WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

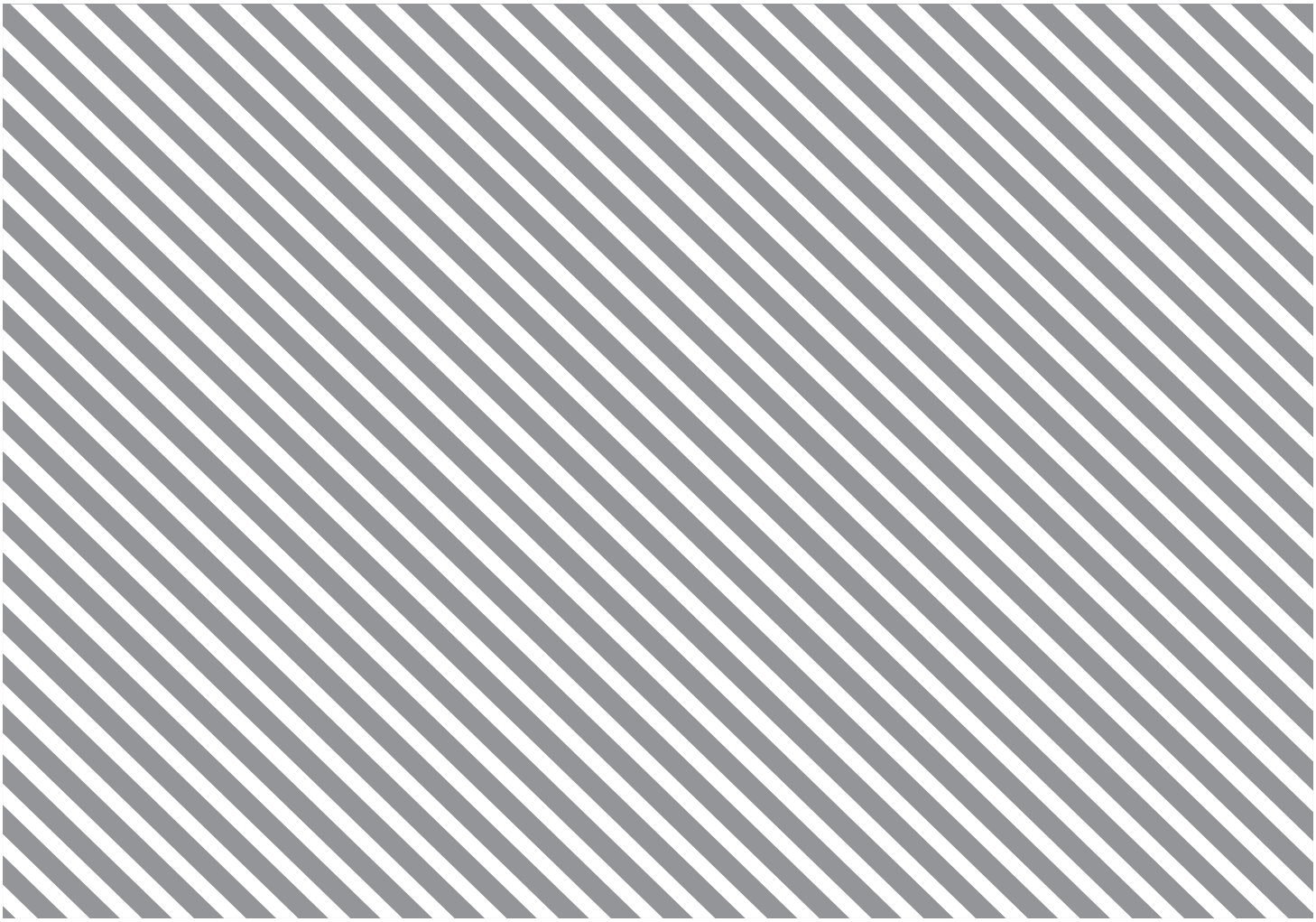
Livre Blanc

Cadre d'action pour un usage responsable de la reconnaissance faciale

Cas d'usage : gestion des flux

Projet pilote

Février 2020



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Table des matières

Introduction

Au cours des dix dernières années, la reconnaissance faciale s'est imposée comme une des plus puissantes technologies biométriques d'identification et de contrôle de l'identité des personnes. Cette technologie permet, à partir d'une image numérique ou d'un support vidéo présentant un visage, de comparer et d'analyser ses caractéristiques en fonction des lignes faciales. L'évolution des systèmes de reconnaissance faciale, qui s'explique principalement par les progrès de l'apprentissage machine et de la technologie des capteurs, devrait stimuler le marché de ces technologies et le porter à hauteur de 7 milliards $ d'ici 2024, à comparer aux 3,2 milliards $ dégagés en 2019[1]. En effet, alors que les systèmes de reconnaissance faciale les plus performants atteignaient un score honorable de 72% de précision en 2010, ils dépassent désormais les 95%[2].

Les technologies de reconnaissance faciale sont désormais utilisées dans de nombreux domaines, de l'amélioration de la satisfaction client dans les secteurs des services bancaires et de la vente au détail à l'accélération des procédures de contrôle aux frontières dans les aéroports.

Le développement de ces technologies promet de nombreuses opportunités d'utilisations bénéfiques d'un point de vue social, il représente également une menace sérieuse pour les droits humains et les libertés individuelles, notamment la liberté d'expression, la liberté de réunion et d'association ainsi que pour le droit au respect de la vie privée. Comme le souligne l'Union américaine pour les libertés civiles (American Civil Liberties Union - ACLU), la principale inquiétude réside dans la perspective de voir des technologies qui « collectent et conservent des informations uniquement en cas de nécessité absolue se transformer en technologies de surveillance active des personnes, souvent en temps réel[3] ».

Avec l'apparition de différentes polémiques, ces derniers mois ont vu un accroissement des inquiétudes de l'opinion publique et des organisations de défense des droits humains, à propos des technologies de reconnaissance faciale. Certains commerçants utilisent ces technologies sans information ni consentement du public[4], un nombre grandissant d'établissements scolaires les déploient afin de surveiller les élèves[5], il est régulièrement fait état d'atteintes à l'intégrité des données biométriques[6] et d'utilisation des données personnelles en vue de développer des systèmes de reconnaissance faciale sans en informer les utilisateurs[7].

