d'un service mettant en œuvre des dispositifs intégrant des technologies de reconnaissance faciale, posturale ou comportementale.
5. L'**utilisateur-exploitant**, qui acquiert le système et utilise ses résultats pour ses propres opérations. *Exemples : gestion d'aéroport, police des frontières (système PARAFE), SNCF, RATP, centre commercial, commune, industriel du numérique (déverrouillage de téléphones, reconnaissance des personnes sur les réseaux sociaux numériques), direction d'entreprises (badges d'accès), etc.*
6. L'**opérateur**, qui est un professionnel chargé de la mise en œuvre, de la supervision et de la maintenance des systèmes technologiques déployés. Cet acteur intervient lorsque la mise en œuvre du système exige une compétence particulière. Par exemple, l'opérateur interprète le résultat fourni par le système et décide des actions qu'il juge appropriées.
7. La **personne physique concernée**, qui est exposée au système, qu'elle connaisse ou non son existence et qu'elle ait ou non donné son consentement. *Exemples : passant, spectateur d'un événement sportif, consommateur, voyageur, personne utilisant la reconnaissance faciale sur son téléphone, utilisateur d'un réseau social numérique, etc.*
8. Le **législateur**, *national* ou *supra-national*, qui a la responsabilité d'établir le cadre juridique et règlementaire de déploiement des dispositifs technologiques. *Exemples : le parlement, le gouvernement, les institutions européennes, etc.*
9. Les **représentants institutionnels**, qui ont la responsabilité du cadre de déploiement de ces dispositifs. *Exemples : les collectivités territoriales, le chef d'État, etc.*
10. Les **régulateurs**, qui sont les autorités publiques qui accompagnent et veillent à la conformité du déploiement du système de reconnaissance à la législation et à la réglementation en vigueur. *Exemples : CNIL, ARCEP, etc.*
11. L'**organisme de certification**, qui exécute des tests et des évaluations de conformité en vue de l'autorisation du déploiement d'un système en fonction de la législation. Cet organisme peut être une autorité de certification publique ou une structure privée, voire le fabricant lui-même (auto-certification), ou une structure indépendante mandatée, selon la législation.
12. Les **représentants** des différentes composantes de la société civile. *Exemples : syndicat, association de riverains, organisation de consommateurs, club de réflexion, ONG, etc.*

2.3 IDENTIFICATION DES BESOINS

Les éléments matériels (en particulier les capteurs) et logiciels constitutifs des dispositifs de reconnaissance faciale, posturale et comportementale doivent répondre à un cahier des charges précis qui, lui-même, doit répondre à une finalité. Ils doivent être réalisés selon des spécifications techniques précises issues du cahier des charges dont on doit pouvoir montrer qu'elles sont respectées et qu'elles répondent bien aux besoins.
Ces besoins sont motivés par des arguments très divers :

- **Efficacité** : gain de temps par rapport à une action (déverrouillage de téléphone) ou une reconnaissance (PARAFE) uniquement manuelle ou humaine ;
- **Performance** : mise en évidence de caractéristiques que l'observateur humain est susceptible de ne pas détecter ;
- **Permanence** : disponibilité dans la durée ;
- **Économie** : réduction du personnel de surveillance, de contrôle ;
- **Couverture** : ampleur du déploiement des capteurs (cas des caméras déployées dans les villes) ;
- **Sécurité** : détection d'événements potentiellement attentatoires aux personnes et aux biens ; régulation des flux (quais de métros, stades) ;
- **Politique** : mise en œuvre d'une politique publique.

[2] https://www.immigration.interieur.gouv.fr/Europe-et-International/La-circulation-transfrontiere/Le-passage-rapide-aux-frontieres-exterieures-PARAFE

2.4 DÉFINITION DES TERMES

2.4.1 RECONNAISSANCE ET RECONNAISSANCE FACIALE, POSTURALE ET COMPORTEMENTALE

Apparu très anciennement dans la langue française, le terme de reconnaissance s'emploie dans de nombreux contextes avec des sens différents. Ainsi, la reconnaissance pour un militaire qui explore un territoire ennemi afin de recueillir des renseignements n'est pas la reconnaissance, entendue au plan juridique, de la paternité ou de la maternité d'un enfant naturel, ni *a fortiori* la reconnaissance politique d'un État. Sur le plan philosophique, on distingue classiquement au moins trois sens du terme reconnaissance[3]. Pour le premier, *reconnaître* quelqu'un signifie que l'on réalise qu'on le connaît déjà. Au deuxième sens, se reconnaître soi-même consiste à reconnaître la portée de ses actes et donc à en assumer, individuellement, la responsabilité ; c'est l'origine de l'éthique. Enfin, au troisième sens, reconnaître une personne[4] consiste à lui attribuer du mérite, de la valeur, du respect, autrement dit à la distinguer. Dans le champ des technologies du numérique, la reconnaissance tient partiellement au premier sens, à savoir retrouver l'identité d'une personne. Elle tient aussi en partie au troisième sens, puisqu'il s'agit de catégoriser une personne, par exemple de la classifier selon le genre, et donc de lui attribuer une qualité.

On distingue la reconnaissance faciale (visage), posturale (position du corps) et comportementale (dynamique des mouvements). Ces trois formes de reconnaissance peuvent être associées, par exemple afin de produire un résultat du type : « Camille Dupont est en train de courir en cachant un objet contre son corps ». Il est aussi loisible d'ajouter les dimensions vocales (le timbre, la hauteur et l'intensité de la voix) et verbales à la dynamique corporelle pour faciliter la reconnaissance ou affiner les résultats. Nous limiterons ici notre regard à des dispositifs non invasifs, ce qui exclut par exemple les analyses ADN ou des techniques d'imagerie cérébrale. Les modules de reconnaissance automatique se distinguent aussi par la nature des signaux - image, vidéo, son, etc. - qu'ils admettent en entrée et par les capteurs qui les recueillent - caméras, microphones, etc.

Notons qu'en toute rigueur, un système numérique ne « reconnaît » pas, aux sens définis ci-dessus, une personne ; par des calculs, il met en correspondance des signaux avec des données stockées en mémoire pour retrouver une identité ou catégoriser un comportement. Un système numérique de reconnaissance ne doit donc pas être mis sur le même plan qu'un être humain. Seul ce dernier reconnaît véritablement, éventuellement avec l'aide d'un système numérique.

2.4.2 OBJECTIFS DU TRAITEMENT : AUTHENTIFICATION, IDENTIFICATION ET CATÉGORISATION

Indépendamment tant des traits physiologiques (visage, voix, etc.) et comportementaux analysés que des signaux physiques traités, on distingue usuellement trois processus de reconnaissance.[5] Ces trois processus reflètent, à certains égards, les différents sens[6] de la reconnaissance évoqués plus haut :

L'**authentification** vise à assurer qu'une personne est bien celle qu'elle est censée être. En pratique, l'authentification est utilisée pour confirmer l'identité d'une personne donnée à partir de son visage, par exemple en déterminant que le porteur d'un passeport est bien celui que mentionne le passeport, ou que la personne qui déverrouille un téléphone est bien la propriétaire de l'appareil.
Du point de vue logique, il s'agit d'un processus d'appariement « 1 avec 1 ».

L'**identification** vise à repérer un individu dans un ensemble de personnes uniquement à partir de son visage, de sa posture, de sa démarche ou plus généralement de son comportement. Il est ainsi possible de repérer qui, parmi les individus figurant dans une base de données, se trouve sur une image ou une vidéo publiée sur un réseau social numérique ou filmée par une caméra dans la rue.
Du point de vue logique, il s'agit d'un processus de recherche de « 1 parmi n ».

La **catégorisation** classifie les individus selon un critère prédéterminé, par exemple leur genre, leur âge, leurs comportements, leurs émotions, etc. Certains travaux essayent même de caractériser les personnes selon l'orientation sexuelle[7], religieuse ou politique[8] ou encore l'origine ethnique. Notons que beaucoup de ces tentatives soulèvent des questions d'ordre épistémologique et éthique. En effet, rien ne prouve que l'orientation sexuelle, religieuse ou politique se traduise par des traits physionomiques et comportementaux.
Du point de vue logique, il s'agit d'un processus de classification de « p parmi n ».

On peut en outre distinguer la reconnaissance **statique**, par exemple l'identification d'un individu à un moment donné, de la reconnaissance **dynamique**, par exemple le suivi d'un individu grâce à la persistance de certains attributs, par exemple ses habits, dans un flot d'images, ce qui ne passe pas nécessairement par une identification de cet individu.

[3] Paul Ricœur. *Parcours de la reconnaissance*. Ed. by Stock. Les Essais. Paris, France, Jan. 2004.
[4] Axel Honneth. *La lutte pour la reconnaissance*. Passage. Paris, France: Editions du Cerf, 2000.
[5] Davide Castelvecchi. "Is facial recognition too biased to be let loose?" In: *Nature* 587.7834 (Nov. 2020), pp. 347–349. doi: 10.1038/d41586-020-03186-4. url: https://www.nature.com/articles/d41586-020- 03186-4.
[6] Les définitions proposées ici diffèrent de celles de la norme ISO/IEC 2382-37:2022, https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:2382:-37:ed-3:v1:fr
[7] En dépit des réserves que nous nourrissons sur la qualité et la probité de ce travail, nous en donnons la référence par souci d'exhaustivité (Yilun Wang and Michal Kosinski. "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images". eng. In: *Journal of Personality and Social Psychology* 114.2 [Feb. 2018], pp. 246–257. doi: 10.1037/pspa0000098)
[8] Avec la même réserve que pour la référence précédente, on peut citer (Michal Kosinski. "Facial recognition technology can expose political orientation from naturalistic facial images". en. In: *Scientific Reports* 11.1 [Dec. 2021], p. 100. doi: https://doi.org/10.1038/s41598- 020-79310-1. url: http://www.nature.com/articles/s41598-020-79310-1)

2.4.3 SURVEILLANCE, CONTRÔLE, PROTECTION

Les notions de surveillance, de contrôle et de protection sont éminemment polysémiques, ce qui explique de multiples malentendus. Nous retiendrons ici les significations qui apparaissent les plus pertinentes dans le contexte de la reconnaissance faciale, posturale et comportementale.

Surveiller, c'est d'abord *veiller*. Cela s'entend tout à la fois au sens de *« veiller sur une personne dont on a la responsabilité morale »* qu'au sens pratique de *« veiller au bon déroulement d'une activité »*[9]. Mais, cela signifie aussi *« se tenir informé, par des moyens policiers, des activités de personnes jugées suspectes, du comportement de collectivités, de groupes, de lieux à risques »*[10]. Il en résulte une tension potentielle entre une signification qui tend à la protection et une autre qui vise à l'investigation policière.

Contrôler signifie tout à la fois *« vérifier quelque chose »* et *« maîtriser volontairement son corps, ses sentiments, ses instincts »* voire *« exercer une domination morale ou politique*[11] *»*. Là encore, il existe une tension entre une simple vérification de la conformité de l'objet du contrôle à une norme fixée par avance et une soumission de cet objet à une norme ou à des individus.

Protéger signifie *« mettre à l'abri »*. Le terme vient du latin *protegere (« couvrir devant, en avant, abriter »)* qui lui-même dérive de l'accolement du préfixe *pro- (« devant, en avant »)* au verbe *tegere (« couvrir, recouvrir; abriter; garantir »)*[12].

Une caméra dite « caméra de surveillance » ne surveille pas, au sens propre, dans la mesure où elle ne « veille » pas par elle-même et où elle se tient moins encore informée : la caméra capte des signaux et les logiciels traitent ces signaux. De même un « système de vidéoprotection » ne protège pas puisqu'il ne met pas à l'abri des dangers. Ces expressions sont de fait des raccourcis sémantiques pour désigner l'ensemble du système constitué des capteurs, des logiciels et des opérateurs humains. Ce système peut alors contribuer à surveiller dans l'un des trois sens du terme, à savoir *veiller sur une personne, s'assurer du bon déroulement d'un processus et se tenir informé par des moyens policiers*. À cet égard, on constate que, de plus en plus, l'expression « vidéoprotection » remplace « vidéosurveillance », du fait de sa connotation plus rassurante (on préfère certainement être protégé plutôt que surveillé).

2.4.4 FONCTION, USAGE ET CONDITIONS D'USAGE

Un dispositif technologique a une **fonction** bien définie, par exemple l'authentification. L'**usage** décrit le mode d'utilisation du dispositif technologique, par exemple la vérification de l'identité ou l'accès à un service numérique. Un dispositif de reconnaissance peut être mis en place dans un environnement public (par exemple la rue), privé mais ouvert au public (par exemple un aéroport), non ouvert au public (par exemple une entreprise), ou bien personnel (par exemple pour l'accès à un téléphone ou à un domicile). Les **conditions d'usage** imposent des contraintes à l'utilisation d'un dispositif, par exemple l'âge pour le passage dans le système de contrôle automatisé aux frontières. Certaines de ces contraintes peuvent être reliées à des enjeux d'ordre réglementaire, par exemple la durée de conservation des données, voire à des enjeux d'éthique.

[9] Dictionnaire de l'Académie française
[10] Trésor de la Langue Française informatisé (TLFi)
[11] TLFi, ibid.
[12] TLFi, ibid.

3. QUESTIONS OUVERTES

3.1 ASPECTS ÉPISTÉMOLOGIQUES

La **finalité** d'un dispositif de reconnaissance doit d'abord et toujours être explicitée, de façon claire, précise et non-ambiguë : que cherche-t-on exactement à faire avec ce dispositif ? Détecter une agression dans un parking, authentifier une personne à partir d'un document d'identité, par exemple de son passeport, identifier une personne lors d'un interrogatoire ou sur un brancard, analyser des bandes vidéo pour retrouver les personnes qui s'y trouvent, déterminer les émotions d'un passant ou la fatigue du conducteur d'une voiture, etc. C'est le premier point, le plus important. Il se peut qu'il existe simultanément **plusieurs finalités** dont certaines peuvent être dissimulées. Par exemple, le recours à une technologie de reconnaissance faciale dans un aéroport peut poursuivre plusieurs finalités comme l'exigence de sécurité, la modernisation de l'aéroport via l'amélioration des services, des gains économiques (résultant éventuellement du licenciement du personnel) ou encore le souci de réaliser des opérations de façon plus rapide afin de faire gagner du temps aux usagers. Celles-ci reflètent les intérêts des différents acteurs et parties prenantes. Il importe, par conséquent, de veiller à énoncer explicitement ces différentes finalités, étant précisé que ces dernières peuvent s'inscrire dans des registres différents (la volonté de réaliser des gains de temps ou d'argent n'est pas à mettre sur le même plan que l'exigence de sécurité). À cela, on doit ajouter le risque de détournement – intentionnel ou non – des dispositifs technologiques. Ainsi, la volonté de renforcer la sécurité ne doit pas conduire à une généralisation de la surveillance de la population ou la mise en œuvre de décisions liberticides. Ces finalités peuvent faire l'objet de débats et éventuellement de régulations (voir recommandations 5.1 et 5.5).

Pour répondre à ces finalités, il faut se demander quels moyens technologiques, tant matériels que logiciels, peuvent être utilisés. Il convient d'analyser en quoi les moyens permettent d'atteindre les finalités en **confrontant les différentes solutions possibles**, sans s'en remettre à la « solution miracle », clé en main, que propose un seul fournisseur. Cette comparaison de différentes solutions technologiques et de différentes architectures matérielles et logicielles devrait aussi s'étendre à d'autres dispositifs existants (patrouilles de police, vigiles à l'entrée d'un supermarché, surveillants à l'entrée des établissements scolaires, etc.).

Enfin, il faut s'interroger sur l'**efficacité respective des différentes solutions possibles** au regard de la (ou des) finalité(s) envisagée(s) initialement. Cet examen doit prendre appui sur une **démarche expérimentale rigoureuse et transparente** reposant sur des bases scientifiques solides. Pour être pertinentes, les expérimentations doivent s'opérer dans des contextes représentatifs des conditions d'utilisation finales. La communication des résultats doit être transparente : un simple pourcentage d'erreur ne suffit pas ; il faut expliciter ce que les chiffres signifient exactement et indiquer les conditions de l'expérimentation. Les expérimentations doivent pouvoir faire l'objet de réflexions et de débats publics de façon à permettre à chacun d'apprécier les conséquences de la mise en place d'un dispositif de reconnaissance faciale, posturale et comportementale. (voir recommandations 5.5).

3.2 DIMENSIONS ÉCONOMIQUES ET ENVIRONNEMENTALES

Il faut souligner les **dimensions économiques du déploiement des différents systèmes**, autrement dit l'évaluation de l'ensemble des dépenses nécessaires à leur mise en œuvre (voir recommandations 5.7). On doit faire cette évaluation très précocement et de manière comparative, en mettant en regard les coûts d'autres solutions, qu'elles soient fondées ou non sur des technologies numériques. On prendra alors en considération :

- **L'infrastructure matérielle**, c'est-à-dire les réseaux de capteurs (par exemple des caméras), en quantifiant leur nombre, les frais d'installation et de maintenance, sans oublier leur durée de vie et leur coût environnemental.

- **Les logiciels de traitement**, en particulier de reconnaissance automatique, en gardant à l'esprit la nécessité de stocker des données de façon sécurisée et d'entraîner des logiciels par apprentissage, ce qui a des coûts économiques et environnementaux conséquents.

- **Les frais induits par la mise en place d'équipes chargées de la supervision et de l'utilisation des systèmes**. En effet, contrairement à une idée répandue, la mise en place de systèmes informatiques de surveillance, même s'ils intègrent des logiciels de reconnaissance faciale, posturale et comportementale, requiert des opérateurs professionnels bien formés et donc coûteux.

- Enfin, **les coûts d'expérimentation, de validation, de certification et d'évaluation des risques**.

3.3 MODIFICATION DES COMPORTEMENTS SOCIAUX

La **massification des usages des technologies de surveillance et de contrôle** conduisent à une **évolution des comportements humains**, avec des attitudes tacites de conformité et des stratégies d'évitement. L'expérience chinoise met en évidence ce double mouvement : d'un côté, une soumission à des contraintes très fortes pour l'ensemble de la population, d'un autre côté des esquives de la part de certains qui par leur accoutrement, leur maquillage ou toutes sortes d'astuces tentent d'échapper à la détection. Il convient, par conséquent, de procéder à une évaluation permanente et globale de l'efficacité de ces technologies, non seulement avant leur installation, mais aussi après que ces dispositifs ont été déployés. À supposer que certains quartiers soient surveillés, on risque par exemple d'observer un déplacement de la criminalité vers d'autres lieux. Dans le cas où de tels systèmes de surveillance et de contrôle seraient déployés, l'anticipation et l'analyse régulière des modifications sociétales voire anthropologiques induites sont indispensables. Dans le cas où des dérives seraient observées, par exemple si l'on met en évidence un déplacement de la criminalité, il faudrait reconsidérer le déploiement de ces systèmes.

4. TENSIONS ÉTHIQUES

4.1 TENSION ENTRE L'INDIVIDUEL ET LE COLLECTIF

Nous trouvons dans les technologies de reconnaissance faciale, posturale et comportementale une tension entre, d'une part, les libertés individuelles et collectives (liberté d'aller et venir, liberté de réunion, etc.) et, d'autre part, la sécurité des personnes. Cette tension fait écho à la tension entre deux des sens du mot « surveiller » mentionnés plus haut : *« veiller sur une personne dont on a la responsabilité morale »* et *« se tenir informé (éventuellement par des moyens policiers) »*. Cette tension est d'autant plus difficile à apprécier par le citoyen que sa connaissance des technologies est limitée et, surtout, que ces technologies sont souvent invisibles. Il en résulte tout à la fois une surestimation des dangers, lorsque l'on craint une exploitation excessive des données par les acteurs publics, alors qu'il existe, au sein de l'Union européenne, des garanties juridiques fortes[1] ; et une sous-estimation due, par exemple, à l'ignorance de certains modes de traçage comme ceux qu'exercent certaines sociétés privées à l'insu des utilisateurs qui n'ont pas pris connaissance des conditions générales d'utilisation des dispositifs qu'ils ont achetés ou dont ils bénéficient « gratuitement ». Cette surestimation et cette sous-estimation s'avèrent toutes deux nuisibles : la première risque de conduire à une forme de fatalisme et la seconde à l'imprudence.

L'environnement urbain est de plus en plus imprégné de capteurs de surveillance de comportements (espace public, en particulier la rue ; services publics : les transports communs ; espace privé : la voiture) actionnés par des acteurs multiples et rarement identifiés par le citoyen.

La superposition des dispositifs venant d'acteurs divers et leur massification sans que nous en ayons une vision et une compréhension globales pose la question fondamentale de la maîtrise des conséquences : le croisement envisageable des données recueillies, l'impact potentiel de l'ensemble des dispositifs sur les citoyens et l'effet pour un individu. Il est aussi nécessaire de développer des écosystèmes d'acteurs du public et du privé permettant de cartographier les dispositifs de façon globale, de contrôler la conformité avec les lois et d'analyser les effets éthiquement non souhaitables pour l'individu et pour la société. La connaissance des systèmes et de leurs finalités est une condition à la préservation des libertés individuelles ; seule cette connaissance permet d'aboutir à un consensus fondé sur une réflexion collective.

Pour amoindrir le sentiment d'intrusion qui saisit le citoyen lorsqu'il réalise que d'autres, en particulier des institutions publiques ou privées (banquiers, assureurs, opérateurs internet ou de téléphonie, etc.) détiennent des informations sur lui, il est nécessaire de faire du consentement éclairé un préalable, sous réserve de l'existence d'autres bases légales prévues notamment par le RGPD[2]. Mais, pour que ce consentement soit vraiment éclairé, il faut que les citoyens puissent mettre en regard des restrictions de la liberté qu'ils concèdent, le bénéfice individuel ou collectif qu'ils escomptent.

4.2 L'UTILITÉ MISE EN REGARD DES CONSÉQUENCES INDUITES

La question de l'**utilité** doit être posée de manière objective, raisonnée et argumentée. Elle ne peut pas être estimée a priori sans explorer les bénéfices et les inconvénients de l'ensemble des solutions possibles. Un exemple isolé de l'utilisation d'un système de reconnaissance faciale, comportementale ou posturale dans une situation donnée ne saurait suffire à démontrer l'utilité de recourir à ces systèmes dans des situations comparables. Ainsi, dans le cas des Jeux olympiques, l'ampleur, la nature et l'impact médiatique d'un tel événement peuvent conduire les organisateurs et les gouvernements à utiliser les technologies de reconnaissance faciale et à permettre aux acteurs économiques de déployer des solutions innovantes ou à leur accorder des avantages économiques. Il peut aussi s'agir de répondre à une perception de sécurité. On peut toutefois questionner l'utilité de mettre en place, comme lors des Jeux olympiques de Tokyo en 2021, un système qui utilise de la reconnaissance faciale pour ouvrir la porte à des athlètes ou au personnel plutôt que d'utiliser un badge magnétique classique.

Au-delà de l'utilité perçue ou déclarée de ces systèmes, il est nécessaire d'évaluer le compromis entre les bénéfices et les risques dans différentes situations, notamment :

- l'utilité mise en regard de l'accoutumance : la généralisation de l'utilisation de systèmes de reconnaissance faciale, comportementale ou posturale pour un bénéfice qui n'est pas toujours démontré ou raisonné peut conduire la société à une forme d'accoutumance à ces technologies et à leur banalisation, sans avoir conscience des conséquences à long terme. Ainsi, le recours à la reconnaissance faciale pour le paiement pourrait conduire à terme à une suppression de la monnaie et des autres instruments usuels. L'utilisation de la reconnaissance faciale de manière ponctuelle ou exceptionnelle à l'occasion d'un grand événement dans un contexte sécuritaire sensible, soulève également un questionnement sur deux plans : d'une part, le public peut perdre la conscience des enjeux éthiques ou sociétaux ; d'autre part, les utilisateurs peuvent tirer un avantage de la facilité que ces dispositifs apportent, au point de ne pouvoir s'en passer lors d'un retour à une situation ordinaire.

- dans les usages militaires et le domaine de la guerre : par exemple, dans le contexte des hostilités en Ukraine, l'initiative de la société américaine Clearview AI (Voir Encadré 2) visant à mettre gratuitement à disposition du peuple ukrainien ses outils de reconnaissance faciale afin d'aider les assiégés à lutter contre leurs assaillants est très discutable au plan éthique. Nonobstant les intentions généreuses poursuivies par une telle proposition (aider le peuple assiégé à repérer les soldats russes infiltrés ainsi que d'éventuels auteurs de crimes de guerre) il convient de rappeler que les systèmes de reconnaissance faciale n'identifient pas un individu avec une parfaite certitude. Les conséquences du recours à cette technologie peuvent se révéler dramatiques en cas d'erreur mais aussi générer de nombreux risques, aussi bien sur le terrain éthique que juridique, en matière de droit international humanitaire et de droit international des droits de l'homme. On peut anticiper, par ailleurs, que ces technologies utilisées dans un contexte militaire ou policier soient couplées avec une action de ciblage qui pourrait être automatisée.

[1] Notons que dans le cas où le citoyen européen se rendrait en Chine, il serait clairement exposé à des technologies prohibées en Europe.
[2] Le règlement général sur la protection des données de l'Union européenne (Règlement (UE) 2016/679).

ENCADRÉ 2

L'UTILISATION DE LA RECONNAISSANCE FACIALE DANS UN CONTEXTE DE GUERRE : UN DÉTOURNEMENT D'USAGE

Au début des hostilités en Ukraine, la plupart de nos concitoyens éprouvèrent une forte émotion à la vue des bombardements russes et de la tentative d'invasion de ce pays. Beaucoup, en France, en Europe ou encore de l'autre côté de l'Atlantique, ont souhaité tout mettre en œuvre pour aider ce peuple à recouvrer sa souveraineté. Dans ce contexte, les initiatives susceptibles d'aider les Ukrainiens dans leur combat contre leurs agresseurs ont été encouragées. L'une d'entre elles, parce qu'elle fait appel à la reconnaissance faciale, a retenu notre attention. Il s'agit de la proposition de la société américaine Clearview AI de mettre gratuitement ses outils de reconnaissance faciale au service des assiégés, dans leur lutte contre leurs assaillants. Selon un article de l'agence de presse Reuters[a], Clearview AI a envisagé plusieurs emplois de ces technologies.

Le premier emploi vise à repérer les soldats russes infiltrés, possiblement espions ou saboteurs, lors des contrôles policiers. Il vise aussi à débusquer d'éventuels auteurs de crimes de guerre lors de procès ultérieurs ou à identifier sans ambiguïté des réfugiés ukrainiens.

Une deuxième catégorie d'applications concerne les prisonniers russes, en avertissant leurs familles qu'ils sont détenus, en leur permettant de communiquer avec elles, puis en diffusant sur des réseaux sociaux leurs photos, voire des vidéos où ils apparaissent captifs.

Enfin, un troisième type d'application porte sur le corps des soldats russes morts au front. Clearview AI propose de déterminer leur identité avec leur technique de reconnaissance faciale, puis d'envoyer leur photographie à leurs familles et amis.

Dans le contexte de cette guerre, les intentions de la société Clearview AI apparaissent salutaires à certains, puisqu'elles promettent aux Ukrainiens des moyens de se défendre.

Soulignons toutefois que les techniques de reconnaissance faciale n'identifient pas un individu avec certitude ; il risque donc d'y avoir des méprises aux conséquences potentiellement dramatiques. En outre, ces utilisations de la reconnaissance faciale pourraient avoir des conséquences très discutables au plan moral. En découleraient injustices, humiliations, violations des conventions de Genève sur les prisonniers de guerre, instrumentalisation et profanation de l'image des morts, autant de pratiques condamnables dans toute situation. La volonté de faire le bien, en aidant l'Ukraine à se battre contre son ennemi, risque donc d'aboutir à l'opposé du résultat espéré. Plus généralement, même au service de finalités estimées légitimes, l'emploi des technologies de reconnaissance faciale, posturale et comportementale peut aboutir à des effets éthiquement discutables.

[a] Paresh Dave and Jeffrey Dastin, "Exclusive: Ukraine has started using Clearview AI's facial recognition during war" dépêche de l'agence", Reuters, 14 mars 2022, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13

- dans le contexte policier : il faut s'interroger sur l'utilité de recourir à des systèmes de reconnaissance faciale à des fins sécuritaires lorsque le nombre de personnes contrôlées est disproportionné par rapport à l'objectif, et au bénéfice escompté, de retrouver une seule personne.

- dans un contexte professionnel : il y a l'éventualité d'actes ou de comportements détectés de façon fortuite. Un système de caméras de vidéosurveillance peut parfaitement détecter certains agissements du personnel d'une entreprise, comme une relation amoureuse entre employés, alors que telle n'était pas la finalité du système. La jurisprudence fait également référence à des systèmes de vidéosurveillance mis en place pour repérer d'éventuels vols de clients dans un magasin, qui ont détecté des vols commis par une caissière[3]. Un système de reconnaissance faciale mis en place dans l'ascenseur ou le hall d'une entreprise peut aussi détecter un handicap de l'un de ses clients ou de ses salariés alors que le responsable de l'entreprise n'est pas censé connaître son dossier médical.

- dans le contexte de la conduite automobile : les systèmes de reconnaissance comportementale sont de plus en plus utilisés pour l'automatisation des véhicules et l'aide à la conduite afin de détecter l'endormissement au volant ou encore améliorer une conduite pour un gain de sécurité ou une consommation énergétique plus optimisée. Mais ils peuvent tout autant renseigner une compagnie d'assurance ou un constructeur sur un handicap, une maladie psychiatrique ou une erreur d'attention, sans consentement ou information préalable de l'utilisateur.

4.3 UTILISATIONS PROBLÉMATIQUES PAR ESSENCE

Certains usages des systèmes de reconnaissance faciale, posturale ou comportementale sont par nature problématiques. Nous pouvons d'ores et déjà identifier deux types d'utilisations qui interrogent sur le plan éthique :

- L'**extraction d'informations « sensibles » au sens du RGPD et de la loi informatique et libertés**. En particulier, la prétendue détection de l'orientation sexuelle, origine ethnique, sensibilité politique, appartenance syndicale.
- La **reconnaissance des émotions** en particulier dans certaines situations telles qu'un processus de recrutement ou une procédure judiciaire.

[3] Cour de Cassation, Chambre sociale, du 20 novembre 1991, 88-43.120, Publié au bulletin, arrêt « La Pomme » du 20 novembre 1991.

4.4 LA QUESTION DU CONSENTEMENT LIBRE ET ÉCLAIRÉ

Ainsi que le mentionne le RGPD, pour être licite, le traitement des données à caractère personnel doit être fondé sur le consentement, qui constitue une base juridique, ou reposer sur d'autres fondements légitimes prévus par le RGPD ou une autre disposition du droit national ou du droit de l'Union européenne. Il convient néanmoins de rappeler que le traitement de la donnée biométrique, en sa qualité de donnée sensible, est interdit, conformément au RGDP, sauf exception relative notamment au consentement et à l'intérêt général, que la loi doit prévoir. Le consentement ne constitue donc pas la seule base légale (l'article 9 du RGPD prévoit, par exemple, la sauvegarde des intérêts vitaux de la personne, des motifs d'intérêt public ou encore la recherche scientifique) mais, il importe de le souligner, lorsque le traitement des données se fonde sur le consentement, il doit respecter certaines conditions. En particulier, le responsable du traitement devra être en mesure de prouver que la personne concernée a consenti à l'opération de traitement de façon libre et éclairée. Dans son Avis 136 sur l'évolution des enjeux éthiques relatifs au consentement dans le soin, le CCNE[4] a rappelé que si le consentement bénéficie d'un cadre juridique clair, l'effectivité du recueil du consentement éclairé est souvent interrogée. En effet, comment consentir à quelque chose que l'on ne comprend pas ? À l'image du développement des nouvelles techniques médicales, l'accélération notable de l'utilisation des systèmes de reconnaissance faciale, posturale ou comportementale a considérablement accru la complexité du cadre dans lequel le consentement est requis. C'est la raison pour laquelle il importe de dépasser la conception d'un consentement binaire (oui/non). Il convient de considérer ce dernier comme un processus dynamique qui peut évoluer dans le cadre d'une relation fondée sur une confiance réciproque. Il s'adapte au gré du cheminement de la personne, de l'évolution de ses choix et peut se concrétiser par un refus qu'il faut respecter. En outre, pour les personnes qui ne sont pas en mesure de décider pour elles-mêmes, se pose la question de la décision pour autrui.

Les systèmes de reconnaissance faciale s'appuient sur la collecte des données biométriques qui sont une catégorie particulière de données à caractère personnel. Conformément au RGPD, il convient de s'assurer que la personne concernée donne son consentement explicite au traitement de ses données biométriques, sauf s'il existe une autre base légale en vertu du RGPD. Pour que le consentement soit valable, les personnes doivent être libres de choisir d'utiliser un système de reconnaissance faciale ou un autre dispositif, sans contraintes particulières :

- La personne doit pouvoir émettre un consentement libre, ce qui induit d'avoir effectivement le choix, et de pouvoir retirer son consentement.
- Le consentement doit être spécifique et porter exclusivement sur le traitement de ses données biométriques. Il doit être recueilli après une information transmise dans un langage clair et accessible.
- Le consentement doit être univoque, c'est-à-dire donné par un acte positif clair par lequel la personne manifeste son accord au traitement de ses données, au moyen d'une déclaration écrite, y compris par voie numérique, ou d'une déclaration orale.

Si en pratique, un consentement libre et éclairé n'est pas toujours possible, comme dans le cas de caméras déployées dans l'espace public, ou lors d'un entretien d'embauche en raison de la pression que pourrait exercer l'employeur sur un candidat, une note d'information doit toujours être rendue accessible.

S'il n'a pas substantiellement modifié la définition du consentement, le RGPD en a renforcé la teneur et la portée, au point d'en faire une exception au principe d'interdiction du traite- ment des données biométriques aux fins d'identifier une personne physique (article 9.1 RGPD). L'appréhension du consentement érigé en base juridique à l'article 9.2 du RGPD, reste difficile, compte tenu des usages différents qui peuvent en être faits. Les enjeux ne sont, par exemple, pas les mêmes, selon qu'il s'agit de donner son consentement à des fins d'authentification ou d'identification.

4.5 LA SUPERVISION HUMAINE

Rappelons que les systèmes de reconnaissance faciale, posturale ou comportementale impliquent de nombreux acteurs dans toutes les phases de leur existence - de leur conception à leur maintenance - et font intervenir différentes parties prenantes à tous les niveaux de leur architecture. Cette multitude d'acteurs impliqués, en plus des difficultés liées à l'intrication d'une chaîne d'interactions entre l'humain et la machine, complexifie la question de la responsabilité et pose un risque de dilution de celle-ci. C'est pourquoi il importe de distinguer les rôles de chacun et de définir en amont le type de responsabilité, tant sur le terrain juridique qu'éthique. Si les systèmes algorithmiques effectuent des calculs à partir d'une masse de données pour aboutir à un résultat, la valeur de ce résultat relève de la qualité des données et des modèles de calcul et d'apprentissage qui peuvent comprendre un certain nombre de biais. Aussi, la façon dont ce résultat contribue à une décision demande à être considérée avec attention.