Bien que de considérables progrès ont été observés ces dernières années, plusieurs études ont démontré[8] que la reconnaissance faciale peut produire des résultats différents en fonction des individus. Selon une étude récente [9], la précision de ces systèmes varie en fonction de la couleur de peau, ce qui risque de donner lieu à des erreurs d'identification des personnes. En outre, en fonction du système utilisé, le genre, l'âge, la taille et le port de lunettes ou d'un foulard peuvent également en affecter la précision et le fonctionnement.

Lors de l'utilisation de ces systèmes en temps réel dans le cadre d'opérations de maintien de l'ordre, ces écarts de performance pourraient augmenter les risques d'erreurs d'identification et créer d'importants problèmes de sécurité. Face à ce contexte, il paraît indispensable d'agir, et cela passe notamment par élaboration d'un cadre de gouvernance qui garantisse une utilisation responsable des technologies de reconnaissance faciale.

À cette fin, le Forum Économique Mondial mène un projet pilote multipartite basé en France et se concentrant sur le cas d'usage spécifique de la gestion des flux. Cette initiative a donc pour objectif d'établir un cadre de gouvernance de la reconnaissance faciale qui a été testé sur le terrain. Tout l'enjeu étant de multiplier les expérimentations similaires autour d'autres cas d'usage, en France ou à l'étranger (en tenant compte des réglementations locales, des normes sociales et autres facteurs propres au lieu d'application) afin de continuellement renforcer ce cadre d'action.

Aussi, ce cadre d'action a vocation à informer le débat public sur l'utilisation des technologies de reconnaissance faciale à l'échelle nationale, européenne et internationale. Dans la mesure où il s'agit d'un sujet qui porte sur des questions relatives aux droits et libertés individuelles et collectives, les citoyens et leurs représentants démocratiques sont les seuls décisionnaires légitimes en ce qui concerne les usages et les conditions d'utilisation qu'ils souhaitent promouvoir ou proscrire. Nous avons pour ambition de les aider à appréhender les différents arbitrages auxquels ils seront confrontés. Ce livre blanc étant la première étape d'un processus itératif, nous invitons les organisations désireuses de prendre part à ce débat à se joindre au projet.

Un cadre d'action pour assurer un usage responsable de la reconnaissance faciale

1. Méthodologie

Afin de bâtir un cadre d'action équilibré à même de garantir un usage responsable de la reconnaissance faciale, l'équipe Intelligence Artificielle et Apprentissage Machine du Centre pour la Quatrième Révolution Industrielle du Forum Économique Mondial, a mené une consultation multipartite et a développé une approche expérimentale structurée en 4 étapes qui consiste à :

- **Définir** ce qui constitue un usage responsable de la reconnaissance facial à travers la corédaction de principes d'action. La première mission de notre groupe de travail, composé de responsables politiques, d'entreprises chargées de concevoir et de fournir les systèmes de reconnaissance faciale, d'organismes de réglementation, de chercheurs et de représentants de la société civile, fut d'établir une définition commune, déclinée autour de 11 principes d'action.

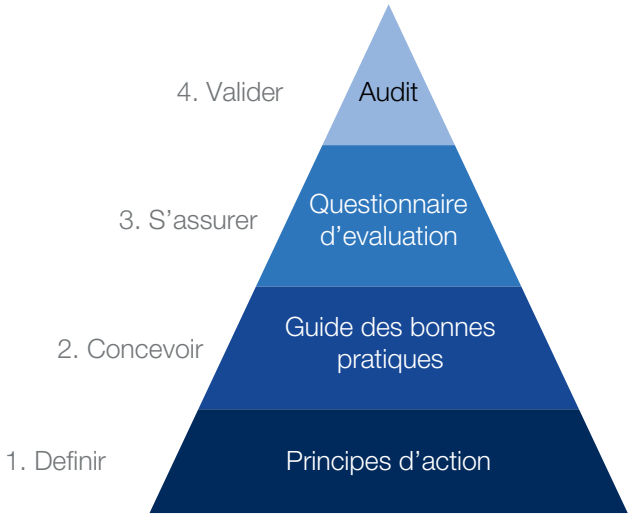
- **Concevoir** un ensemble de bonnes pratiques permettant la création d'un système « Responsable par design », cas d'usage par cas d'usage, afin d'accompagner les équipes produit dans le développement de leurs systèmes.

- **S'assurer** du caractère responsable des systèmes développés à travers un questionnaire d'évaluation décrivant pour chaque cas d'usage les règles devant être respectées afin de répondre aux attentes des principes d'action.

- **Valider** le respect des principes d'action à travers la conception d'un référentiel d'audit par un tiers de confiance

Cette méthode, qui a vocation à être déployée cas d'usage par cas d'usage, nous apparaît essentielle dans la mesure où les risques liés à l'utilisation des technologies de reconnaissance faciale, varient considérablement en fonction des contextes d'utilisation.

4 étapes pour assurer un usage responsable de la reconnaissance faciale



Groupe de travail

Pour atteindre cet objectif, un groupe de travail a été réuni pour collaborer autour d'un projet pilote, mené en France, et visant à concevoir conjointement ce cadre d'action.

Les membres de ce groupe de travail ont joué deux rôles complémentaires :

- **Un rôle de contributeur :** représentants des organisations qui envisagent de se procurer des systèmes de reconnaissance faciale (Groupe ADP, SNCF), des fournisseurs de technologies (Amazon Web Services, IDEMIA, IN Groupe et Microsoft), des responsables politiques (membres du parlement français, OPECST), des universitaires, des organisations de la société civile et AFNOR Certification.