Ainsi, il est essentiel d'identifier les tensions éthiques induites par la mise en œuvre des technologies de reconnaissance faciale, posturale ou comportementale et l'utilisation de ces systèmes dans différents contextes d'usage au regard du rôle de l'humain et des éventuels « conflits d'autorité » qui peuvent advenir lors du processus de décision. Il peut s'agir de litiges sur l'identité ou l'intention d'une personne lors d'un transit ou d'un accès, de l'analyse d'une douleur conduisant à un diagnostic ou un traitement, ou encore la détection d'un comportement aboutissant à une décision policière.
Les conséquences d'une décision affectant des individus impliquent une responsabilité qui ne pourra pas être attribuée à une technologie, un système ou une machine : seuls des êtres humains ou des organisations représentées par des êtres humains peuvent porter la responsabilité juridique d'une décision affectant les individus (cf. recommandations 5.6).
Par ailleurs, l'utilisation de systèmes algorithmiques obéit à des réglementations qui exigent une transparence de ces décisions.

Penser le partage des rôles et l'interaction entre l'humain et la machine dans l'objectif de rendre l'utilisation d'un système de reconnaissance faciale, posturale ou comportementale la plus performante possible soulève deux tensions :

[4] Le Comité consultatif national d'éthique pour les sciences de la vie et de la santé : https://www.ccne- ethique.fr/fr

- la mise en place du système est souvent motivée par la nécessité de traitements rapides et automatisés, ce qui rend inopérante la supervision humaine en temps réel ; celle-ci ne peut donc être systématique ;

- l'humain n'est lui-même pas infaillible : il peut se tromper, ou être influencé par les résultats de la machine du fait d'un biais d'automatisation.

Par ailleurs, la mise en place des systèmes de reconnaissance faciale, posturale ou comportementale dans des environnements aussi divers que des lieux de transit, des sites marchands, des entreprises ou des centres médicaux, pose des enjeux de formation et de maintenance et questionne les moyens humains pour assurer la supervision nécessaire à leur bon fonctionnement.
Il s'agit, par exemple, de fournir une formation appropriée aux opérateurs du système afin qu'ils puissent comprendre comment celui-ci fonctionne et juger les performances et la qualité des résultats obtenus. Il est indispensable qu'ils connaissent les limitations des algorithmes, notamment la présence d'artefacts, le degré de précision, d'erreurs et de défaillances du système. Il convient aussi que les opérateurs soient entraînés à son utilisation, pour pouvoir juger de la gravité de la situation et du risque encouru selon le degré de confiance dans les calculs et résultats produits, afin de calibrer au mieux leurs interactions avec la machine. Dans les situations où une réaction en temps réel est exigée, celle-ci devrait dépendre de la confiance accordée au résultat de la machine, évaluée en fonction de ses performances. Il convient aussi de concevoir un système de reconnaissance faciale, posturale ou comportementale d'une manière adaptée au contexte de son utilisation et de préconiser dans cette conception :

- une analyse et une évaluation de la fiabilité des résultats du système (degré de précision de détection, taux de détections erronées) en effectuant des tests périodiques ;

- une interface de visualisation des événements détectés par le système qui présente les incertitudes, des informations de pertinence ou des explications adaptées à un contexte de validation en temps réel ;

- la possibilité pour le système de présenter plusieurs hypothèses de détection et d'interprétation et non pas uniquement celle qui est la plus probable ;

- un enregistrement des sessions (données, interprétation, action humaine) dans la perspective d'audits.

Enfin, les résultats fournis par un système de reconnaissance faciale, posturale ou comportementale ne doivent pas constituer, en eux-mêmes, des éléments de preuve. Ils contribuent à établir la preuve avec des données factuelles, recueillies à travers les capteurs, qu'ils aident à interpréter. Les résultats des systèmes de reconnaissance faciale, posturale ou comportementale ne devraient pas être considérés comme absolus, mais comme des indices. La décision finale doit toujours revenir à l'être humain qui supervise la machine et à qui il revient d'être capable de rendre compte de la responsabilité engagée, quelle que soit l'autorité concernée.

5. RECOMMANDATIONS

Certaines recommandations reprennent des notions bien connues comme la finalité (cf. §5.1), la proportionnalité (cf. §5.2), la transparence (cf. §5.3) et l'équité (cf. §5.4), lesquelles demandent à être transposées au domaine des technologies de reconnaissance faciale, posturale ou comportementale. D'autres sont plus spécifiques, comme l'examen des dimensions scientifiques et épistémologiques (cf. §5.5) des expérimentations ou l'étude des questions économiques (cf. §5.7) et sociales (cf. §5.6) relatives au déploiement de ces dispositifs technologiques.

Les présentes recommandations s'adressent aux différents acteurs impliqués que nous rangeons sous les catégories que nous avons définies dans la section 2.2.

5.1 FINALITÉ ET UTILITÉ

La finalité est le but recherché, soit l'objectif consciemment poursuivi, qui détermine l'intention de concevoir, d'expérimenter ou de commercialiser un service ou un usage faisant appel à un système de reconnaissance faciale, posturale ou comportementale. Des tensions peuvent apparaître entre différentes finalités dans la mesure où, face au recours à un même système de reconnaissance faciale, les parties prenantes peuvent avoir des intérêts divergents (cf. §2.3) et poursuivre des objectifs potentiellement différents (par exemple, les gestionnaires d'un aéroport poursuivront un objectif de fluidification du parcours des voyageurs, les services de sécurité privilégieront la sécurité tandis que les clients auront tendance à mettre l'accent sur la rapidité et l'efficacité dudit système). L'utilité est le bénéfice réel, tangible voire auditable pour ceux à qui s'adresse ce service. La finalité et l'utilité ne doivent pas se confondre. Mais l'une au regard de l'autre permet de déterminer la raison d'être d'un recours à des technologies de reconnaissance faciale, posturale ou comportementale ou au contraire conduit à limiter ou interdire leur utilisation. Il est ainsi nécessaire de préciser clairement et sans ambiguïté la **finalité** et de démontrer l'**utilité** au regard de cette finalité. Cette utilité doit être instruite par des parties multiples sur une base expérimentale et par des résultats tangibles. D'où les recommandations suivantes :

RECOMMANDATION 5.1.1

(UTILISATEURS-EXPLOITANTS, LÉGISLATEURS)

Clarifier la ou les finalités d'un dispositif de reconnaissance faciale, posturale ou comportementale dans un contexte donné, en démontrant clairement son utilité au regard de cette ou de ces finalités. Mettre l'accent sur les raisons qui motivent le recours à ce dispositif dans tel ou tel lieu, ou telle ou telle circonstance.

RECOMMANDATION 5.1.2

(UTILISATEURS-EXPLOITANTS, LÉGISLATEURS)

Établir une cartographie des risques pour les droits et les libertés des personnes mis en jeu par l'utilisation d'un dispositif de reconnaissance faciale, posturale ou comportementale. Mettre ces risques en regard de la raison d'être du dispositif.

RECOMMANDATION 5.1.3

(UTILISATEURS-EXPLOITANTS, LÉGISLATEURS)

Pour identifier et éviter les dérives au regard de la ou des finalité(s) du dispositif de reconnaissance faciale, posturale ou comportementale, prévoir et décrire des procédures périodiques de contrôle, de concertation avec les différentes parties prenantes, d'auditabilité et de certification externes, en mettant l'accent sur l'indépendance de ces dernières. Il importe, par ailleurs, de prendre en considération les retours d'expérience.

ENCADRÉ 3

UN RECOURS DE PLUS EN PLUS FRÉQUENT À LA RECONNAISSANCE FACIALE DANS LES AÉROPORTS EN EUROPE : ENTRE PRUDENCE ET BANALISATION

Le 26 octobre 2023, l'aéroport de Francfort a annoncé la généralisation de son système de reconnaissance faciale, ce qui en fait le premier en Europe à offrir la possibilité à tous les passagers de passer les contrôles de sécurité en recourant intégralement à la technologie biométrique de l'enregistrement à l'embarquement. En Allemagne, d'autres aéroports comme ceux de Hambourg ou Munich, proposent cette technologie mais de façon encore limitée puisqu'elle ne concerne que certains voyageurs (Lufthansa ou Star Alliance). En parallèle à ces initiatives, l'Association du transport aérien international (l'IATA) cherche à promouvoir l'utilisation de l'identification biométrique dans les aéroports en faisant valoir les résultats de ses enquêtes qui tendent à montrer que les passagers sont favorables au traitement de leurs données biométriques si cela accélère les procédures auxquelles ils sont soumis. En France, la reconnaissance faciale est testée à l'aéroport de Lyon depuis 2020 et l'aéroport de Paris-Orly s'apprête également à mettre à l'essai cette technologie pour l'embarquement des passagers. La vision d'un transport aérien entièrement numérique et sécurisé grâce à l'identification biométrique (via le recours, le cas échéant, à « l'identité numérique de voyage »[a]), comme celle promue par l'IATA[b], ne fait cependant pas l'unanimité en Europe et est susceptible de diviser les autorités nationales de régulation sur l'interprétation du RGPD, notamment sur la question du stockage de certaines données. Ainsi, en France, la CNIL a pu, à l'occasion d'une saisine du ministre de l'intérieur[c], exprimer dans sa délibération 2016-012 du 28 janvier 2016 des réserves sur les conditions de conservation des données administratives et techniques[d] collectées et conservées en local à des fins d'analyse statistique des performances des algorithmes de reconnaissance faciale.

La CNIL avait également rappelé les « risques importants » que la reconnaissance faciale fait peser sur les libertés individuelles dans un contexte « caractérisé par une multiplication du nombre des systèmes de vidéoprotection, permettant en théorie le développement massif de la reconnaissance faciale, avec des risques accrus en matière de protection des données et de la vie privée ».
Enfin, l'autorité française soulignait que « les performances de cette technologie, qui n'a pas encore été mise en œuvre par l'État à grande échelle, sont encore à démontrer ». Les doutes persistants exprimés par certains acteurs, malgré des sondages laissant apparaître une certaine confiance des voyageurs dans la technologie biométrique, et la prudence qui entoure la généralisation du recours à la reconnaissance faciale en Europe, laissent entrevoir un paysage à géométrie variable : le déploiement de la reconnaissance faciale est encore très localisé, les expérimentations restent ponctuelles et fortement encadrées, malgré la pression exercée par les associations des sociétés de transport aérien largement favorables à la généralisation des technologies biométriques dans les aéroports.
Ce manque d'harmonisation dans une Europe soucieuse de favoriser la libre concurrence et la libre circulation des personnes, tout en assurant un haut niveau de protection des droits fondamentaux et en préservant la compétitivité sur son marché, pose des questions. Une situation différente en fonction de chaque aéroport pourrait se révéler préjudiciable aussi bien pour les entreprises que pour les citoyens, lesquels s'attendent à être traités de la même façon dans la mesure où le RGPD a vocation à s'appliquer dans tous les États membres de l'Union européenne.

[a] https://www.businesstravel.fr/laeroport-de-francfort-generalise-la-reconnaissance-faciale.html
[b] https://www.air-journal.fr/2021-11-16-iata-ce-que-veulent-les-passagers-du-transport-aerien-5231669.html
[c] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000032372514
[d] Il s'agit des données relatives à la lecture du passeport, aux caractéristiques du passeport, à son détenteur, aux dates et lieux de passage, à la qualité du portrait de référence et du portrait pris sur le moment, à la mesure de la correspondance entre ces deux images et à l'authenticité des données du passeport.

5.2 PROPORTIONNALITÉ

La notion de proportionnalité est essentielle en ce qu'elle permet d'assurer un juste équilibre entre les moyens et les buts et, éventuellement, de procéder à une mise en balance entre différentes finalités. En particulier, la proportionnalité implique de respecter certaines conditions, comme le caractère approprié d'une action (l'action envisagée doit permettre d'atteindre effectivement la finalité poursuivie définie de manière concrète) et sa nécessité (l'action est nécessaire au regard de ce qu'exige la réalisation de cette finalité) ; rapportée à un dispositif technologique, la proportionnalité s'entend au regard des finalités pour lesquelles ce dispositif est conçu et déployé. La proportionnalité s'apprécie selon différents critères, éventuellement incommensurables, tels que les atteintes aux droits et libertés, les impacts environnementaux, les incidences sur la société et la démocratie, les coûts et les efforts économiques.

Notons qu'il convient de ne pas confondre la proportionnalité au regard des finalités avec l'analyse du rapport entre les bénéfices et les risques.

RECOMMANDATION 5.2.1

(SCIENTIFIQUES, LÉGISLATEURS, REPRÉSENTANTS INSTITUTIONNELS, UTILISATEURS-EXPLOITANTS)

Apprécier, sur la base d'arguments tangibles (fondés sur des éléments concrets), la proportionnalité, c'est-à-dire le caractère nécessaire et approprié, de l'emploi des technologies de reconnaissance faciale, posturale ou comportementale au regard des finalités définies de manière concrète et objectivable par des études réalisées à différentes périodes, dans chaque contexte. Prendre également en compte les conséquences induites non recherchées, notamment le traitement des informations recueillies de façon fortuite.

5.3 TRANSPARENCE

La notion de transparence comporte plusieurs dimensions. Une de ces dimensions concerne l'information des personnes. Par exemple, l'emploi de dispositifs de reconnaissance faciale sur le lieu de travail, au moyen de caméras, devrait être clairement mentionné aux salariés.
Une autre dimension tient à la méthodologie d'ensemble qui doit être explicitée pour que toutes les parties prenantes puissent, en particulier en amont, prendre position en connaissance de cause. Enfin, la transparence porte sur les études préalables qui doivent être décrites précisément et dont les conclusions doivent être très largement communiquées, quelles qu'elles soient.

RECOMMANDATION 5.3.1

(FABRICANTS, INTÉGRATEURS)

Mettre à disposition des opérateurs, régulateurs, représentants institutionnels et utilisateurs-exploitants la description de l'architecture matérielle et logicielle du dispositif, la méthodologie d'acquisition et de traitement des données utilisées, les tests effectués ainsi que la base d'apprentissage.

RECOMMANDATION 5.3.2

(UTILISATEURS-EXPLOITANTS, SCIENTIFIQUES)

Énoncer de façon explicite les finalités poursuivies par le recours aux systèmes de reconnaissance faciale, posturale ou comportementale, afin qu'aucune finalité ne soit passée sous silence ou dissimulée. Procéder à des analyses de fiabilité et d'impact des systèmes de reconnaissance faciale, posturale ou comportementale, fondées sur des expérimentations précisément définies et conduites rigoureusement à tous les stades du projet, puis rendre publics via une divulgation transparente mais responsable (pour préserver la sécurité des systèmes d'information) les résultats de ces analyses.

RECOMMANDATION 5.3.3

(TOUS, EN PARTICULIER POUR LES LÉGISLATEURS ET LES MÉDIAS)

Veiller à employer des termes appropriés pour parler des systèmes de reconnaissance faciale, posturale ou comportementale et à éviter les approximations qui induisent en erreur et créent des représentations erronées, que ce soit dans les cahiers des charges, les textes officiels ou les médias.

ENCADRÉ 4

CLARTÉ DU LANGAGE

La qualité du débat relatif à ces technologies nécessite une certaine rigueur sémantique, y compris lorsqu'il s'agit de résumer ou vulgariser des textes dont la technicité implique une adaptation ou une simplification. À cette fin, et dans la mesure du possible, il faut soit proscrire certaines formules, soit les définir précisément. À titre d'exemple, voici une liste d'expressions qui ont été associées à l'usage des technologies de reconnaissance faciale, posturale ou comportementale :

- « vidéoprotection intelligente » ou « vidéo intelligente » au lieu de système de reconnaissance faciale, posturale ou comportementale ou plus généralement de systèmes de traitement algorithmique d'images.
- « caméras intelligentes » ou « augmentées » ou encore « caméras algorithmiques » pour des caméras couplées à des logiciels de reconnaissance faciale, posturale ou comportementale programmés avec des techniques d'intelligence artificielle. Autrement dit, il ne faut pas confondre le capteur avec les techniques de traitement des informations issues de ces capteurs.
- les « intelligences artificielles » ou « les IA » au lieu de systèmes programmés avec des techniques d'intelligence artificielle.
- *« Cette prétention incroyable que l'article 7 de la loi a de confier à une autorité non humaine la gestion de millions d'images captées dans l'espace public porte une atteinte inédite aux droits fondamentaux à la sûreté et à la dignité »*[a]. Le terme « autorité non humaine » est un non sens, car derrière tout système informatique il y a des personnes et des institutions qui doivent rester responsables des conséquences de leurs actes.
- *« si l'algorithme considère que certaines caractéristiques telles que le port d'un vêtement particulier ou une couleur de peau sont plus susceptibles d'être associées au risque recherché, (…) cela fait de l'utilisation de la vidéoprotection par algorithme une pratique potentiellement discriminatoire et raciste »*[b] ; rappelons que les algorithmes ne sont pas des personnes ; ils ne « considèrent pas » au sens propre du terme.

[a] *Recours au Conseil constitutionnel sur le projet de loi relatif aux Jeux olympiques et paralympiques de 2024 et portant diverses autres dispositions*, déposé par Madame Mathilde Panot le 17 avril 2023, p. 13
[b] ibid. p. 12

5.4 BIAIS ET DISCRIMINATIONS INJUSTIFIÉES

Les systèmes de reconnaissance faciale, posturale ou comportementale peuvent comporter des biais (cf. encadré 5) susceptibles d'engendrer des discriminations injustifiées (cf. encadré 6), ou bien des erreurs d'interprétation.

Il faut prévenir les biais afin d'anticiper les risques de discrimination qu'ils sont susceptibles d'induire. Cela passe par un examen de la répartition des données d'apprentissage, une analyse des sources possibles de biais et enfin par des tests. Il importe de renouveler ces études à intervalles réguliers afin d'éviter toute dérive. Soulignons, à cet égard, les très nombreux travaux scientifiques qui ont récemment porté sur ces problématiques[1].

[1] Luciano Floridi. *L'éthique de l'intelligence artificielle : principes, défis et opportunités* - Mimesis Philosophie, 2023

ENCADRÉ 5

LES BIAIS

Selon l'acception courante et dans le contexte de cet avis, un biais est une déformation, un travers ; plus spécifiquement, au sens technique, c'est *« 1. une distorsion, déformation systématique d'un échantillon statistique choisi par un procédé défectueux, ou d'une évaluation ou 2. la différence entre l'espérance mathématique d'un estimateur et la grandeur à estimer. »*[a] À cela, il faut ajouter que certains biais sont issus de considérations subjectives, par exemple la tendance consciente ou non à favoriser ou, au contraire, à défavoriser des catégories de personnes selon leur nom, leurs loisirs ou d'autres critères.
Si dans la littérature sur l'équité (*fairness*) algorithmique, le biais est souvent synonyme de discrimination, il convient de rappeler que tout biais n'entraîne pas nécessairement une discrimination et que toute discrimination n'est pas la conséquence d'un biais. En effet, la discrimination obéit à une définition juridique précise de sorte que seuls les biais conduisant à opérer des différences de traitement injustifiées selon les personnes doivent être considérés comme discriminatoires (voir encadré 6).
Les algorithmes étant conçus par des êtres humains, les biais susceptibles de conduire à des discriminations peuvent refléter des préjugés déjà présents dans la société. Si ces biais ne sont pas identifiés, ils risquent de systématiser les discriminations. Les biais peuvent se glisser dans les bases de données ainsi qu'à toutes les étapes de la spécification, de l'élaboration et du déploiement et de la maintenance de ces systèmes.

[a] https://www.larousse.fr/dictionnaires/francais/biais/9021

ENCADRÉ 6

LES DISCRIMINATIONS

Une discrimination, au sens A (sans idée de traitement inégal) du Trésor de la Langue Française[a], est le fait de différencier, en vue d'un traitement séparé, des éléments les uns des autres en les identifiant comme distincts. Au sens B (avec une idée de traitement inégal), la discrimination est entendue comme un traitement différencié appliqué à des personnes sur la base de critères injustifiés.
En droit français et européen, constitue une discrimination toute pratique, même neutre en apparence, susceptible d'entraîner un désavantage particulier pour des personnes par rapport à d'autres personnes, à moins que cette pratique ne soit objectivement justifiée par un but légitime et que les moyens pour réaliser ce but ne soient nécessaires et appropriés. La discrimination inclut tout agissement lié à l'un des motifs suivants : l'appartenance ou la non-appartenance, vraie ou supposée, à une ethnie ou une race, le sexe, la religion, les convictions, l'âge, le handicap, l'orientation sexuelle. Toute discrimination fondée sur l'un de ces motifs est interdite en matière de protection sociale, de santé, d'avantages sociaux, d'éducation, d'accès aux biens et services ou de fourniture de biens et services[b].

[a] http://atilf.atilf.fr/dendien/scripts/tlfiv5/visusel.exe?26;s=1905154725;r=2;nat=;sol=0;
[b] Loi n° 2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de la lutte contre les discriminations

RECOMMANDATION 5.4.1

(UTILISATEURS-EXPLOITANTS, SCIENTIFIQUES, DÉVELOPPEURS ET OPÉRATEURS)

La présence potentielle de biais nécessite d'utiliser les résultats du système de reconnaissance faciale, posturale ou comportementale avec précaution et discernement. Ces systèmes doivent, lors de leur installation, porter mention explicite de la présence potentielle de biais, en particulier à destination des opérateurs.

RECOMMANDATION 5.4.2

(SCIENTIFIQUES)

Promouvoir des recherches sur l'évaluation des dispositifs de reconnaissance faciale, posturale ou comportementale afin de qualifier, d'apprécier et de limiter autant que faire se peut les biais éventuels.

5.5 ASPECTS SCIENTIFIQUES ET ÉPISTÉMOLOGIQUES

Dès lors qu'il est envisagé de déployer un système de reconnaissance faciale, posturale ou comportementale, il convient de s'assurer, au moyen d'une démarche scientifique rigoureuse reposant sur des données objectives d'observation, que les protocoles et dispositifs expérimentaux mis en œuvre démontrent l'adéquation des technologies envisagées aux finalités.

La première phase consiste à identifier clairement, dans chaque cas, le ou les **objectifs poursuivis**, par exemple la protection d'intérêts légitimes – sécurité publique, santé publique, ordre public, protection des personnes et des biens, etc. Ensuite, on doit faire des hypothèses sur la contribution des dispositifs technologiques envisagés à la réalisation de ces objectifs et sur leur valeur ajoutée par rapport aux dispositifs qui existent déjà. Enfin, dans un troisième temps, on doit procéder à des **expérimentations** pour valider ou invalider, scientifiquement, ces hypothèses. Dans ce but, et dans ce seul but, de telles expérimentation sont légitimes. Pour qu'une expérimentation se justifie, il faut que ses finalités soient clairement posées et que le protocole en soit bien défini, voir en particulier l'encadré 7.

ENCADRÉ 7

EXPÉRIMENTATION SCIENTIFIQUE ET EXPÉRIMENTATION JURIDIQUE

Au plan scientifique, une expérimentation procède à des observations variées et répétées en modifiant, de manière contrôlée, certaines conditions initiales. Ces conditions peuvent porter sur la valeur de certains paramètres, ou sur la présence ou l'absence d'un facteur, par exemple d'un dispositif. Cela permet d'établir un lien entre les paramètres et le facteur et les observations. Par ce moyen, et à condition que les modifications de paramètres soient bien distribuées, une expérimentation permet de valider ou d'invalider des hypothèses portant sur des caractéristiques des observations.

La démarche expérimentale se retrouve également dans l'action publique et revêt alors une forte dimension juridique. En matière de politiques publiques, les autorités disposant d'un pouvoir législatif ou réglementaire, y compris les autorités administratives indépendantes et les collectivités territoriales[a], peuvent recourir à des « expérimentations », sous réserve de respecter un certain cadre juridique[b]. Ces expérimentations recouvrent des réalités variées car elles peuvent se déployer dans un cadre juridique existant ou nécessiter l'édiction d'une nouvelle règle, afin de déroger au droit en vigueur. Le Conseil d'État a d'ailleurs relevé que l'expérimentation juridique qui permet d'évaluer les modalités de mise en œuvre d'une réforme constitue un outil particulièrement approprié pour les mesures visant à « tester des nouveaux outils numériques » (comme l'intelligence artificielle et les logiciels de reconnaissance faciale en matière de police) « dès lors qu'ils nécessitent d'être développés de manière séquencée, en lien direct avec leurs utilisateurs, et font l'objet d'une évaluation régulière »[c]. À l'instar des expérimentations scientifiques, les expérimentations juridiques doivent répondre à certaines exigences méthodologiques. Le Conseil d'État a listé comme suit les principes essentiels : la définition précise des hypothèses et des objectifs, la fixation d'un délai pour dégager des résultats probants, la constitution éventuelle d'un échantillon, la collecte de données permettant des comparaisons, la détermination en amont de ses critères de succès et modalités d'évaluation[d]. Si le recours croissant, en France, à la méthode expérimentale dans la conception des politiques publiques traduit un certain progrès, tant dans les méthodes d'élaboration que d'évaluation de ces politiques, le Conseil d'État a souligné que les services chargés de concevoir et de conduire lesdites expérimentations ont souvent « une connaissance insuffisante de cette méthodologie »[e]. Cette carence est préjudiciable car elle peut fausser le débat public. Un autre écueil a pu être relevé : les autorités compétentes mettent parfois en place un dispositif expérimental, non pas pour s'assurer de la pertinence d'une réforme mais pour faciliter son acceptation « parce que le recours aux expérimentations rassurent ». Enfin, ainsi que l'a relevé le Conseil d'État, certaines réformes peuvent être adoptées en raison de la multiplication d'expériences sollicitées par des acteurs privés. L'expérimentation entendue dans un sens juridique revêt, par conséquent, une certaine complexité, car elle doit éviter le double écueil de l'instrumentalisation politique (dans le contexte, par exemple, d'une réforme impopulaire) et d'une rigueur épistémologique excessive. Dans ce dernier cas de figure, le Conseil d'État a affirmé que si les méthodes des sciences expérimentales peuvent, dans certains cas, être transposées pour l'expérimentation des politiques publiques, hisser la « rigueur scientifique en exigence juridique applicable à toute expérimentation en matière de politique publique conduirait à dissuader le recours à cette méthode dans un grand nombre de cas où elle s'avère précieuse et où elle peut être fructueuse à moindre coût ».

[a] La Constitution autorise ainsi le législateur à habiliter les collectivités territoriales à déroger, à titre expérimental, aux dispositions législatives et réglementaires en vigueur.
[b] Dans la mesure où les dispositions à caractère expérimental d'une loi ou d'un règlement dérogent au principe d'égalité, elles sont strictement encadrées.
[c] Étude du Conseil d'État, « Les expérimentations : comment innover dans la conduite des politiques publiques », adoptée le 4 juillet 2019. La documentation française.
[d] Ibid.
[e] Pour un exemple de « fausses expérimentations » qui ne sont pas accompagnées d'un minimum de méthode et d'un protocole expérimental, cf. CE, AG, 3 avril 2014, n°388486.

D'où les recommandations suivantes :

RECOMMANDATION 5.5.1

(TOUS)

Définir systématiquement un protocole qui précise les finalités (scientifiques, d'usage, test d'un nouveau modèle économique, etc.), les hypothèses, le détail de la mise en œuvre (matériel et méthode), les acteurs impliqués, le cadre (lieu et circonstances) ainsi que la durée, pour toute expérimentation d'un système de reconnaissance faciale, posturale ou comportementale.

RECOMMANDATION 5.5.2

(REPRÉSENTANTS INSTITUTIONNELS)

Mettre en place systématiquement un audit indépendant chargé de la validation et du suivi du protocole, qui devra faire l'objet de rapports périodiques ; ces rapports devront être mis à la disposition des parties prenantes qui en feraient la demande. Veiller, par ailleurs, à objectiver les conditions d'obtention des taux de réussite affichés par certains systèmes de reconnaissance faciale.

RECOMMANDATION 5.5.3

(SCIENTIFIQUES, UTILISATEURS-EXPLOITANTS, LEGISLATEURS)

Veiller à ne pas qualifier d'expérimentation le déploiement opérationnel d'un système de reconnaissance faciale, posturale ou comportementale si cela ne s'inscrit pas dans un contexte scientifique ou juridique clairement défini et justifié.

RECOMMANDATION 5.5.4

(SCIENTIFIQUES)

Encourager des recherches interdisciplinaires, alliant les sciences sociales, juridiques, l'informatique et l'ingénierie, sur la conception des protocoles d'expérimentation des systèmes de reconnaissance faciale, posturale ou comportementale, sur l'interprétation de leurs résultats ainsi que sur les procédures d'évaluation, de vérification, de validation et de certification.

Ces dernières années en France, plusieurs expérimentations de la reconnaissance faciale ont été conduites dans des espaces accessibles au public. En attestent les expérimentations menées par la Ville de Nice (lors du carnaval en février-mars 2019) et celles de la société Aéroports de Paris (retardées à cause de la crise sanitaire, ces expérimentations ont eu lieu entre mars et juillet 2021 et entre février et avril 2022). La CNIL ne s'y est pas opposée car les principes du RGPD étaient respectés. Aucune de ces expérimentations n'a cependant débouché sur une pérennisation de ces systèmes. Relevons encore que dans un rapport sénatorial publié le 12 mai 2022, les rapporteurs préconisent de privilégier, en matière de reconnaissance faciale, la voie expérimentale dans le cadre d'une loi. L'adoption d'une loi d'expérimentation permettrait de déterminer les usages pertinents de la reconnaissance biométrique. Selon les sénateurs, l'expérimentation pourrait être autorisée pour une période de trois ans, ce qui obligerait le Gouvernement et le Parlement à réévaluer le besoin et recadrer le dispositif en fonction des résultats obtenus. Le rapport préconise une évaluation publique et indépendante pour examiner l'efficacité de la technologie dans le cas d'usage envisagé. Celle-ci serait conduite par un comité composé de scientifiques et de spécialistes des questions éthiques dont les rapports seraient rendus publics.[2] Plus récemment, la Loi du 19 mai 2023 relative aux Jeux olympiques de 2024 a permis à titre expérimental et jusqu'au 31 mars 2025, le traitement des images collectées par des caméras fixes ou installées sur des aéronefs, dans les lieux accueillant les manifestations sportives.

ENCADRÉ 8

EXPÉRIMENTATION ET « BACS À SABLE RÉGLEMENTAIRES » : STIMULER L'INNOVATION

Les Principes sur l'intelligence artificielle de l'OCDE de 2019 préconisent aux États de recourir « à l'expérimentation, afin de fournir un environnement contrôlé dans lequel les systèmes d'IA peuvent être testés et mis à l'échelle ». De cette façon, les pouvoirs publics seraient en mesure de favoriser un cadre d'action qui soutienne une transition souple du stade de recherche et développement à celui de déploiement de systèmes d'IA dignes de confiance[a]. De plus, l'expérimentation permet de tester de nouvelles approches économiques, institutionnelles et technologiques, ainsi que des dispositions juridiques en dehors des structures réglementaires existantes. Les approches réglementaires expérimentales comprennent ainsi les centres d'innovation, les « bacs à sable réglementaires », la normalisation et la corégulation impliquant les régulateurs et les marchés[b]. Dans son rapport de 2023 sur les « bacs à sable réglementaires », l'OCDE affirme que ceux-ci sont prometteurs pour les domaines ayant des cycles d'innovation rapides, à l'instar de l'intelligence artificielle. Les « bacs à sable » qui réunissent les régulateurs et les entreprises permettent aux autorités de collaborer avec des entreprises pour tester des produits et services innovants, sans être contraints par le cadre juridique existant. Afin de stimuler l'innovation, les entreprises peuvent bénéficier d'une exemption de certaines dispositions légales ou de procédures de conformité, ce qui leur permet de bénéficier d'un soutien juridique sur mesure pour un projet spécifique (basé sur des essais et des erreurs). Ces « bacs à sable » sont soumis à certaines conditions car ils sont temporaires, avec un processus de test généralement limité à six mois. Enfin, soulignons que les informations et les données techniques et commerciales recueillies permettent aux autorités d'évaluer si le cadre juridique doit être adapté.

[a] OCDE, Recommandation du Conseil sur l'intelligence artificielle, OECD/LEGAL/0449
[b] Regulatory sandboxes in artificial intelligence, OECD digital economy papers July 2023 No. 356

[2] https://www.senat.fr/rap/r21-627/r21-6271.pdf

ENCADRÉ 9

TAUX DE RECONNAISSANCE

Les taux de réussite affichés pour certains systèmes de reconnaissance faciale doivent être pris avec circonspection. En effet, la signification de certains chiffres est souvent absente ou obscure. L'annonce d'un « pourcentage de reconnaissance » devrait être complétée par une description des conditions d'utilisation du dispositif et par une définition de la méthodologie d'évaluation. Qui plus est, on sait que la performance de la reconnaissance faciale, qu'elle soit humaine ou automatisée, dépend de la qualité de l'éclairage, de la résolution des capteurs et des images, du cadrage, etc.

5.6 CONDITIONS D'USAGE

Lors de la mise en œuvre d'un dispositif technologique quel qu'il soit, en particulier, lorsque ce dispositif recourt à la reconnaissance faciale, posturale et comportementale, ou plus généralement à l'exploitation de données biométriques, il importe de déterminer les conditions sous lesquelles son emploi se justifie. Les recommandations qui suivent visent à préciser les questions qu'il convient de se poser et qui portent sur le contexte social et politique dans lequel le système sera déployé.

RECOMMANDATION 5.6.1

(OPÉRATEURS, UTILISATEURS-EXPLOITANTS)

Veiller à ce que les conditions d'usage du système de reconnaissance faciale, posturale ou comportementale restent toujours strictement en adéquation avec ses finalités déclarées. Informer les personnes physiques concernées afin qu'elles puissent exercer un contrôle et être incitées, le cas échéant, à demander à ce qu'un contrôle soit effectué.

RECOMMANDATION 5.6.2

(REPRÉSENTANTS DE LA SOCIÉTÉ, UTILISATEURS-EXPLOITANTS, OPÉRATEURS)

Procéder à des évaluations régulières, par des organismes de certification indépendants, de l'utilisation effective des dispositifs de reconnaissance faciale, posturale ou comportementale et être en mesure de tirer parti des conclusions de ces évaluations.

RECOMMANDATION 5.6.3

(UTILISATEURS-EXPLOITANTS, OPÉRATEURS)

Veiller à la place de l'opérateur humain au sein des dispositifs de reconnaissance faciale, posturale ou comportementale, à la compétence qu'il doit avoir, aux rôles qu'il doit conserver ainsi qu'aux risques que tant son absence que sa présence induisent. De tels dispositifs doivent être envisagés dans le cadre d'une réflexion générale sur l'organisation sociale à l'intérieur de laquelle ils s'insèrent.

RECOMMANDATION 5.6.4

(OPÉRATEURS, UTILISATEURS-EXPLOITANTS, PERSONNES PHYSIQUES CONCERNÉES, REPRÉSENTANTS DE LA SOCIÉTÉ)

Les méthodes classiques, sans recours aux données biométriques, doivent rester accessibles à la fois aux opérateurs, en cas de défaillance par exemple, et aux personnes concernées, si elles le souhaitent. Ainsi doit-il en aller dans les aéroports ou pour les paiements, où l'on doit autoriser l'usage de méthodes alternatives, qui ne soient pas pénalisantes, en particulier au regard des durées des processus.