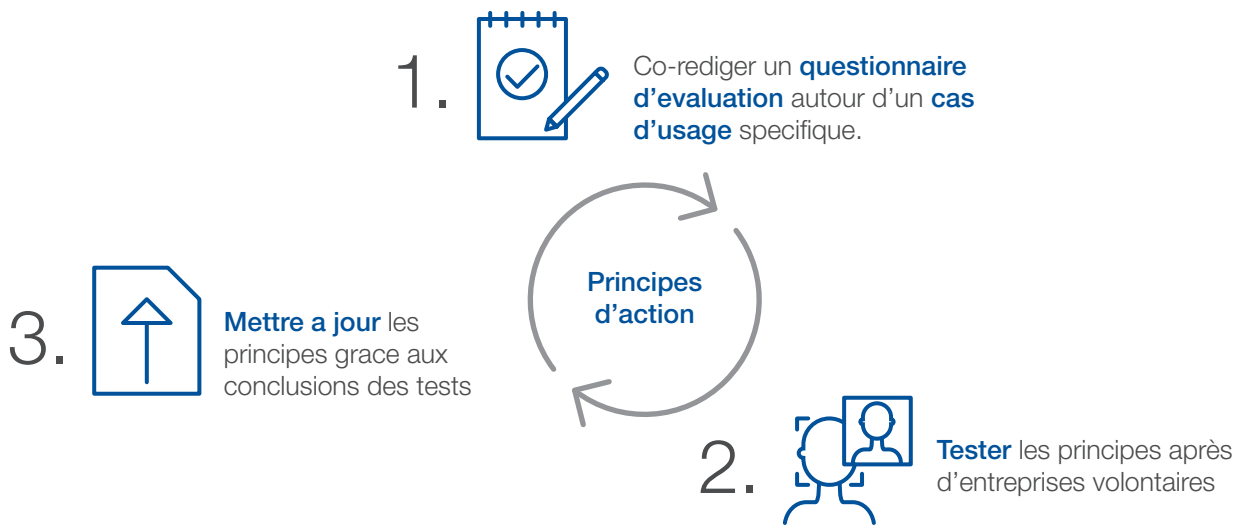
- **Un rôle d'observateur :** Commission Nationale de l'informatique et des libertés et Conseil National du Numérique.

Programme

Le projet pilote a vocation à être mené sur une période de 18 mois, et suit le calendrier suivant :

- Définition du champ d'application (avril à septembre 2019) : identifier les cas d'usage potentiels des technologies de reconnaissance faciale et les parties prenantes concernées.
- Conception (octobre 2019 à janvier 2020) : développer un cadre d'action qui inclut un ensemble de principes d'action, un guide des bonnes pratiques, un questionnaire d'évaluation et un référentiel d'audit :
  - **Principes d'action :** définir les composantes d'un usage responsable des technologies de reconnaissance faciale.
  - **Guide des bonnes pratiques :** permet d'apporter aux fournisseurs et/ou utilisateurs de la technologie un guide permettant de construire de son développement à son déploiement des solutions de reconnaissance faciale responsables
  - **Questionnaire d'évaluation :** appliquer ces principes à la situation d'utilisation sélectionnée et permettre ainsi aux organisations d'évaluer leurs processus d'atténuation des risques.
  - **Référentiel d'audit :** afin de veiller à ce que les organisations respectent bien les principes d'action. Ces travaux sont confiés à AFNOR Certification. En premier lieu, le référentiel d'audit doit reposer sur une revue du questionnaire d'évaluation. Son examen sur le terrain permettra de garantir que le questionnaire atteint les objectifs du cadre d'action. À cet égard, nous encourageons les audits par tierce partie externes. Il pourra également se révéler utile d'évaluer le potentiel d'autocontrôles, à compléter par des audits de certification réalisés par un organisme indépendant.
- **Test (entre février et juillet 2020) :** tester ce cadre d'action pour un cas d'usage spécifique pendant une phase pilote et réviser le cadre d'action (qui comprend les principes d'action, le guide des bonnes pratiques, le questionnaire d'évaluation et le référentiel d'audit).
- **Déploiement (à partir de juillet 2020) :** soutenir le déploiement du cadre d'action à travers plusieurs scenarios (qui seront sélectionnés ultérieurement pendant le déroulement du projet. Un ou plusieurs scenarios pourront alors être sélectionnés) :
  - **Scenario n° 1 :** engager les fournisseurs et utilisateurs de reconnaissance faciale à soutenir le cadre d'action.
  - **Scenario n° 2 :** porter un cadre de normalisation et/ou de certification afin de créer un modèle de transparence durable
  - **Scenario n° 3 :** soutenir un cadre législatif permettant d'encadrer à la fois un bac à sable d'expérimentation et/ou le déploiement des technologies de reconnaissance faciale (reproductible dans différentes juridictions).

La phase pilote se déroulera sur trois phases :

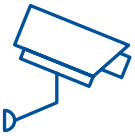


2. Cas d'usages identifiés

Aborder la reconnaissance faciale à travers différents cas d'usage permet de mieux comprendre les arbitrages à effectuer. Cette liste a pour seul but d'illustrer les cas d'usages actuels et potentiels qui nous permettront de tester notre cadre d'action, conformément aux législations nationales applicables.

Ces différents cas d'usage ont été classés selon quatre grandes catégories :

Cas d'usage
Accès par reconnaissance faciale



Cas d'usage
Sûreté et sécurité dans les espaces publics

Cas d'usage
Marketing et services clients

Cas d'usage
Services de santé

Accès par reconnaissance faciale

Les cas d'usages de cette catégorie concernent l'accès des utilisateurs finaux à des services publics ou privés, y compris, mais sans se limiter à :

- Gestion de flux : remplacement de la billetterie par un système de reconnaissance faciale pour l'accès à des locaux ou à des modes de transport collectif, tel que l'accès au train, au métro ou au bus, l'embarquement à bord d'un avion, l'accès à des stades, des salles de concert, des festivals musicaux et des événements publics rassemblant un large public ainsi que le droit d'accès des VIP.
- Clés : accès à des chambres d'hôtels, maisons et immeubles d'habitation.
- Déverrouillage d'appareils : smartphone, ordinateur ou véhicule.
- Paiements et opérations financières : accès à des distributeurs de billets, guichets avec hôte ou hôtesse de caisse, caisses automatiques ou paiement automatique.
- Alternative aux noms d'utilisateurs et mots de passe : connexion à des services en ligne.
- Services d'enregistrement en ligne et hors ligne : vérification d'âge, vérification d'identité, enregistrement à l'hôtel et à l'aéroport.
- Authentification légale : accès à des locaux publics nécessitant la présentation d'une pièce d'identité, identification de visiteurs en milieu carcéral, authentification de citoyens : accès aux bureaux de vote, remplacement de carte d'identité ou de passeport.