5.7 ASPECTS ÉCONOMIQUES ET ENVIRONNEMENTAUX

Les dispositifs intégrant de la reconnaissance faciale, posturale ou comportementale ont un coût important tant pour leur développement que pour leur maintenance et leur mise en œuvre. Beaucoup pensent qu'ils permettraient de diminuer les effectifs les personnes impliquées dans la surveillance. Or, on ne peut faire l'économie d'une supervision humaine des alertes lancées par ces dispositifs. Il apparaît donc nécessaire de mettre le coût de ces dispositifs en regard de celui d'autres moyens qui atteindraient les mêmes objectifs de façon tout aussi efficace. De plus, ce coût n'est pas uniquement financier. En effet, tant le déploiement des caméras que l'entraînement et l'exécution des algorithmes ont des incidences environnementales non négligeables. D'où les recommandations suivantes :

RECOMMANDATION 5.7.1

(UTILISATEURS-EXPLOITANTS, LÉGISLATEURS)

Évaluer l'ensemble des moyens nécessaires à la mise en œuvre de dispositifs incluant de la reconnaissance faciale, posturale ou comportementale. Ceux-ci incluent les dépenses initiales d'infrastructures matérielles et logicielles ainsi que les coûts induits par le personnel requis et la maintenance des installations.

RECOMMANDATION 5.7.2

(UTILISATEURS-EXPLOITANTS, SCIENTIFIQUES)

Mettre les coûts financiers et environnementaux des systèmes de reconnaissance faciale, posturale ou comportementale en regard de ceux de l'ensemble des autres solutions, afin de permettre de faire un choix rationnel fondé sur des considérations éthiques, financières et opérationnelles. Mener des études relatives à l'impact sur les métiers, les compétences, les conditions de travail, les relations sociales et l'environnement.

6. CONCLUSION

Nous souhaitons insister sur la légitimité des inquiétudes que beaucoup nourrissent à l'égard des technologies de reconnaissance faciale, posturale ou comportementale, en particulier lors de leur usage dans l'espace public où elles peuvent se révéler attentatoires aux libertés individuelles et collectives. Ces craintes ont conduit à des propositions de réglementations, voire de moratoires, à l'échelle nationale mais également européenne et internationale, émanant d'institutions étatiques ou supra-étatiques, comme le Parlement européen ou la Commission européenne, et de certains groupes industriels. Ainsi, dans sa résolution du 20 janvier 2021 sur l'intelligence artificielle le Parlement européen « invite la Commission à évaluer les conséquences d'un moratoire sur l'utilisation des systèmes de reconnaissance faciale ». De même, la Commission européenne, dans sa proposition de règlement du 21 avril 2021, propose dans son article 5 d'interdire, sauf dans certaines situations exceptionnelles, « l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives », ce qui recouvre, entre autres, les technologies de reconnaissance faciale, posturale ou comportementale. Signalons encore que la société IBM a annoncé, en juin 2020, qu'elle se retirait du secteur de la reconnaissance faciale en raison des inquiétudes suscitées par son utilisation à des fins de surveillance de masse et de profilage racial. Cependant, cette prise de position éthique semble avoir été assez rapidement contredite dans les faits[1].

Toutes ces propositions, hésitations et tergiversations attestent d'un malaise que beaucoup ressentent aujourd'hui vis-à-vis d'un emploi massif de ces technologies. Dans le même temps, des applications peuvent se révéler bénéfiques tant pour la collectivité que pour les individus ; on peut notamment citer la protection des personnes pour répondre aux besoins d'authentification, la justice afin d'aider à conduire des enquêtes, la culture qui expérimente l'oculométrie (le suivi du regard) dans les musées, ou encore le secteur de la santé. Les projets de régulation doivent donc faire la part entre l'utilité, les bénéfices et les risques des différentes applications. Cette recherche d'un équilibre rend problématique toute interdiction générale et tout moratoire sur les recherches relatives à la reconnaissance faciale, posturale ou comportementale, d'autant plus que ces recherches ne sont pas spécifiques et qu'elles sont utilisées dans d'autres domaines (reconnaissance d'objets, de scènes, etc.).

Il convient donc d'examiner avec attention, discernement et vigilance, l'ensemble des applications de la reconnaissance faciale, posturale et comportementale, ainsi que leurs effets, sachant que dans ce domaine comme dans bien d'autres, les arguments simplistes, d'où qu'ils viennent, sont néfastes et contre-productifs. Ceci doit conduire à adopter une démarche tout à la fois transparente et fondée sur des évaluations expérimentales rigoureuses des performances de ces technologies. Ces résultats doivent être mis en regard des besoins auxquels ces technologies sont censées répondre. Enfin, il est essentiel de suivre l'usage de ces technologies dans le temps, afin d'éviter des dérives délétères.

Soulignons que l'emploi généralisé des technologies dites de surveillance, dont la reconnaissance faciale, posturale ou comportementale est un volet, a une incidence sur les relations entre les personnes, sur les modes de vie et donc sur la condition humaine. Ces évolutions se produisent petit à petit, de façon insidieuse, « sans qu'on s'en rende vraiment compte ». Dans ce contexte, et même si la question du contrôle social est loin d'être neuve[2], il importe d'aider les citoyens à prendre conscience de ces évolutions afin qu'ils soient en mesure de décider démocratiquement de la société dans laquelle ils souhaitent vivre, en arbitrant entre le besoin de sécurité, le bénéfice des commodités procurées par ces technologies et les risques pour les libertés individuelles et collectives.

[1] Après avoir publiquement pris ses distances avec la reconnaissance faciale en 2020, IBM a signé un contrat de 64 millions d'euros avec le gouvernement britannique pour développer une plateforme biométrique nationale.

[2] Le souci du « qu'en dira-t-on » et les questions relatives à la présence policière, la carte bancaire et le passe Navigo sont anciens.

7. REMERCIEMENTS, AUDITIONS ET GROUPE DE TRAVAIL IMPLIQUÉ

7.1 REMERCIEMENTS

Nos remerciements vont en particulier aux personnes suivantes que nous avons auditionnées ou qui nous ont aidées dans la mise au point de cet avis.
Toute erreur ou inexactitude reste évidemment de notre pleine responsabilité.

7.2 PERSONNES AUDITIONNEES

- **Véronique Borre,**
directrice générale adjointe de la sécurité de la ville de Nice
- **Sébastien Louradour & Lofred Madzou**
World Economic Forum
- **Maryne Cotty-Eslous,**
directrice générale et fondatrice de Lucine
- **Xavier Fischer,**
directeur général de Datakalab
- **Emmanuel Bloch,**
directeur de l'information stratégique de Thalès
- **William Eldin,**
co-fondateur de XXII
- **Olivier de Mazières, Elisabeth Sellos-Cartel et Michel Cadic,**
ministère de l'Intérieur et des Outre-mer
- **Gaëtan Goldberg,**
chargé de mission numérique au sein du Défenseur des droits
- **Claire Nicodeme,**
SNCF
- **Xavier Chapuis et Fabrice Sabourin,**
RATP
- **Félix Tréguer et Arthur Messaud,**
La Quadrature du Net
- **Romain Galesne-Fontaine et Yann Haguet,**
IN Group
- **Tanguy Bertolus,**
PDG de Lyon Aéroport
- **Pascal Deborde,**
chef de projet à la DSI des Aéroports de Lyon
- **Natacha Liaboeuf,**
juriste au sein des Aéroports de Lyon

7.3 MEMBRES DU GROUPE DE TRAVAIL

- **Raja Chatila**
- **Laure Coulombel**
- **Laurence Devillers**
- **Karine Dognin-Sauze** – co-rapporteure
- **Jean-Gabriel Ganascia** – co-rapporteur
- **Claude Kirchner**
- **Catherine Tessier**
- **Célia Zolynski**

accompagnés de :

- **Mélanie Gornet** (stagiaire)
- **Anaëlle Martin** (rédactrice)
- **Alexia Pronesti** (rédactrice)
- **Amélie Turci** (rédactrice-stagiaire)

8. BIBLIOGRAPHIE

Castelvecchi, Davide.
"Is facial recognition too biased to be let loose?"
In: *Nature* 587.7834 (Nov. 2020), pp. 347–349.
doi: 10 . 1038 / d41586 - 020 - 03186 - 4.
url: https:// www. nature.com/articles/d41586-020-03186-4.

Castets-Renard, Céline.
"Caméras augmentées" : un danger pour les libertés lors des Jeux Olympiques et Paralympiques (et au-delà) ?"
In: *Recueil Dalloz 22* (2023), pp. 1138–1141.

Commission de l'éthique en science et en technologie.
"Les enjeux éthiques soulevés par la reconnaissance faciale"
In: *8e Commission Jeunesse* (2020), p. 46.

Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene.
Éthique de la recherche en apprentissage machine.
Tech. rep. CERNA, 2017.
http : / / cerna - ethics - allistene . org / digitalAssets / 53 / 53991 _ cerna _ _ _ thique_apprentissage.pdf.

Commission nationale de l'informatique et des libertés, CNIL.
Reconnaissance faciale : pour un débat à la hauteur des enjeux.
Tech. rep. 2019.
url: https://www.cnil.fr/sites/cnil/ files/atoms/files/ reconnaissance_faciale.pdf.

Défenseur des droits.
Technologies biométriques : l'impératif respect des droits fondamentaux.
Tech. rep. 2021.

EDRi and EIJI.
"A legal analysis of biometric mass surveillance practices in Germany, the Netherlands, and Poland".
In: *The rise and rise of biometric mass surveillance in the EU* (2021), p. 160.

Floridi, Luciano.
L'éthique de l'intelligence artificielle : principes, défis et opportunités.
Passage. Paris, France: Mimesis Philosophie, 2023.

Honneth, Axel.
La lutte pour la reconnaissance.
Passage. Paris, France: Editions du Cerf, 2000.
Kosinski, Michal.
"Facial recognition technology can expose political orientation from naturalistic facial images".
en. In: *Scientific Reports* 11.1 (Dec. 2021), p. 100.
doi: https://doi. org/ 10 . 1038 / s41598 - 020 - 79310 - 1.
url: http:// www. nature. com/ articles/s41598-020-79310-1.

Martinez-Martin, Nicole.
"What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?"
In: *AMA Journal of Ethics* 21.2 (Feb. 2019), E180–187.
issn: 2376-6980.
doi: 10.1001/amajethics.2019.180.
url: https://journalofethics. ama- assn. org/ article/ what- are- important- ethical- implications- using- facial-recognition-technology-health-care/2019-02

Moosavi-Dezfooli, Seyed-Mohsen et al.
"Universal Adversarial Perturbations".
In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (CVPR). July 2017.
Projet VOIE (Vidéoprotection Ouverte et IntégréE)

Ricœur, Paul.
Parcours de la reconnaissance.
Ed. by Stock. Les Essais. Paris, France, Jan. 2004.

Romdhane, Rim et al.
"Activity Recognition and Uncertain Knowledge in Video Scenes".
In: *IEEE International Conference on Advanced Video and Signal-Based Surveillance* (AVSS). Krakow, Poland, Aug. 2013.
url: https://hal.inria.fr/hal-01059602.
Secur ED. en-US. May 2020.
url: https://www.secur-ed.eu/ (visited on 01/07/2022).

The Lancet Digital Health.
"On the face of it"
In: *The Lancet Digital Health* 3.10 (Oct. 2021), e612.
issn: 25897500.
doi: 10.1016/S2589- 7500(21) 00217- X.
url: https://linkinghub.elsevier.com/retrieve/pii/ S258975002100217X (visited on 10/01/2021).

Wang, Yilun and Michal Kosinski.
"Deep neural networks are more accurate than humans at detecting sexual orientation from facial images"
In: *Journal of Personality and Social Psychology* 114.2 (Feb. 2018), pp. 246–257.
doi: 10.1037/pspa0000098.

INDEX ALPHABÉTIQUE

9. ANNEXES

9.1 CONSULTATION OUVERTE DU COMITÉ NATIONAL PILOTE D'ÉTHIQUE DU NUMÉRIQUE

9.1.1 OBJECTIF DU DOCUMENT

Le Comité national pilote d'éthique du numérique (CNPEN) a été créé en 2019 sous l'égide du CCNE pour les sciences de la vie et de la santé. Il s'est saisi sur des questions éthiques que soulèvent l'utilisation de technologies de reconnaissance automatique (reconnaissance faciale, posturale, comportementale).
Cette consultation ouverte a pour objectif de comprendre la perception qu'ont les personnes des technologies de reconnaissance automatique, au travers de leurs propres expériences au quotidien. Le but est d'engager un débat constructif sur les questions d'éthique soulevées par ces technologies et de promouvoir une technologie respectueuse du bien commun. Les réponses à cette consultation ouverte ont vocation à enrichir les réflexions du Comité et permettront d'affiner la perception des enjeux éthiques soulevés par les technologies de reconnaissance.

Cette consultation se divise en deux parties :

- La première partie aborde des questions qui ont trait à la perception et à l'expérience que vous avez des techniques de reconnaissance faciale. Cette partie comporte essentiellement des questions fermées qui débouchent parfois sur des questions conditionnelles plus ouvertes. Elle comprend aussi quelques questions ouvertes, généralement facultatives. Le temps nécessaire pour répondre à cette partie est de 15 à 30 minutes.
- La seconde partie est facultative. Les questions portent sur des enjeux plus techniques (erreurs des systèmes de reconnaissance automatique, conservation des données...) et appellent des réponses plus développées. Le temps nécessaire pour répondre aux questions de cette partie est d'environ de 10 à 15 minutes.

UTILISATION ET PROTECTION DE VOS DONNÉES PERSONNELLES

Nous ne demandons pas de nom ni de prénom, seules les adresses IP seront conservées pour un temps donné. Les données personnelles demandées (sexe, genre, âge, profession) ou celles que vous pourriez fournir de façon spontanée dans vos réponses à la consultation , ne seront traitées qui si elles sont utiles à l'analyse et à la réflexion du comité. Toutes les données récoltées seront stockées sur le serveur de Limesurvey en Allemagne, elles seront traitées de manière confidentielle uniquement par le personnel du CNPEN ou les membres du groupe de travail du CNPEN sur la reconnaissance faciale. Elles seront conservées au maximum dix-huit mois après la clôture de la consultation et jusqu'à douze mois après la publication de l'avis du comité.
Dans les conditions définies par la Loi Informatique et Libertés du 6 janvier 1978 et par le Règlement Européen sur la Protection des Données Personnelles entré en vigueur le 25 mai 2018, chaque contributeur bénéficie d'un droit d'accès aux données le concernant, de rectification, d'interrogation, de limitation, de portabilité et d'effacement. Chaque contributeur peut également, pour des motifs légitimes, s'opposer au traitement de ses données personnelles.
Le contributeur peut exercer l'ensemble des droits mentionnés ci-dessus en s'adressant au CNPEN à l'adresse:
consultation-reconnaissance@ccne.fr.

Mise en ligne de la consultation:
La consultation a été mise en ligne sur la plateforme LimeSurvey et est accessible via cette URL : **https://survey.ccne.fr/96563.**
Les contributions à cette consultation sont au nombre de 239.

9.1.2 INTRODUCTION

Que sont les systèmes de reconnaissance faciale, posturale, et/ou comportementale ?
La reconnaissance faciale consiste à identifier, authentifier ou catégoriser une personne à partir des traits de son visage, à l'aide d'un algorithme et de données de référence. La reconnaissance posturale consiste à s'intéresser à la démarche, à la position du corps, d'une personne. D'une manière plus générale, on parle de reconnaissance comportementale, qui consiste à identifier les comportements des personnes par exemple en s'intéressant à la dynamique des mouvements. Ces technologies fonctionnent avec de l'apprentissage machine (*machine learning*) qui est une branche de l'intelligence artificielle fondée sur l'utilisation de données massives. Nous déclinerons différents types d'usage au cours de cette consultation.

DE QUOI S'AGIT-IL ?

Il existe plusieurs types de reconnaissance, l'authentification, l'identification et la catégorisation, qui vont être mis en œuvre en fonction du type d'usage que l'on veut en faire.

- L'authentification permet de s'assurer qu'une personne correspond bien à ce qu'elle est censée être. En pratique, elle est utilisée pour confirmer l'identité d'une personne donnée à partir de son visage, par exemple en déterminant que le porteur d'un passeport est bien celui que mentionne le passeport ou que la personne qui déverrouille un téléphone est bien le propriétaire de l'appareil. Du point de vue logique, cela correspond à un processus d'appariement 1 avec 1.

- L'identification vise à repérer un individu dans un ensemble de personnes uniquement à partir de son visage ou de sa démarche, autrement dit à repérer 1 parmi n. Il est ainsi possible de repérer qui, parmi les individus figurant dans une base de données, se trouve sur une image ou une vidéo prise par un de vos amis sur Facebook ou par une caméra de surveillance, dans la rue.

- Enfin, la catégorisation classifie les individus selon un critère prédéterminé, par exemple leur genre, leur âge, leurs comportements, leurs émotions, etc. Certains travaux essayent même de caractériser les personnes selon l'orientation sexuelle, religieuse ou politique ou encore l'origine ethnique. Pour reprendre notre caractérisation logique, cela revient à repérer p individus parmi n. Notons que ces tentatives soulèvent des questions d'ordre épistémologique et éthique. En effet, rien ne prouve que l'orientation sexuelle, religieuse ou politique se traduise par des traits physionomiques et comportementaux

9.1.3 PRÉAMBULE

Vous répondez à cette consultation :

- ☐ En tant que représentant d'un collectif
- ☐ À titre individuel

Tranche d'âge :

- ☐ Inférieur à 25 ans
- ☐ Entre 25 et 45 ans
- ☐ Entre 45 et 65 ans
- ☐ Plus de 65 ans

Genre :

- ☐ Homme
- ☐ Femme
- ☐ Autre

Votre localisation :

- ☐ Grande ville
- ☐ Ville moyenne
- ☐ Petite ville
- ☐ Commune rurale

Formation:

- ☐ Scientifique
- ☐ Juridique
- ☐ Économique
- ☐ Littérature
- ☐ Sciences humaines et sociales
- ☐ Médicale
- ☐ Autre (précisez)

Catégorie professionnelle :

- ☐ Étudiant(e)
- ☐ Retraité(e)
- ☐ En activité professionnelle
- ☐ Sans activité professionnelle
- ☐ Autre

PREMIÈRE PARTIE DE LA CONSULTATION :

9.1.4 LES ENJEUX ÉTHIQUES DE L'AUTHENTIFICATION PAR RECONNAISSANCE AUTOMATIQUE

1. Utiliser un système de reconnaissance pour s'authentifier à des fins privées

a) Avez-vous déjà utilisé un système de reconnaissance faciale pour vous authentifier ?

- ■ Oui
- ■ Non
- ■ Ne sait pas

Si oui, dans quelles circonstances ?
QCM avec commentaires

- ■ Déverrouillage d'un appareil numérique (téléphone, tablette, ordinateur . . .)
- ■ Applications (bancaires, CAF...)
- ■ Autres

b) Si vous avez le choix entre déverrouiller votre appareil numérique (téléphone, tablette, ordinateur...) à l'aide de la reconnaissance faciale, à l'aide de reconnaissance d'empreinte digitale ou à l'aide d'un mot de passe, que choisissez-vous ? Pourquoi ? (Vous pouvez sélectionner une ou plusieurs réponses.) *QCM avec commentaires*

- ■ Reconnaissance faciale
- ■ Reconnaissance d'empreinte digitale
- ■ Mot de passe

c) Selon vous quels sont les bénéfices et les inconvénients de l'utilisation d'un système d'authentification fondé sur la reconnaissance faciale ?
d) Est-ce que votre rapport au déverrouillage par empreinte digitale a évolué depuis son apparition ? Si oui, pourquoi ?

- ■ Oui
- ■ Non
- ■ Cela dépend

2. Être l'objet de l'authentification. L'authentification est de plus en plus présente dans la sphère publique. Par exemple, pour passer le contrôle aux frontières, le logiciel de reconnaissance faciale PARAFE a été mis en place dans les aéroports français pour authentifier les passagers ; aux États-Unis ou en Chine, ces systèmes sont utilisés dans les écoles.

a) Avez-vous déjà été l'objet d'authentification par reconnaissance automatique ?

- ■ Oui
- ■ Non
- ■ Ne sait pas

Si oui, dans quelles circonstances ?

Les techniques de reconnaissance faciale pourraient être utilisées pour authentifier les élèves à l'entrée des établissements scolaires. Certains lycées français ont souhaité l'expérimenter afin de détecter les éventuels intrus. Cette technique viendrait en complément des dispositifs de badges d'ores et déjà existants : le lycéen devrait présenter son badge ou un pictogramme sur son téléphone qui serait scanné et une caméra comparerait le visage de l'élève avec celui qui est enregistré dans la base de données de l'établissement.

b) À l'heure actuelle ce type de contrôle est effectué par des badges ou par visuellement par une personne. Si un dispositif de reconnaissance faciale était mis en place, quels en seraient, selon vous, les bénéfices supplémentaires ? les inconvénients ?

9.1.5 LES ENJEUX ÉTHIQUES DE L'IDENTIFICATION

1. L'identification par reconnaissance faciale dans nos applications numériques (applications de divertissements, ...).

Nos smartphones ainsi que nos réseaux sociaux numériques utilisent les techniques d'identification qui, entre autres, permettent de reconnaître les personnes sur les photos.

a) Vous a-t-il déjà été proposé d'identifier par reconnaissance faciale des personnes dans l'album photo de votre smartphone ou bien sur l'un de vos réseaux sociaux numériques (Facebook, Instagram, etc.) ?
- Oui
- Non

Si oui, utilisez-vous cette fonctionnalité ?
- Oui
- Non
- Cela dépend

L'appréciez-vous ?
- Oui
- Non
- Cela dépend

Votre position a-t-elle évolué depuis l'apparition de cette fonctionnalité sur les réseaux sociaux numériques ? Si oui, dans quel sens ? Pourquoi ?
- Oui
- Non
- Cela dépend

b) Sur les réseaux sociaux numériques, il arrive que des personnes créent un compte en utilisant la photo d'une autre personne sans leur accord (par exemple, une personnalité publique). Afin d'assurer une meilleure protection de leurs utilisateurs contre les pratiques d'usurpation d'identité, certains réseaux sociaux numériques analysent donc les photos de profil des utilisateurs à l'aide de systèmes d'identification par reconnaissance faciale : lorsque le visage d'un individu est reconnu sur une photo associée à un autre profil, une alerte est envoyée à la personne concernée.
Comment voyez-vous ces techniques d'identification par reconnaissance faciale sur les réseaux sociaux numériques en matière de sécurité et de libertés ?

2. La sécurité par reconnaissance faciale

La question de l'identification par reconnaissance faciale est de plus en plus présente dans le débat public. La reconnaissance faciale peut se faire de manière rétrospective ou à la volée (autrement dit, en temps réel). Aujourd'hui, la reconnaissance faciale dite « à la volée » est interdite en France sauf dans des cas spécifiques, par exemple dans le cadre d'expérimentations. En France, une expérimentation de reconnaissance à la volée encadrée a été réalisée par la mairie de Nice lors de la 135e édition de son Carnaval en 2019. Cette expérimentation avait pour but de montrer le potentiel du dispositif en matière sécuritaire.

a) Savez-vous si vous avez déjà fait l'objet d'un système d'identification par reconnaissance faciale à la volée ?
- Oui
- Non
- Ne sait pas

b) Selon vous, est-il justifié d'utiliser cette technologie en matière de sécurité ?
- Oui
- Non
- Cela dépend

Si oui ou si cela dépend :
Aujourd'hui, l'expérimentation de la reconnaissance faciale à la volée est autorisée (cf. Mairie de Nice). Cependant la Commission européenne a récemment proposé que son utilisation dans les lieux publics soit prohibée sauf dans des cas bien spécifiques.

Dans quels cas est-ce justifié de prohiber /d'autoriser selon vous ?
Si non, pourquoi ?

Le post-traitement :

Les logiciels de reconnaissance faciale ne fonctionnent pas nécessairement à la volée mais sont réalisés à partir d'enregistrements vidéos. Ce type de systèmes peut par exemple aider à retrouver un suspect ou une personne disparue en analysant des enregistrements de vidéosurveillance[1].

c) Parmi les cas d'usage suivants utilisant ce type de dispositifs : lesquels vous paraissent justifiés ? Pourquoi ?
(Vous pouvez sélectionner une ou plusieurs réponses.)
- Retrouver un suspect dans une enquête de police
- Retrouver une personne disparue (enfant, personne malade, etc.)
- Reconnaître des manifestants qui ont participé à une manifestation illégale ou interdite
- Autre (précisez)

d) Parmi les cas d'usage suivants utilisant ce type de dispositifs : lesquels vous paraissent injustifiés ? Pourquoi ?
(Vous pouvez sélectionner une ou plusieurs réponses.)
- Retrouver un suspect dans une enquête de police
- Retrouver une personne disparue (enfant, personne malade etc.)
- Reconnaître des manifestants qui ont participé à une manifestation illégale ou interdite
- Autre (précisez)

e) Faut-il mentionner de façon explicite l'utilisation de reconnaissance faciale dans les lieux publics ? Précisez.
QCM avec commentaires
- Oui
- Non
- Cela dépend

f) Une augmentation croissante des expérimentations de reconnaissance automatique, pour vous : Précisez vos réponses
(Vous pouvez sélectionner une ou plusieurs réponses)
QCM avec commentaires
- Serait nécessaire à l'amélioration de ces technologies.
- Conduirait à la banalisation de ces technologies.
- Habituerait la population à ces technologies.
- Ne sait pas.

[1] https://www.assemblee-nationale.fr/dyn/opendata/AVISANR5L15B3404-tVII.html_Toc256000026

9.1.6 LES ENJEUX ÉTHIQUES DE LA CATÉGORISATION

1.Catégoriser dans le domaine commercial et professionnel

Dans le domaine du marché du travail, certaines applications sont utilisées par des entreprises américaines pour réaliser des entretiens d'embauche vidéos. L'application détecte les indices non-verbaux comme les expressions du visage, les mouvements des yeux, les mouvements du corps, les détails des vêtements et les nuances de la voix. Ces données sont ensuite traitées par l'algorithme qui attribue une note au candidat en fonction des attentes de l'employeur.

a) Approuvez-vous l'utilisation d'une telle application ? Pourquoi ? *Avec commentaires*
- Oui
- Non
- Cela dépend

Dans le domaine du marketing, la catégorisation peut permettre d'établir le profil des utilisateurs afin de leur proposer des services personnalisés.

b) Appréciez-vous recevoir ce type de publicités personnalisées ?
- Oui
- Non
- Cela dépend

Cas fictif : Vous voulez souscrire à un abonnement d'un site de diffusion de films en ligne , ce dernier propose deux types d'abonnements : l'un avec reconnaissance faciale automatique qui détecte vos émotions et vous propose des publicités ciblées, l'autre sans reconnaissance faciale.

c) Vous pouvez choisir d'utiliser le premier type d'abonnement et payer moitié prix ou bien choisir le second mais en payant l'abonnement plein tarif, lequel choisissez- vous ? Pourquoi ? *QCM avec commentaires*
- Celui avec reconnaissance faciale
- Celui sans reconnaissance faciale

2. Catégoriser pour le maintien de l'ordre public

Dans le domaine de l'ordre public, la reconnaissance automatique pourrait être utilisée pour détecter des comportements agressifs, pour l'appréhension de suspects mais également pour détecter l'abandon de détritus ou l'absence de ramassage des déjections canines.

a) Pensez-vous qu'il soit justifié d'utiliser la reconnaissance comportementale pour détecter des comportements particuliers dans les bouches de métro, dans les parkings, dans une foule, etc.? *Avec commentaires*
- Oui
- Non
- Cela dépend

b) La reconnaissance comportementale peut aussi être utilisée pour détecter des comportements agressifs lors d'événements publics de masse exposés au risque terroriste (Jeux olympiques, etc.). Comment voyez-vous ce cas d'usage en matière de sécurité et de libertés ?

3. Les techniques d'identification dans la gestion des flux : suivi de personnes dont l'identité est connue

La gestion des flux consiste en l'accès à un service grâce au suivi des personnes par reconnaissance faciale. Ces systèmes commencent à être utilisés dans les aéroports, à Tokyo par exemple, où votre visage devient votre passeport et carte d'embarquement. Dans certains pays, le paiement par reconnaissance faciale a été mis en place dans les supermarchés. Vous vous trouvez dans un supermarché qui pratique le paiement par reconnaissance faciale. Vous avez la possibilité d'aller dans la file avec reconnaissance faciale ou dans la file avec paiement traditionnel.

a) Il n'y a pas d'attente dans aucune des deux files. Laquelle choisissez-vous ? Expliquez votre choix.
- La file sans reconnaissance faciale
- La file avec reconnaissance faciale
- L'une ou l'autre

b) Il y a une longue file d'attente pour le système « traditionnel ». Laquelle choisissez- vous ? Expliquez votre choix.
- La file sans reconnaissance faciale
- La file avec reconnaissance faciale
- L'une ou l'autre

c) Pensez-vous qu'il soit nécessaire de maintenir un système traditionnel qui n'utiliserait pas de reconnaissance faciale ? *QCM avec commentaires*
- Oui
- Non
- Cela dépend

d) Approuvez-vous l'utilisation de ce type de dispositifs ? Précisez.
- Oui
- Non

4. Les techniques d'identification dans la gestion des flux : suivi des personnes dont l'identité est inconnue

Les technologies de reconnaissance faciale sont parfois utilisées pour suivre les personnes sans pour autant connaître leur identité. Dans les supermarchés, les lieux publics, les transports en commun, ces dispositifs peuvent aussi être utilisés pour améliorer la gestion des flux.

a) Avez-vous déjà fait l'expérience de ce type de dispositifs ?
- Oui
- Non
- Ne sait pas

Si oui, dans quelles circonstances ?

b) Approuvez-vous l'utilisation de ce type de dispositifs ? *Avec commentaires*
- Oui
- Non
- Cela dépend

3. Catégoriser dans le cadre éducatif.

a) Dans la ville de Hangzhou, en Chine, tous les comportements des élèves sont observés afin d'« optimiser l'enseignement ». Des caméras ont été installées dans les salles de classe afin de suivre les réactions des élèves, leur niveau de concentration mais également de reconnaître leur état émotionnel. Une alerte est envoyée au professeur lorsqu'un élève se comporte mal ou est déconcentré.

- Accepteriez-vous, en tant que parent, que vos enfants soient l'objet de reconnaissance faciale à l'école ?

Avec commentaires

- Oui
- Non
- Ne sait pas

- Accepteriez-vous, en tant qu'étudiant, que ce type d'application soit mise en place ?

Avec commentaires

- Oui
- Non
- Ne sait pas

- Accepteriez-vous, en tant que professeur, que ce type d'application soit mise en place ?

Avec commentaires

- Oui
- Non
- Ne sait pas

b) Quels sont les bénéfices et les inconvénients à utiliser la reconnaissance comportementale dans le cadre éducatif ?

c) Dans le cas de la surveillance des examens à distance, la caméra de l'ordinateur pouvait suivre le mouvement des yeux des étudiants pour éviter la fraude.

Comment envisagez-vous la surveillance à distance des examens par reconnaissance comportementale, en matière de valeur des examens et de libertés ?
Expliquez

4. Catégoriser dans le domaine de la santé

La catégorisation peut également être utilisée dans un contexte sanitaire, par exemple dans le cas de la crise sanitaire pour détecter des signes d'infection. Dans certaines zones (aéroports, entreprises...), les caméras thermiques associées à un système de reconnaissance faciale ont été utilisées afin de déterminer des signes d'infection au virus de la Covid-19 mais également pour contrôler le port du masque :

a) Trouvez-vous justifié l'utilisation de ce type de technologies pour détecter la température des personnes ? Pour détecter le port du masque ? Pourquoi ?

Avec commentaires

- Oui, pour l'état de santé des personnes et pour le port du masque
- Oui pour l'état de santé des personnes mais non pour le port du masque
- Non pour l'état de santé des personnes mais oui pour le port du masque
- Non pour les deux
- Ne sait pas

b) Certains systèmes sont capables grâce à la reconnaissance faciale, vocale et posturale, d'identifier, mesurer et analyser la douleur de l'utilisateur.

Dans quelles circonstances approuvez-vous l'utilisation de ce type de système dans le cadre de la détection de la douleur ? Pourquoi ?*
Avec commentaires*

- Pour les personnes capables de s'exprimer
- Pour les personnes incapables de s'exprimer
- Autre

5. Catégoriser selon les supposées origine ethnique, opinions politiques, religieuses, appartenance syndicale, orientation sexuelle

Certains chercheurs ont mis en avant qu'il serait possible, à l'aide de technologies de reconnaissance faciale, de déterminer des traits de personnalité mais aussi certaines orientations (politiques, sexuelles, religieuses...).

a) Pensez-vous qu'il soit acceptable et justifiable, pour autant que des technologies y parviendraient, de détecter au travers des techniques de reconnaissance les origines ethniques, les opinions politiques, philosophiques et religieuses, l'appartenance syndicale, l'orientation sexuelle d'une personne ? Pourquoi ?

- Oui
- Non
- Cela dépend

b) Comment réagiriez-vous si une association ou un parti politique utilisait ce type de technologies pour recruter ses membres ?

Dans le cas de l'application Gendnotes utilisée par la gendarmerie, des caractéristiques telles que les supposées orientations sexuelle, religieuse, politique, origines ethniques peuvent être collectées si elles sont considérées comme strictement nécessaires. Certaines associations craignent que des technologies de reconnaissance automatique soient ajoutées à ce dispositif.

c) Pensez-vous qu'il soit justifié d'utiliser la reconnaissance automatique afin d'établir le plus précisément possible le profil d'une personne recherchée dans une visée sécuritaire ?

Avec commentaires

- Oui
- Non
- Cela dépend

6. Catégoriser dans le cadre de manifestations publiques

Comment voyez-vous l'utilisation des techniques de reconnaissance faciale lors des manifestations publiques ?
Précisez.
Avec commentaires*

- À des fins de sécurité
- À des fins statistiques

9.1.7 CONCLUSION : CONFIANCE ET TECHNIQUES DE RECONNAISSANCE AUTOMATIQUE

Les techniques numériques de reconnaissance sont actuellement au cœur du débat public et un clivage important se dessine les concernant, notamment au sujet de la confiance à leur accorder.

1. Quelle est ou quelles sont, selon vous, la ou les technique(s) (authentification, identification et/ou catégorisation) qui soulèvent les questions éthiques les plus importantes ? Pourquoi ? (Vous pouvez choisir une ou plusieurs réponses.)
Avec commentaires
- Authentification
- Identification
- Catégorisation

2. La nature de l'opérateur a-t-elle une influence sur votre degré de confiance envers les technologies de reconnaissance faciale – en particulier, le traitement de vos données par des opérateurs de l'État suscite-t-il pour vous plus/moins/autant/ pas de craintes que le traitement de ces mêmes données par des opérateurs d'entreprises privées (par exemple, les GAFAM[2], les BATX[3])?
Justifiez votre choix.