Sûreté et sécurité dans les espaces publics

Ces situations incluent les opérations de maintien de l'ordre et les activités de sécurité privée :

- Douanes et protection des frontières : contrôle d'identité.
- Pistage d'un suspect faisant l'objet d'un mandat ou présentant un risque terroriste.
- Surveillance de voisinage : caméras de porte d'entrée de domicile privé ou caméras externes installées sur des véhicules à des fins de reconnaissance faciale.
- Recherche de personnes disparues.
- Sécurité privée : pistage de voleurs à l'étalage et prévention des cambriolages.
- Sécurité des événements publics tels que des manifestations et carnavals.
- Sécurité des espaces publics : vidéosurveillance automatique, établissements scolaires, quais de gare ou de métro, détection de mouvements.
- Patrouille de police : caméras corporelles.
- Présence de personnes : suivi de l'assiduité des élèves.

Marketing et services clients

Cette catégorie comporte tous les services marketing, publicitaires et clients reposant sur la reconnaissance faciale.

- Achats personnalisés : recommandations esthétiques personnalisées, publicités basées sur les recherches des clients ou leur position dans la boutique, suivi des clients en boutiques.
- Reconnaissance automatique de photos sur les réseaux sociaux.
- Ludification des visages et divertissements : émojis personnalisés, filtres, objectifs de déformation des visages ou réalité augmentée.
- Reconnaissance d'émotions : publicités et services reposant sur les émotions et l'expression faciale, sécurité routière (surveillance de l'attention des conducteurs), évaluations préalables à l'embauche.

Services de santé

Cette catégorie comporte tous les services médicaux et destinés aux patients utilisant la reconnaissance faciale.

– Dispositifs portables destinés aux personnes aveugles ou malvoyantes : reconnaissance faciale pour identifier des personnes.

– Authentification des patients : pour éviter les erreurs ou la confusion entre patients.

– Identification ou suivi de pathologies : amélioration du diagnostic et du dépistage de l'autisme, anomalies cardiovasculaires, identification de diabète, diagnostic de troubles congénitaux et de déficience neurologique du développement.

3. Principes d'action

3.1. Recommandations pour utiliser les Principes d'action

Comme indiqué, la première version des Principes d'action sera révisée en fonction des résultats observés au cours du projet pilote. Toute organisation, publique ou privée, intéressée par l'application de ces principes à un projet pilote similaire doit s'assurer de la légalité de la situation d'utilisation. Nous recommandons aux organisations de respecter le cadre suivant :

- **Légalité :** respecter les législations nationales applicables et, dans le cas de l'UE, s'assurer que le déploiement de la reconnaissance faciale est conforme au Règlement Général sur la Protection des Données (RGPD). La société/organisation qui utilise ces technologies doit également produire une analyse d'impact relative à la protection des données (DPIA) disponible sur demande auprès des autorités compétentes de protection des données. Par conséquent, nous encourageons fortement les organisations désireuses de mener un projet pilote en matière de reconnaissance faciale à en informer au préalable les autorités compétentes de protection des données.

- **Audit par un tiers :** pour appliquer et tester ces principes, AFNOR Certification élabore un référentiel d'audit. Ce référentiel permettra d'évaluer l'efficacité des processus de gestion des risques et de gouvernance mis en place par les organisations s'engageant à respecter les principes présentés ci-après. Bien que cet audit puisse être réalisé de façon interne, nous encourageons vivement les organisations à se soumettre à un audit externe réalisé par une tierce partie.

- **Compte-rendu à un organisme de supervision :** Toute organisation intéressée par l'expérimentation d'un cas d'usage de la reconnaissance faciale doit entrer en contact avec l'organisme de réglementation compétent dans sa juridiction. Dans l'UE, cet organisme sera l'autorité nationale de protection des données, par exemple la CNIL en France. Il est à noter que la CNIL a récemment publié une déclaration de principes qui énonce les modalités de conception et de réalisation d'une expérimentation portant sur des technologies de reconnaissance faciale[10].

- **Conduite d'une analyse d'impact portant sur les cas d'usages sensibles :** dans la mesure où notre projet ne consiste pas à évaluer les résultats d'une expérimentation de reconnaissance faciale mais à mener un projet pilote consistant à tester des principes de certification et de transparence, nous encourageons les organisations désireuses d'expérimenter dans une situation sensible, par exemple dans les espaces publics, à réaliser une étude d'impact. Les arbitrages à opérer pour certaines situations d'utilisation ne peuvent être engagés sans débat public ni méthodologie appropriée pour envisager le recours éventuel à la reconnaissance faciale. À cet égard, l'INRIA a récemment publié une méthodologie détaillée pour déployer une analyse d'impact[11].

3.2. Première version des Principes d'action

La première version de ces principes a été rédigée à l'aide d'un processus multipartite tout en prêtant une attention particulière au Règlement Général Européen sur la Protection des Données[12] et à la Directive Police-Justice[13] ; qui ont parfois inspiré certains de ces principes. Nous avons également tenu compte des recommandations en matière d'éthique émises par le Groupe d'experts de haut niveau sur l'intelligence artificielle de la Commission Européenne, un document essentiel qui ouvre la voie à une utilisation éthique des technologies d'IA sur l'ensemble du territoire européen.

Ces principes ont pour objet de garantir une utilisation responsable des technologies de reconnaissance faciale. À cet égard, ils ne concernent pas les autres données biométriques, notamment l'ADN, les empreintes digitales, la reconnaissance d'iris ou de la démarche. Enfin, ces principes représentent la première étape charnière de ce projet pilote de réglementation et doivent être examinés en se référant aux résultats de l'application du pilote obtenus sur le terrain. Pendant la phase de test, nous prêterons particulièrement attention à leur potentiel de mise en œuvre, d'exhaustivité et de pertinence.

Biais et discrimination

Les organisations qui utilisent des systèmes de reconnaissance faciale doivent prendre des mesures appropriées pour garantir que tous les biais ou conséquences inéquitables peuvent être détectés, identifiés et atténués autant que possible. Tout en reconnaissant que l'élimination complète des biais représente l'un des défis majeurs dans le domaine de la recherche en IA, les organisations doivent allouer des ressources appropriées à la mise en œuvre d'outils et de processus qui minimisent les biais et conséquences inéquitables.

Utilisation proportionnelle du système de reconnaissance faciale

Les organisations qui utilisent des systèmes de reconnaissance faciale doivent prendre des mesures raisonnables pour évaluer la pertinence et les limites des systèmes qu'ils envisagent d'utiliser et pour s'assurer que leurs systèmes sont appropriés pour l'usage prévu. Les systèmes de reconnaissance faciale doivent être parfaitement ajustés et limités à l'usage prévu.

Respect de la vie privée dès la conception

Les organisations qui utilisent des systèmes de reconnaissance faciale doivent concevoir des systèmes de respect de la vie privée, notamment en incluant des considérations de confidentialité dans les exigences associées aux systèmes, en intégrant ce principe dans les phases de conception, de développement et de test des technologies et en favorisant les pratiques professionnelles et la maintenance continue des systèmes.

Responsabilité
Les organisations qui utilisent des systèmes de reconnaissance faciale doivent garantir l'existence d'une culture de la responsabilité en interne et auprès de leurs prestataires tiers ou partenaires commerciaux. À cette fin, elles doivent instaurer et communiquer des principes de gouvernance qui déterminent la conception et l'utilisation de leurs systèmes. Cette contrainte ne s'applique pas aux caractéristiques techniques de leurs systèmes destinés à prévenir les cyberattaques potentielles.

Évaluation des risques et audit
Les organisations qui produisent des plateformes de reconnaissance faciale ou qui utilisent la reconnaissance faciale dans le cadre d'une expérience ou de systèmes doivent réaliser une évaluation complète des risques associés à leurs systèmes, notamment leur impact sur la vie privée, le risque d'erreurs, leur prédisposition à produire des biais, leur vulnérabilité face au piratage et aux cyberattaques, le manque de transparence du processus de prise de décisions et le risque de violation de droits civiques.

Performance
Les organisations qui produisent des plateformes de reconnaissance faciale ou qui utilisent la reconnaissance faciale dans le cadre d'une expérience ou de systèmes doivent respecter les critères d'évaluation de la précision et du fonctionnement de leurs systèmes aux stades de conception (tests en laboratoire) et de déploiement (tests de terrain). Ces évaluations du fonctionnement doivent pouvoir être contrôlées par des organismes tiers compétents et leurs comptes-rendus doivent être consultables par les utilisateurs des systèmes.

Droit à l'information
Des processus doivent être mis en place pour informer les utilisateurs finaux qui ont des questions à poser et/ou recherchent des informations concernant l'utilisation des systèmes de reconnaissance faciale. Les utilisateurs finaux doivent avoir accès à leurs données biométriques personnelles sur demande.

Consentement
Les utilisateurs finaux doivent fournir un consentement éclairé, explicite et affirmatif à propos de l'utilisation de systèmes de reconnaissance faciale. Chaque fois qu'une personne concernée souscrit un nouveau service reposant sur une technologie de reconnaissance faciale, elle doit exprimer clairement son consentement pour la durée de conservation des données.

Affichage de l'information
Lorsque ces systèmes sont utilisés dans des espaces publics, une signalisation claire doit être mise en place pour garantir une communication évidente auprès des utilisateurs finaux à propos du recours à la reconnaissance faciale. Les espaces dans lesquels des systèmes de reconnaissance faciale sont utilisés doivent toujours être délimités et indiqués. Un signal visuel doit également informer les personnes lorsque le système en question est en service.

Droit d'accès et droits de l'enfant
La reconnaissance faciale ne doit exclure personne et doit toujours rester accessible et utilisable par tous les groupes de personnes, y compris les personnes âgées et les personnes en situation de handicap. Il est admis que, dans certains cas, par exemple en présence de nourrissons et d'enfants, une exception à ce principe se révèle appropriée et une alternative à l'identification faciale doit être proposée.

Autre option/présence humaine
Un examen manuel (supervision humaine) doit être réalisé chaque fois qu'une utilisation est susceptible de donner lieu à une décision portant à conséquences telle que la violation de droits civiques. Dans le cas des systèmes entièrement automatisés, un système de redondance impliquant l'intervention d'un humain doit toujours être en place pour répondre aux situations exceptionnelles et aux erreurs imprévues. Une alternative à la reconnaissance faciale doit toujours être possible et raisonnable.

Projet pilote portant sur le cas d'usage de la gestion des flux

Parmi les divers cas d'usages présentés dans la première partie du livre blanc, le groupe de travail a décidé de se pencher en priorité sur la « gestion de flux » (accès à un service par reconnaissance faciale) pour plusieurs raisons. En premier lieu, ce cas d'usage représente un fort potentiel de développement dans les années à venir. Par exemple, les organisateurs des Jeux olympiques de Tokyo ont annoncé leur intention de recourir à la reconnaissance faciale pour gérer l'accès des athlètes et du personnel aux stades et aux sites olympiques[14]. De plus, les aéroports et les compagnies aériennes ont commencé à utiliser ces technologies[15].