- Pour détecter le port du masque dans la rue :
  - Plus de craintes envers leur traitement par des opérateurs de l'État
  - Plus de craintes envers leur traitement par des opérateurs d'entreprises privées
  - Autant de craintes dans les deux cas
  - Pas de craintes

- Pour identifier des personnes dans la rue à la volée (recherche de suspect, identification des trajectoires etc.) :
  - Plus de craintes envers leur traitement par des opérateurs de l'État
  - Plus de craintes envers leur traitement par des opérateurs d'entreprises privées
  - Autant de craintes dans les deux cas
  - Pas de craintes

- Pour identifier des personnes sur des images a posteriori (vidéos / photos) :
  - Plus de craintes envers leur traitement par des opérateurs de l'État
  - Plus de craintes envers leur traitement par des opérateurs d'entreprises privées
  - Autant de craintes dans les deux cas
  - Pas de craintes

- Pour s'authentifier sur une application :
  - Plus de craintes envers leur traitement par des opérateurs de l'État
  - Plus de craintes envers leur traitement par des opérateurs d'entreprises privées
  - Autant de craintes dans les deux cas
  - Pas de craintes

3. Votre réponse serait-elle différente s'il s'agissait d'autres technologies numériques ? Expliquez.

4. Utilisateurs : Avez-vous connaissance de supervision par des opérateurs humains d'applications de reconnaissance automatique ? Est-ce suffisant selon vous ? Expliquez.
- Oui j'ai connaissance de moyens de supervision humaine et je pense qu'ils sont suffisants
- Oui j'ai connaissance de moyens de supervision humaine et je pense qu'ils ne sont pas suffisants
- Non je n'ai pas connaissance de moyens de supervision humaine.

5. Opérateurs : Avez-vous mis en place une supervision par des opérateurs humains ? Est-ce suffisant ? Expliquez.
- Oui nous avons mis en place des moyens de supervision humaine et je pense qu'ils sont suffisants
- Oui nous avons mis en place des moyens de supervision humaine et je pense qu'ils ne sont pas suffisants
- Non nous n'avons pas mis en place des de moyens de supervision humaine mais je pense qu'ils sont nécessaires
- Non nous n'avons pas mis en place des de moyens de supervision humaine mais je pense qu'ils ne sont pas nécessaires

6. À quelles instances ou modalités démocratiques feriez-vous confiance pour contrôler le développement de ces nouvelles technologies de reconnaissance faciale ?

Merci d'avoir répondu à notre consultation. La partie qui suit est facultative, vous pouvez donc vous arrêter là ou poursuivre selon votre envie. Il s'agit d'une partie qui aborde des enjeux éthiques transversaux relatifs aux technologies de reconnaissance, notamment la question des erreurs dans les systèmes de reconnaissance et la conservation des données personnelles. Les questions qui y figurent peuvent être plus techniques et demandent parfois une rédaction plus longue que précédemment.

Souhaitez-vous continuer ?
- Oui
- Non

*Si oui, merci de poursuivre la deuxième partie de la consultation. *Si non, la consultation est terminée

[2] Google, Apple, Facebook, Amazon, Microsoft
[3] Baidu, Alibaba, Tencent, Xiaomi

9.1.8 LES ENJEUX ÉTHIQUES TRANSVERSAUX RELATIFS AUX TECHNOLOGIES DE RECONNAISSANCE AUTOMATIQUE

1. Erreurs et systèmes de reconnaissance

Le fonctionnement d'un algorithme de reconnaissance faciale peut ne pas être fiable, il peut comporter des biais statistiques, tout comme l'être humain[4], qui peut faire des erreurs cognitives. Par exemple, pour distinguer un loup d'un chien, le système de reconnaissance part de ce qu'on lui a appris[5], à savoir qu'il y a plus de loups que de chiens dans la neige. Ainsi, un chien sur fond blanc pourra être incorrectement reconnu comme un loup. Dans le cas de la reconnaissance faciale, un phénomène similaire peut se produire, notamment quand la base de données d'apprentissage n'est pas représentative de toute la population sur laquelle il va être utilisé.

a) Utilisateurs et consommateurs : Avez-vous déjà été témoin d'une erreur d'authentification par un système de reconnaissance faciale ?
- Oui
- Non

Pour les utilisateurs : si oui, dans quelles circonstances ?
Pour les opérateurs : quelles sont les erreurs les plus fréquentes ?
Pour les utilisateurs et les opérateurs : Selon vous, quelles peuvent être les conséquences si l'algorithme n'arrive pas à authentifier une personne ? si ces erreurs touchent certaines personnes de façon répétée ?

b) Dans le cas d'un système d'identification pouvant permettre aux forces de l'ordre d'appréhender des personnes recherchées, quelles sont les conséquences si l'algorithme se trompe ?
c) On se place maintenant dans le cas de la catégorisation par système de reconnaissance à l'embauche, quelles peuvent-être les conséquences si l'algorithme est défaillant ?
d) Opérateurs : Quels moyens mettez-vous ou pourriez-vous mettre en place pour limiter ces conséquences ?

Des algorithmes[6] ont été conçus dans le but de créer une perturbation unique et indiscernable pour chaque type de système de reconnaissance faciale. Cette perturbation a pour conséquence le changement de la classification des images avec une très haute probabilité. Par exemple, au lieu de reconnaître un micro-onde, un réfrigérateur, le système de reconnaissance d'images les classifiera comme oreiller. L'œil humain ne verra, quant à lui, aucun changement.
e) Opérateurs : À quoi êtes-vous / devez-vous être vigilants pour éviter ce type de problèmes ?

2. L'utilisation et la conservation des données

Les systèmes de reconnaissance utilisent les données personnelles des utilisateurs ou des personnes qui en sont l'objet, pour l'authentification. Selon le RGPD, la conservation des données à caractère personnel est limitée dans le temps, limitation décidée par le responsable du traitement en fonction des objectifs qu'il s'est fixés et dans la limite du cadre légal imposé. Dans le cas du smartphone, le traitement des données n'est pas soumis au RGPD sous réserve de plusieurs conditions. Au contraire, dans le cas d'une entreprise, par exemple, les données devront être conformes au RGPD et conservées selon une limite de temps fixée.

a) Opérateurs :Dans le cadre du déploiement de ces technologies, conservez-vous les données des utilisateurs ? Si oui, comment ?
b) Utilisateurs : Dans quel(s) cas d'usage des systèmes numériques de reconnaissance, l'utilisation et la conservation de vos données personnelles pourrait vous poser problème ? Pourquoi ?
c) Utilisateurs : La nature de l'opérateur (État, entreprise etc.) a-t-elle une influence sur votre réticence ou confiance dans l'utilisation et la conservation de vos données personnelles ?
Avec commentaires
- Oui
- Non
- Cela dépend

Si oui ou si cela dépend, au(x)quel(s) faites-vous le plus confiance et pourquoi ?

d) La localisation ou le contexte de conservation des données exercent-ils également une influence sur votre réticence ou confiance ?
- Oui
- Non
- Cela dépend

Si oui ou si cela dépend, envers le(s)quel(s) avez-vous le plus de réticence et pourquoi ?

e) Opérateurs : L'origine du logiciel a-t-elle une influence sur votre décision de déploiement ?
f) Opérateurs et utilisateurs : Selon vous, les dispositions mises en place en matière d'utilisation et conservation des données sont-elles adaptées ? Ce type de dispositions est-il suffisant, selon vous ? Expliquez. *Avec commentaires*
- Oui, les dispositions mises en place sont adaptées et elles sont suffisantes.
- Oui, les dispositions mises en place sont adaptées mais elles ne sont pas suffisantes.
- Non, les dispositions mises en place ne sont ni adaptées ni suffisantes.
- Ne sait pas

3. La question de la gouvernance de la reconnaissance faciale, posturale et comportementale

Au regard des questionnements éthiques soulevés par l'authentification, l'identification et la catégorisation par reconnaissance faciale, posturale et comportementale :
Êtes-vous favorable au libre usage de ces technologies ou à un usage contrôlé ? Justifiez.
QCM avec commentaires

- Tout le monde doit pouvoir utiliser ces technologies que ce soit pour un usage personnel ou pour un déploiement dans l'espace public.
- Il est nécessaire d'avoir une autorité de vigilance et de régulation sur les données (par exemple, confier cette mission à la CNIL, une association citoyenne etc.).
- Il faut mettre en place un principe d'homologation de ces technologies.
- Ces technologies doivent être restreintes à des applications très spécifiques.
- Ces technologies doivent être totalement interdites, quels qu'en soient les domaines d'application.
- Il faut un moratoire sur le recours aux technologies de reconnaissance faciale, comportementale et posturale dans l'espace public. (Précisez la manière dont pourrait être mis à profit ce moratoire.)
- Il faut un moratoire sur les expérimentations des technologies de reconnaissance faciale, comportementale et posturale dans les espaces publics et les lieux ouverts au public. Précisez la manière dont pourrait être mis à profit ce moratoire.

[4] Ici, il s'agit d'une image, les erreurs faites par l'être humain ne sont pas de la même nature.
[5] Dans cette introduction, nous utilisons le terme d'« apprentissage » ou le « système apprend », qui est un anthropomorphisme mais cela nous semble plus facile pour expliquer l'idée dont il est question ici.
[6] Seyed-Mohsen Moosavi-Dezfooli et al. "Universal Adversarial Perturbations". In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. July 2017.

9.2 SYNTHÈSE DES CONTRIBUTIONS À LA CONSULTATION

9.2.1 ORIENTATION GÉNÉRALE DES CONTRIBUTIONS

Dans un premier temps, nous avons relevé que la majorité des répondants n'utilise pas ou ne souhaite pas utiliser de technologies de reconnaissance faciale. Les avis mentionnent le caractère intrusif de ces dispositifs et les éventuelles dérives sécuritaires voire totalitaires qu'ils peuvent engendrer. D'autres arguments ont trait aux limites techniques des dispositifs : manque de fiabilité, failles de sécurité, défaillances, risques d'erreurs dans les résultats.
Parmi les répondants qui utilisent ou sont plus enclins à utiliser ce type d'artefacts technologiques, les critères majoritaires sont le caractère pratique, la facilité d'usage, la rapidité de ces technologies. Une tension apparaît concernant l'habituation à ces technologies, certains considèrent qu'il s'agit d'un risque tandis que d'autres trouvent que cela s'inscrit dans l'ordre des choses. Par exemple, certaines contributions mettent en avant le fait que l'utilisation de dispositifs de reconnaissance automatique à des fins statistiques conduirait à une banalisation de ces dispositifs. Dans un deuxième temps, nous pouvons observer une évolution des avis selon les études de cas :

- Les déploiements exceptionnels et de courte durée paraissent plus acceptables et légitimes;
- Certains usages semblent plus justifiés que d'autres : e.g. le suivi des personnes dans un aéroport par rapport au magasin. Les finalités y sont liées, dans un cas il s'agit de la sécurité au passage aux frontières et dans l'autre, il est question de rapidité de passage à la caisse;
- Les garanties mises en place exercent une influence sur l'acceptation de ces dispositifs : une alternative efficace et comparable, l'anonymisation des données, garantie d'efficacité du dispositif, importance du consentement sont autant d'éléments à prendre en compte.

D'autres déploiements apparaissent comme inacceptables. On peut citer, par exemple, la détection, au travers de techniques de reconnaissance automatique, des origines ethniques, les opinions politiques, philosophiques et religieuses, l'appartenance syndicale, l'orientation sexuelle d'une personne.
Dans un troisième temps, les contributions font état de plusieurs tensions :

- **Entre liberté et sécurité** : par exemple, pour l'authentification à l'entrée des établissements scolaires, les parents expliquent qu'ils seraient plus rassurés si de tels dispositifs étaient mis en place mais cela entraverait aussi la liberté de l'enfant, son émancipation. Les questions d'autonomie et d'intégrité font également état de cette tension. Certaines contributions considèrent que l'utilisation de la reconnaissance faciale peut être utilisée lorsque la sécurité de la ville ou du pays est en jeu, là où d'autres y voient une « hérésie démocratique ». Ces dispositifs doivent être accompagnés d'équipes d'interventions sinon ils n'ont pas d'utilité. Le cas de la manifestation souligne bien les tensions entre sécurité et liberté : sécurité des manifestants et des citoyens et liberté de manifester.
- **Sur le consentement libre et éclairé** : les contributions soulignent le fait que le consentement ne peut pas toujours être demandé. Les avis divergent sur la nécessité d'une note d'information. Les répondants considèrent qu'un individu mineur ne peut pas fournir de consentement libre et éclairé, notamment lorsque le dispositif est déployé à l'école ou à l'université (reconnaissance comportementale lors des examens à distance par exemple).
- **Sur la nature de l'opérateur** : celle-ci peut exercer une influence sur l'acceptation des utilisateurs. La majorité des répondants ont autant de craintes que ce soit l'État ou les entreprises privées mais la tendance penche plus vers une appréhension envers les entreprises privées. Cela se justifie par la commercialisation des données qui est faite par les entreprise. Quelques contributions mentionnent néanmoins des réticences, envers les déploiements numériques étatiques. Ces craintes se justifie par le pouvoir contraignant dont dispose l'État. Dans plusieurs contributions, la confiance envers l'État est présentée comme une chose qui « devrait être ».:

Plusieurs contributions questionnent la proportionnalité des déploiements technologiques au regard des finalités. Dans différents cas, l'utilisation de la reconnaissance automatique n'est pas considérée comme proportionnelle au regard des finalités. Cet aspect est présent dans les réponses sur l'utilisation de la reconnaissance comportementale pour surveiller les examens à distance. Plusieurs contributions, soulignent l'inutilité du dispositif et proposent plutôt de revoir les modalités d'évaluations. Il s'agit également d'éviter le « solutionnisme technologique ».
Les avis soulignent les modifications anthropologiques qu'entraînent ces solutions technologiques. Nombreux sont ceux qui s'inquiètent d'une déshumanisation des rapports sociaux (recrutement, rapport élève/professeur...). Les contributeurs soulignent l'impact de ces technologies quand leur cible est constituée de personnes mineures. Ces derniers concernent le bon développement de l'enfant, son autonomisation, sa créativité, sa sociabilité.
Pour plusieurs répondants, l'utilisation de ces technologies donnent l'impression de vivre dans une société où le risque est permanent, elles interrogent la teneur du danger « réel », la surenchère sécuritaire et le maintien de la population dans un climat de peur.
Les limites techniques des dispositifs sont fortement représentées dans les avis et viennent remettre en cause leur utilisation.
Certains usages sont majoritairement considérés comme inacceptables : la catégorisation selon les supposées origines ethniques, opinions politiques, religieuses, appartenances syndicales, orientations sexuelles. Cette technologie est qualifiée de « *deep-raciste* » dans un avis.
Finalement ces contributions mettent en avant la nécessité d'un encadrement, d'une contextualisation de ces technologies et de la mise en place de garanties et d'alternatives efficaces à ces dernières.

- **Les traitements qui soulèvent le plus de questions d'éthique**

Les contributions mettent en avant le lien entre les différents usages (authentification, identification et catégorisation) et donc que tous posent des questions éthiques, même si l'identification et la catégorisation semblent questionner davantage. Pour l'identification, les avis différencient identification avec consentement et sans ; explicite ou à l'insu, considérant qu'avec consentement l'utilisation est acceptable tandis que sans, cela devient de la surveillance. La catégorisation apparaît comme dangereuse, discriminatoire, les dérives apparaissent comme trop importantes. Une contribution souligne que les individus sont plus complexes que toutes les catégories imaginables ; deux autres désignent ce traitement comme le seul « qui pose vraiment problème ».

- **La supervision humaine**

Une partie des répondants n'a pas connaissance de moyens de supervision humaine même si parmi eux certains soulignent leur nécessité. Parmi ceux qui en ont connaissance, la majorité ne les trouve pas suffisants, certains mentionnent que les mécanismes purement informatifs ne le sont pas également. De manière générale, les avis mentionnent la nécessité de ces moyens de supervision humaine tout en soulignant que des efforts doivent être poursuivis dans ce sens. Un avis interroge : « La vraie question est: le superviseur est-il plus malin que la machine? » Du côté des opérateurs, la moitié considère que la supervision humaine est nécessaire ou en ont, au moins, mis en place tandis que la seconde moitié n'en a pas déployés et ne les trouve pas nécessaires. Une contribution sous-entend qu'il faudrait également, dans ce cas, superviser les superviseurs.

- **Les instances ou modalités démocratiques auxquelles les personnes font confiance pour le contrôle et développement des nouvelles technologies**

On retrouve dans les contributions : Des organismes élus, des autorités indépendantes, la CNIL – plusieurs contributions soulignent la nécessité de renforcer les pouvoirs de la CNIL – , les associations spécifiques, le Défenseur des Droits, ANSSI, les ONG, les comités d'éthique, les débats publics, l'État, le CNPEN, le Conseil Constitutionnel avec une formation obligatoire et un conseil citoyen avec des spécialistes.

- **Deuxième partie du questionnaire**

Parmi les erreurs de résultats soulevées par les contributeurs, – dans le cas de l'authentification par reconnaissance faciale – celle-ci ont lieu lors du déverrouillage des appareils électroniques personnels (smartphone, ordinateur...) ; dans le cadre de la recherche ; lorsqu'il s'agit de personnes de la même famille ; lors d'un changement d'apparence pour déverrouiller une application bancaire ; via Parafe. Les erreurs les plus fréquentes sont la non-détection et les biais cognitifs.

Les conséquences relevées par les contributeurs en cas d'erreur d'authentification répétée sur une personne sont parfois immédiates (le blocage de mobilité, le déni d'accès à des droits, des accusations infondées, la perte de temps) et parfois de long terme (l'impact sur la confiance des autres personnes envers cet individu, discrimination, stigmatisation, erreurs judiciaires, exclusion sociale, rejet envers l'utilisation des technologies). Dans le cas de l'identification pour appréhender des personnes recherchées, les conséquences éventuelles mentionnées sont : l'arrestation de la mauvaise personne (donc le « vrai coupable » en liberté), une perte de temps pour la police, des impacts physiques et psychologiques sur l'individu en question. Dans le cas de la catégorisation pour l'embauche, cela peut conduire à la remise en question du candidat (conséquences psychologiques), déshumanisation des rapports, discriminations, à des problèmes d'embauche pour l'entreprise et une perte d'emploi pour le candidat. Il s'agit d'une perte de temps et a un coût économique.