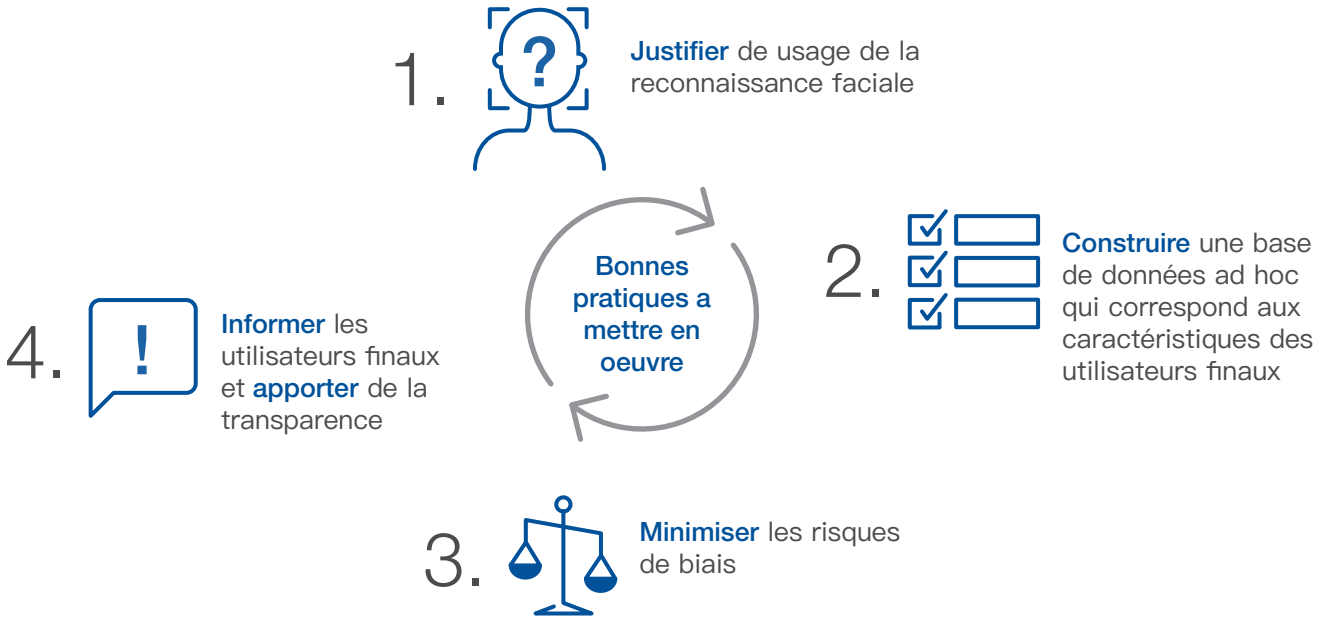
Enfin, tout système de reconnaissance faciale comporte des risques inhérents. En reconnaissant ce postulat et en l'appliquant au cas d'usage de la gestion des flux, les participants aux travaux ont d'une part identifié les risques pouvant apparaître et d'autre part réfléchi à des règles de gestion des risques pour atténuer leurs effets.

La méthodologie ainsi mise en œuvre, dont l'objectif est la prise en compte des enjeux éthiques dans la conception produit, pourrait ainsi servir de fondation pour guider les fournisseurs et utilisateurs de reconnaissance faciale.

1. Bonnes pratiques pour assurer la conception de systèmes de reconnaissance faciale responsables

Afin de faciliter la conception et le déploiement de systèmes de reconnaissance faciale conforme aux principes d'action énoncés pour la gestion des flux, les fournisseurs et utilisateurs de tels systèmes sont encouragés à respecter un certain nombre de prérequis. Ceux-ci portent sur quatre dimensions clés : (i) Justifier de l'usage de la reconnaissance faciale, (ii) construire une base de données ad hoc qui correspond aux caractéristiques des utilisateurs finaux, (iii) minimiser les risques de biais, et (iv) informer les utilisateurs finaux. Ces bonnes pratiques ont vocation à non seulement guider le travail des équipes de développement produit, mais également l'ensemble des opérations des organisations qui fournissent ou utilisent cette technologie.

Bien que ces prérequis puissent s'avérer pertinents pour divers cas d'usages de reconnaissance faciale, ils ont été conçus avant tout pour ceux associés à la gestion des flux. En outre, ils représentent un ensemble minimum de bonnes pratiques qui pourront être revues et complétées en fonction des résultats du projet pilote.



Justifier de l'usage de la reconnaissance faciale

Cette étape permet de définir le problème à résoudre et d'expliquer pourquoi un système de reconnaissance faciale permet de mieux résoudre celui-ci que d'autres méthodes alternatives (par exemple une revue manuelle des titres de transport). Pour cela, il est conseillé de réaliser une analyse des avantages et inconvénients identifiés qui ont conduit à privilégier une solution de reconnaissance faciale. En outre, les organisations désireuses de déployer une telle technologie devraient définir quelles hypothèses (par exemple, taux de faux positifs et de faux négatifs attendus, performance attendue) doivent se révéler justes pour valider le choix de la reconnaissance faciale. Si ces hypothèses n'ont pas été vérifiées, les organisations concernées sont alors invitées à collecter les données nécessaires permettant de les confirmer.

Construire une base de données ad hoc qui correspond aux caractéristiques des utilisateurs finaux

Sur la base de l'observation des caractéristiques des utilisateurs finaux, il est recommandé de construire une base de données ad hoc qui comprend des échantillons suffisamment égaux des sous-groupes qui composent la population d'utilisateurs finaux et de collecter les données en conséquence. Dans la mesure du possible, ces données doivent également refléter des conditions similaires à celles où le système sera déployé. Même lors de l'utilisation d'un modèle pré- entraîné, il est important de collecter un ensemble de données de test spécifiques aux conditions d'utilisation et aux caractéristiques des utilisateurs finaux pour évaluer le système et les risques de biais. En cela, il est essentiel de valider que les données de test soient cohérentes avec celles de la base de données qui sera utilisée.

Atténuer les risques de biais

Définir les risques de biais dans le système à développer au regard de son usage pour faciliter la gestion des flux.

À cette fin, les organisations qui fournissent ou utilisent une technologie de reconnaissance faciale devraient :

- Évaluer chaque étape de leur processus d'utilisation (par exemple, en observant les biais basés sur la capture d'image et les biais basés sur les performances du modèle). Considérer et documenter l'impact des faux positifs et des faux négatifs dans chaque cas.

- Documenter les caractéristiques des utilisateurs finaux du système, en tenant par exemple compte des tranches d'âge, du sexe, des pays de naissance, de l'origine ethnique, et réunir par priorité les groupes qui nécessitent une attention particulière en raison des risques de biais dont ils peuvent faire l'objet. Réaliser ensuite les analyses suivantes :

  - Comment le système va-t-il se comporter pour les personnes en fauteuil roulant ou particulièrement grandes ou encore pour les personnes qui portent des turbans, foulards ou couvre-chefs?

  - Pour chaque risque de discrimination identifié, déterminer comment l'organisation évalue la performance du système de reconnaissance faciale pour atténuer ce biais : Quels paramètres sont utilisés? Comment sont-t-ils mesurés? Quels critères doivent être réunis pour chaque paramètre afin que le système soit prêt à être déployé?

- Définir l'environnement dans lequel chacun des risques identifiés sera évalué et justifier dans quelle mesure il reflète l'environnement au sein duquel le système sera déployé.

Définir et documenter la façon dont les biais identifiés seront atténués

Il est important d'évaluer continuellement les risques de biais et de concevoir des processus permettant leur atténuation tout au long du développement du système de reconnaissance faciale et lors de son fonctionnement opérationnel. Certaines stratégies d'atténuation peuvent être définies au cours de la phase de conception, par exemple lors de la spécification de la qualité des capteurs ou en s'assurant de la qualité de l'éclairage de la zone de capture. D'autres stratégies peuvent également être mises en œuvre par les fournisseurs de systèmes de reconnaissance faciale, telles que le recadrage de photos pour éviter d'inclure les cheveux afin d'améliorer la précision du système pour les personnes portant des turbans, foulards ou autres couvre-chefs. Au-delà de ces interventions purement techniques, d'autres options existent : offrir la possibilité aux individus de réessayer immédiatement en cas d'erreur du système. Peu importe l'étape (création de la base de données d'entraînement, conception du système, déploiement opérationnel, etc.) à laquelle un risque de biais est identifié ou une stratégie d'atténuation des risques de biais est mise en œuvre, il est essentiel d'évaluer régulièrement l'efficacité de ces stratégies.

Évaluer le système pour détecter les risques de biais au cours du processus de développement

Il est essentiel d'aménager le temps nécessaire pour de multiples évaluations du système de reconnaissance faciale afin de mieux détecter et atténuer les risques de biais ; lors de son processus de développement. Si certains risques demeurent trop importants, il est nécessaire de repousser le déploiement opérationnel du système jusqu'à ce que ces risques soient correctement atténués.

Bâtir un processus d'implémentation

Mettre en œuvre des processus pour établir des bonnes pratiques et examiner les systèmes de détection, d'identification et d'atténuation des biais.

Informer les utilisateurs finaux et apporter de la transparence

Les utilisateurs finaux devraient avoir un accès simplifié :

- Aux informations pertinentes sur le fonctionnement du système de reconnaissance faciale ;
- Aux principes de gouvernance qui guident la conception et l'utilisation du système et ce dans un format intelligible pour les non-experts
- A la politique de consentement comprenant un résumé des dispositions clés (par exemple, les finalités prévues, la période de conservation des données, la protection des données et les politiques de partage).

En outre, l'utilisateur de la technologie doit fournir la preuve que l'espace de capture est compréhensible pour les utilisateurs et que l'affichage associé est visible et lisible.

2. Première version du questionnaire d'évaluation

La première version du questionnaire d'évaluation a été conçue selon la même méthode multipartite utilisée pour les principes d'action. Ce questionnaire a pour objectif de permettre une évaluation minutieuse des systèmes de reconnaissance faciale déployés pour la gestion des flux et assurer leur conformité avec les principes d'actions énoncés en première partie. Il s'agit donc d'une déclinaison opérationnelle de ces principes qui a vocation à être instruite par les entreprises et organisations fournissant et utilisant des systèmes de reconnaissance faciale.

Ce questionnaire représente la seconde étape charnière de ce projet, après la rédaction des principes d'action. Aussi, il est susceptible d'évoluer en fonction des résultats du projet pilote qui va être mené prochainement. Pendant la phase de test, nous prêterons particulièrement attention à leur potentiel de mise en œuvre, d'exhaustivité et de pertinence. Enfin, pour simplifier la lecture du questionnaire, nous avons repris les titres des principes d'action et présenté sous chacun d'eux les questions d'évaluation associées.

Biais et discrimination

- Quelle est votre définition d'un biais dans votre cas d'utilisation? Décrire les paramètres utilisés pour évaluer chacun d'entre eux.
- Quel est votre référentiel d'analyse des risques? Décrivez les risques de biais identifiés pour votre cas d'usage et les caractéristiques des groupes d'utilisateurs finaux qui pourraient subir ces risques de biais.
- Comment les risques sont-ils hiérarchisés dans ce processus? Comment les intérêts divergents sont-ils traités?
- Veuillez décrire les meilleures pratiques qui ont été appliquées à votre cas d'usage pour détecter, identifier et atténuer les biais.
- Quels processus et ressources avez-vous mis en œuvre pour garantir que les résultats potentiellement discriminants soient détectés, et atténués de la meilleure façon possible?
- Quels sont vos cas de tests du système biométrique ainsi que votre cahier de recette pour valider l'algorithme?
- Quelle est la distribution de vos données d'entraînement et dans quelle mesure est-elle similaire/différente à celle des utilisateurs de votre système? S'il existe des écarts, comment avez-vous évalué leurs impacts et comment les avez-vous réduits?
- À quels arbitrages pour vos clients/utilisateurs faites-vous face (ex : arbitrages entre avantages et inconvénients produits par la technologie)? Quel est votre processus de résolution des arbitrages lorsque ces intérêts divergents apparaissent?
- Si vous avez fait face à des écarts entre les critères annoncés et les performances réelles, comment ces écarts ont-ils été atténués?

Utilisation proportionnelle du système de reconnaissance faciale

- Quelles sont les alternatives à votre système de reconnaissance faciale? Quel processus/méthodologie vous a conduit à les écarter? Quels sont les critères utilisés pour déterminer les avantages et inconvénients des différentes options?
- Comment avez-vous évalué la pertinence de votre système par rapport à son objectif?
- Avez-vous décrit les besoins techniques pour atteindre les objectifs assignés à votre système et cela sous un format compréhensible pour des acteurs tiers de contrôle?
- Avez-vous réalisé une analyse de risque sur les situations de faux positifs et de faux négatifs (notamment sur les risques de violation des droits civils ?)

Respect de la vie privée dès la conception

- Quels processus et ressources avez-vous déployé pour assurer la confidentialité des données biométriques (ex : afin d'éviter une sur-collecte de données biométriques au vu des finalités d'usages)?
- Avez-vous créé un poste de délégué à la protection des données?
- Comment formez-vous vos équipes au développement de produits de reconnaissance faciale respectant dès leur conception la vie privée (notamment les chefs de produit, l'équipe juridique, les concepteurs UX, les data scientists et les développeurs) pour assurer un niveau élevé de protection des données?