Pour limiter ces conséquences les opérateurs préconisent l'interdiction, la systématisation des procédures « humains dans la boucle » et la construction de modèles explicables. Certains contributeurs « opérateurs » expliquent que lorsqu'une perturbation est remarquée, ils la signalent, des tests peuvent être réalisés afin de déterminer ce qui provoque la perturbation. Ils expliquent que des vérifications périodiques sont nécessaires afin de voir s'il n'y a pas eu de modifications par un tiers et si l'algorithme est toujours effectif.

Une contribution explique que conserver les données des utilisateurs sur les serveurs cloud est moins risqué que sur un local, tandis qu'une autre explique les conserver dans une mémoire cache inexploitable. Un répondant avance que le RGPD ne peut pas tout le temps être respecté tandis que d'autres considèrent que les données ne doivent être conservées que si nécessaire, dans le cadre de la loi voire ne pas être conservées du tout. Elles peuvent aussi être conservées sur le smartphone sans renvoi aux opérateurs/constructeurs.

Pour les utilisateurs la finalité exerce une influence sur le degré d'acceptation de la conservation de leurs données et certains considèrent que celles-ci ne doivent jamais être conservées. Pour la moitié des contributions l'opérateur a une importance pour la confiance ou la réticence envers l'utilisation et la conservation des données ; on retrouve dans les commentaires l'ambivalence des relations à l'État. Pour l'autre moitié, l'opérateur n'exerce pas d'influence c'est surtout le type de données qui importent. La localisation est aussi prise en considération pour une majorité des contributeurs, ils ont plus confiance envers les pays européens soumis au RGPD et demandent une plus grande transparence. Dans ce contexte, les dispositions mises en place pour éviter les dérives ne sont pas suffisantes et pour certains, elles ne sont pas adaptées.

La majorité des contributions considèrent que tout le monde ne doit pas avoir le pouvoir d'utiliser ces technologies pour un usage privé ou public. Concernant les autorités de vigilance et de régulation, les avis sont mitigés : certains considèrent qu'elles sont nécessaires tandis que d'autres non. Ils sont également mitigés sur la restriction des technologies à certaines applications car ils considèrent qu'au vu de l'effervescence des technologies, les limiter seraient impossibles. La majorité des répondants trouvent que la mise en place d'un principe d'homologation n'est pas nécessaire ; que ces technologies ne devraient pas être interdites et qu'ils ne devraient ni y avoir de moratoires sur les technologies ni sur les expérimentations. Ces dernières peuvent permettre l'amélioration des technologies.

9.2.2 DES CONTRIBUTIONS QUI INVITENT À CLARIFIER CERTAINS ASPECTS (VOCABULAIRES, CHOIX, POSITION DU COMITÉ ...)

- **Précisions sur le sujet abordé par l'avis**

– Sur les droits du RGPD Un avis mentionne le fait que les individus dont on collecte les données devraient avoir le droit de retirer leurs données. Or, il existe des droits dans le RGPD comme le droit d'effacement des données, de déférencement du contenu, de gel de l'utilisation des données qui permettent cela.

– Les solutions alternatives Les avis montrent que, parfois, les personnes n'ont pas connaissance des solutions alternatives à la reconnaissance faciale dont ils disposent. Par exemple, l'utilisation de la reconnaissance faciale n'est pas obligatoire sur un téléphone, il est possible d'utiliser le mot de passe et l'empreinte digitale.

– Les aspects techniques

Le premier point concerne le manque d'efficacité des systèmes lorsque l'on porte le masque. Cette remarque revient souvent, alors qu'aujourd'hui les algorithmes de reconnaissance automatique ont été adaptés à la situation et cela ne constitue plus une limite de la technique.

Le deuxième point concerne l'empreinte digitale : dans le commentaire qui suit, le contributeur considère qu'elle ne constitue pas un moyen d'authentification :« L'empreinte digitale est une information d'identification, pas d'authentification (comme le visage), car elle est réputée publique (nous la laissons partout).Il s'agit toujours de la même erreur fondamentale ; je vous renvoie aux notions élémentaires de cryptographie à nouveau (à moins que cette confusion soit intentionnelle, sans relever de la simple ignorance). »

Une troisième question, qui émane des contributions, concerne le type de système dont il est question : s'agit-il de système adaptatifs ou automatiques ? « D'abord parce que le caractère "automatique" traduit mal les évolutions actuelles en Intelligence Artificielle. Il vaudrait mieux parler de systèmes adaptatifs. D'autre part parce que la technologie évoluant tellement vite qu'on ne peut pas prévoir aujourd'hui quels seront les systèmes d'identification de demain. Enfin parce s'il existe en effet des risques faces à nos

vies privées, d'une part cela a toujours été le cas des sociétés humaines à vouloir se contrôler et que d'autre part, il vaut mieux suivre la technologie afin d'en comprendre les usages possibles que de faire l'autruche. L'outil, s'il crée la fonction, ne préjuge pas de son usage. Un couteau sert à couper, que ce soit pour couper une pomme ou tuer son voisin. »
Un contributeur corrige une question qu'il considère mal posée : Comment voyez- vous ces techniques d'identification par reconnaissance faciale sur les réseaux sociaux numériques en matière de sécurité et de libertés ? « Je corrige: les réseaux sociaux utilisent la reconnaissance faciale pour de multiples usages. Le premier usage n'est probablement pas la détection de l'usurpation d'identité qui ne rapporte rien financièrement. En revanche, reconstituer le graphe social d'une personne de façon plus efficace (même des personnes non inscrites) sur ce réseau est probablement la vraie motivation de création de cette technologie par les géants du net.»
L'estimation la douleur est interrogée dans un avis qui met en avant que celle-ci est ressentie différemment selon les personnes. La résistance à la douleur dépend de plusieurs paramètres. La contribution souligne l'opportunité que constitue ce type de systèmes : ils peuvent donner de l'importance à la douleur ressentie par le patient. Ici, l'avis fait référence au journal Pediatrics qui présente une étude sur un logiciel de mesure de la douleur par reconnaissance faciale (FACS) en 2015, ainsi qu'au Dr Chantal Delafosse.
Finalement, un avis interroge l'utilisation de l'expression « capable de s'exprimer » : « (...) L'expression corporelle multimodale est dans la très grande majorité des cas possibles et rend la question partiale, de même que la réponse évidente : le système de reconnaissance biométrique est ici superflu. »

- **Demande de clarification sur la position du comité**

À plusieurs reprises les commentaires sont adressés au pronom « vous » pour demander si ou affirmer que cette consultation vient légitimer l'utilisation de ce type de technologies. Les tournures semblent parfois porter à confusion. En voici quelques exemples : « Vous usez de la commodité pour imposer un consentement arraché ! C'est toujours non ! ;) »
« Essayez-vous de légitimer la reconnaissance faciale avec des exemples complètement anecdotiques ? » « La formulation de la question me paraît fallacieuse car de nature à induire une réponse favorable à l'adoption de la reconnaissance faciale. » « Et c'est grave, vos réponses laissent supposer que vous cherchez à l'imposer, quel que soit l'avis des sondés ! » « Non. L'outil est disproportionné par rapport à son efficacité. Regardez déjà les rapports sur la vidéosurveillance... Le coût par rapport à l'efficacité. Votre proposition est indécente ! »

- **Sur le vocabulaire utilisé**

Plusieurs contributeurs s'interrogent sur le vocabulaire utilisé :
L'usage du terme sécurité peut déranger et porter à confusion au sens où ce ne sont pas les dispositifs qui permettent la sécurité mais les policiers ou personnels de sécurité associés à la reconnaissance automatique.
Plusieurs contributions s'interrogent sur l'usage du terme « particulier », sa définition, ce qu'il recouvre. Le terme « suspect » est lui aussi questionné et la contribution précise le fait que suspect ne signifie pas coupable.
Un avis souligne la confusion entre « technologie » au sens habituel du terme et algorithmes d'intelligence artificielle : « Parler de « technologie » déporte le problème sur l'outil au lieu de le focaliser sur une conception qui intègre des choix proprement humains. Même pour des outils assez simples, il faut faire la distinction par exemple entre un couteau de cuisine, un couteau de chasse ou un couteau de fusiller-marin. L'intention qui a prévalu à leur fabrication n'est, de toute évidence, pas la même. »

9.2.3 EXEMPLES DE POINTS D'ATTENTION RELEVÉS PAR LES PARTICIPANTS

DETTE ÉTHIQUE :

Une contribution met en avant la « dette éthique » que crée la banalisation de l'usage motivée économiquement.

MANQUE DE FLEXIBILITÉ DE LA TECHNOLOGIE :

Par exemple, l'authentification à l'école peut empêcher l'arrivée d'une personne en cas d'urgence.

ACCULTURATION DES PLUS JEUNES :

Certaines contributions mettent en avant le fait que la confrontation des enfants aux nouvelles technologies peut engendrer une automatisation du contrôle social, de la régulation sociale, de la perte des données et les atteintes aux libertés publiques et individuelles.

CONSENTEMENT PASSIF VS ACTIF :

Une contribution souligne que les empreintes digitales demandent un geste volontaire tandis que les technologies de reconnaissance faciale peuvent être utilisées à l'insu de l'individu.

AUGMENTATION DES INÉGALITÉS, BIAIS ET DISCRIMINATIONS :

Plusieurs contributions soulignent l'augmentation des inégalités que peuvent engendrer de tels systèmes, dus aux biais algorithmiques mais également par les finalités. Si on prend l'exemple de la reconnaissance comportementale à l'école, cela peut engendrer des inégalités chez les enfants atteints de troubles autistiques ou d'hyperactivité.

LA CRÉATION DE PROFILS FANTÔMES :

L'utilisation de technologies de reconnaissance faciale peut conduire à la création de profils fantômes, de personnes qui n'utilisent pas les réseaux socionumériques.

LES UTILISATIONS QUI POURRAIENT ÊTRE ACCEPTABLES POUR CERTAINS CONTRIBUTEURS :

Certaines contributions soulignent que les technologies de catégorisation de la douleur peuvent être utiles dans différents cas : pour les psychiatres et les aides-soignants dans les EHPAD, dans les transports publics (pour les malaises).

CNPEN 2 avril 2021

Comité National Pilote d'Éthique du Numérique

Autosaisine

Reconnaissance faciale, posturale et comportementale : entre questionnements et enjeux d'éthique

Tirant partie du perfectionnement des logiciels, de la collecte de grandes masses données et de leur exploitation, l'intelligence artificielle conduit à des techniques et des applications inédites qui ouvrent de nouveaux questionnements éthiques.

Parmi celles-ci, la reconnaissance faciale, qui analyse les traits du visage d'un individu avec la prétention de l'identifier, de déterminer ses émotions ou de révéler son origine ethnique, voire son orientation sexuelle ou politique, et la reconnaissance posturale qui repère les traits discriminant de la démarche et, plus généralement, du comportement, se sont répandues si vite qu'on n'a pris ni le temps, ni la peine d'aborder les questionnements éthiques et épistémologiques qu'elles suscitent.

Ces nouvelles possibilités technologiques associées à une forte pression sociale venant d'un sentiment croissant d'insécurité pourraient aisément conduire à une tentation solutionniste. Il en résulterait une surveillance incessante pour l'ensemble de la population. Tant les motivations politiques que les conséquences pour les libertés publiques demandent à être examinées avec soin.

Au-delà du modèle de société vers lequel ces choix ou ces non-choix pourraient conduire, il conviendra d'aborder la question du consentement et du débat avec les citoyens, les acteurs de la société civile et des sphères législative, économique et politique.

Nous pouvons faire le constat ces dernières années de l'émergence de nombreux usages faisant appel à ces technologies de reconnaissance faciale, posturale et comportementale sans certitude absolue que la qualité algorithmique n'induise pas de biais discriminants. Le contexte sécuritaire et sanitaire actuel est également particulièrement incitatif. Et de nombreux démonstrateurs vont prochainement être déployés dans le cadre de grands événements en France et à l'étranger.

Certains se réjouissent de voir des applications améliorer les interfaces humains-machines, faciliter l'accès aux bases de données multimédias ou encore assurer la sécurité sanitaire (par exemple, en repérant les personnes qui ne portent pas de masques). D'autres s'inquiètent d'applications susceptibles de porter atteinte aux libertés civiles et à l'anonymat. D'autres encore vont jusqu'à demander un moratoire.

Cette saisine s'intéressera plus spécifiquement aux implications éthiques de ces technologies.

Pour conduire l'analyse, et distinguer les différents usages, on distinguera trois scénarios :

1. L'**authentification**
2. L'**identification**
3. La **catégorisation**.

L'authentification, à savoir la confrontation des données biométriques enregistrées avec celles que présente un individu tend à se généraliser avec les possibilités de l'IA et n'est pas sans rappeler des pratiques anciennes comme le relevé d'empreintes digitales. La logique sous-jacente est le *1 pour 1*. L'authentification existe depuis longtemps dans les aéroports, avec par exemple le système Paraphe pour passer la douane, le selfie check pour des opérations de paiement automatique, le

déblocage de son téléphone ou de comptes informatiques. Cela repose généralement sur le croisement de plusieurs indices généralement avec le consentement de la personne.

L'identification qui consiste à repérer un individu dans une foule pourrait du fait de la démultiplication des systèmes de surveillance conduire à une société contrôlée à son insu. Dans ce cas, la logique correspond au *1 parmi n.* L'identification n'induit pas nécessairement d'avoir obtenu un consentement préalable. De nombreuses questions d'ordre éthique mais aussi juridiques portent sur les conditions d'utilisation potentielle pour reconnaître les personnes et leurs intentions dans les vidéos de surveillance de parkings ou d'aéroports. Peut-on utiliser cela n'importe où, au risque de tracer les déplacements et les contacts de chacun d'entre nous ? Ou, au contraire, doit-on le proscrire définitivement, en s'interdisant nombre d'applications utiles, par exemple pour faire des enquêtes sur requête de juges ?

La catégorisation qui vise à classifier les individus et leur comportement à partir de leur visage ou de leur posture présente un risque de discrimination des individus à partir de leur apparence, leur orientation sexuelle ou politique, voire en raison leur origine ethnique. La logique relève alors d'une répartition en classes, à savoir du *p parmi n*. La catégorisation fait la corrélation entre, d'un côté, les traits de leur visage ou leurs caractéristiques posturales, et d'un autre, leurs émotions, leurs activités, leur caractère, leur origine ethnique ou leur sincérité dans des situations aussi particulière que la détection de mensonges. Nous retrouvons là probablement de très anciennes conceptions physiognomonistes que l'on voit se réactiver à l'époque contemporaine. Outre des questions d'ordre épistémologique sur la solidité des expériences conduites en ces matières, il conviendra de se demander jusqu'où de telles applications sont acceptables et quelles sont leurs effets sur la société, sur le rapport État-Citoyen, etc.

Pour chaque scénario d'applications génériques, le Comité cherchera à formuler et à analyser les limites, et les conditions des usages possibles ou constatés pour préserver la dignité de la personne, le sens de la justice et de ce qui est éthiquement acceptable pour notre société au regard de ses valeurs.

Outre les scénarios d'applications génériques et leurs usages, nous nous intéresserons aux données, et en particulier aux données biométriques utilisées en entrée des systèmes de catégorisation, tant pour l'apprentissage algorithmique que pour la reconnaissance, mais aussi à la collecte, à l'accessibilité et à la circulation de ces données.

Nous nous interrogerons sur le rôle et la légitimité des différentes partie-prenantes qui interviennent aujourd'hui dans la conception de ces technologies de reconnaissances faciales, posturales et comportementales mais aussi leur diffusion et massification. Entre l'Etat, les collectivités, les entreprises et les citoyens quels sont les garde-fous à prévoir pour assurer des conditions d'usage éthiquement acceptables ?

Enfin, nous étendrons nos investigations aux enjeux culturels, géopolitiques et de souveraineté liés à la maîtrise et l'usage de ces technologies.

Le comité vise à rendre son avis pour la fin de l'année 2021.

Rapporteurs : Karine Dognin-Sauze & Jean-Gabriel Ganascia.

Le Comité national pilote d'éthique du numérique (CNPEN) a été créé en décembre 2019 à l'initiative du Premier ministre et placé sous l'égide du Comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE). Il est constitué de personnalités du monde académique, industriel et institutionnel. Experts du numérique, de la technologie, du droit, de l'économie, de la philosophie, du langage, de la logique, de la médecine, tous concourent à une réflexion éthique rendue indispensable par le développement du numérique et participent ainsi à éclairer le débat public. Des avis précédents du CNPEN concernent par exemple l'éthique des véhicules « autonomes » (mai 2021), des agents conversationnels (septembre 2021) ou encore, conjointement avec le CCNE, les enjeux d'éthique de l'utilisation de l'intelligence artificielle dans le champ du diagnostic médical (novembre 2022) et des plateformes de données de santé (février 2023). Plus récemment, il a abordé les enjeux d'éthique de la rétroactivité du changement de nom dans les documents scientifiques numériques (juin 2023) et ceux des systèmes d'IA générative (juin 2023).

LES MEMBRES DU COMITÉ NATIONAL PILOTE D'ÉTHIQUE DU NUMÉRIQUE

Gilles Adda
Raja Chatila
Theodore Christakis
Laure Coulombel
Jean-François Delfraissy
Laurence Devillers
Karine Dognin-Sauze
Gilles Dowek
Valeria Faure-Muntian
Christine Froidevaux
Jean-Gabriel Ganascia
Eric Germain
Alexei Grinbaum
David Gruson
Emmanuel Hirsch
Jeany Jean-Baptiste
Claude Kirchner - directeur
Augustin Landier
Gwendal Le Grand
Claire Levallois-Barth
Caroline Martin
Tristan Nitot
Jérôme Perrin
Catherine Tessier
Serena Villata
Célia Zolynski