Responsabilité

- Quels sont les mécanismes que vous avez mis en œuvre pour assurer une gouvernance transparente de votre système?
- Avez-vous mis en place un processus de revue et de validation?

Évaluation des risques et audit

- Avez-vous soigneusement identifié les risques liés à l'utilisation de votre système avant (grâce à un référentiel d'évaluation des risques) et pendant son déploiement opérationnel (par exemple via un référentiel d'audit in situ) avec une attention particulière portée sur les dimensions suivantes?
  - Impact sur la vie privée,
  - Potentiel d'erreurs,
  - Susceptibilité d'un biais,
  - Vulnérabilité au piratage et aux cyberattaques,
  - Manque de transparence dans le processus de prise de décision,
  - Violation potentielle des droits civils.

Performance

- S'agissant des tests laboratoire et terrain, quels standards et/ou normes suivez-vous pour évaluer la précision et la performance de vos systèmes (par exemple NIST, ISO, CEN)? Quel critère a été utilisé pour choisir les standards et normes que vous suivez?
- Avez-vous soumis votre système de reconnaissance faciale à l'étude comparative réalisée par le NIST?
- Quel processus avez-vous mis en place pour que vos évaluations de performance soient auditées ; quelles sont les mesures prises pour permettre un audit suffisant de ces résultats par un acteur tiers?
- Quelle est la pertinence des tests de performance conduits au regard du cas d'étude en présence?
- Comment justifiez-vous le seuil de performance choisi qui induit un taux théorique de faux positifs et un taux mesuré de faux négatifs?

Droit à l'information

- Quels processus ont été mis en œuvre pour tenir les utilisateurs finaux informés de l'utilisation de votre système et de leurs données biométriques? En outre, quels processus (par exemple, procédures d'escalade et de résolution) ont été mis en œuvre pour traiter les cas de préjudice subi par les utilisateurs. Les meilleures pratiques incluent mais ne sont pas limitées à la mise à disposition :
  - D'une adresse e-mail
  - D'un numéro de téléphone
  - D'une FAQ d'assistance client
  - D'un chatbot d'assistance client
- Les utilisateurs peuvent-ils accéder, récupérer, et demander la suppression des données personnelles (photo, vidéo, données biométriques rattachées à l'identité de la personne : historique des événements du compte, historique des consentements, historique de l'effacement des données biométriques, informations partagées, historiques de l'utilisation des données biométriques) dans un format lisible par machine et dans un délai raisonnable (par exemple 30 jours)?
- Avez-vous établi et divulgué publiquement (par exemple sur votre site Web) les principes de gouvernance qui guident la conception et l'utilisation de votre système dans des formes intelligibles pour les non-experts?
- Avez-vous mis en place un processus permettant aux individus d'accéder anonymement aux informations pertinentes sur le fonctionnement du système?

Consentement

- La politique de consentement fournit-elle des informations explicites et claires aux utilisateurs, à savoir :
  - La page de consentement est-elle accessible au maximum après 2 clics et est-elle facilement visible dans la page « profil » ?
  - Un résumé des dispositions clés est-il accessible dans cette même page ?
  - Celui-ci contient-il les informations suivantes :
    - Description de l'ensemble des finalités prévues,
    - Durée de conservation des données,
    - Politique de partage des données (notamment avec quels tiers ces données vont être partagées),
    - Moyen mis en place pour protéger, sécuriser et stocker les données
  - Ce résumé doit être synthétique, lisible pour des personnes non expertes et ne pas dépasser l'équivalent de deux pages format A4.
- La page permettant d'apporter ou de retirer son consentement permet-elle d'apporter ou de retirer son consentement pour chacune des finalités existantes?
  - Toutes ces options sont-elles bien accessibles sur la même page ?
  - La liste des finalités existantes est-elle bien à jour ?

Affichage de l'information

- Quel moyen a été mis en place pour informer les individus qu'ils entrent dans une zone où le système de reconnaissance faciale est utilisé? Ce moyen est-il suffisamment visible et explicite pour les individus? Un affichage de rappel de droits de l'utilisateur est-il en place?
- Pour un dispositif d'accès à un service physique, de gestion de flux, et/ou d'enrôlement dans un lieu public, vous-êtes-vous assurés que le volume de capture ne dépasse pas la zone de capture délimitée et identifiée par les utilisateurs. Comment vous assurez-vous que la zone de capture est clairement comprise par les utilisateurs? (Fournir pour cela le processus qui a permis de s'en assurer et suivant la démarche évaluation/recherche/test)
- Un affichage de taille suffisante permet-il de rappeler la finalité du dispositif de reconnaissance faciale? Comment vous êtes-vous assurés que l'affichage est visible et lisible? (Fournir pour cela le processus qui a permis de s'en assurer et suivant la démarche évaluation/recherche/test)

Droit à l'accessibilité et droits de l'enfant

- Pouvez-vous décrire la façon dont votre système a été défini et évalué pour accompagner les personnes âgées et/ou souffrant d'handicaps (notamment visuels ou auditifs).
- Votre système de reconnaissance faciale est-il accessible à tous, y compris aux personnes âgées et aux personnes handicapées?
- Quelles ressources avez-vous allouées pour accompagner les personnes âgées et les personnes handicapées?
- Quelle option alternative avez-vous mis en place pour les nourrissons, les enfants et leurs familles?
- Dans les cas où le système de reconnaissance faciale est incompatible avec un usage par des personnes souffrant de handicaps, des personnes âgées, des enfants ou des familles, il est indispensable que l'option alternative ait été pensée pour assurer un service approprié pour ces personnes.

Option alternative / présence humaine

- Avez-vous mis en place un processus d'examen manuel pour les situations ou le rapprochement entre un visage et un document d'identité comportant une photo entraine un faux négatif, notamment au cours de la phase d'enrôlement ?
- Pour les systèmes de reconnaissance faciale, l'option alternative est-elle systématiquement mise en place et :
  - Opérée par des agents humains? (Ces opérateurs sont-ils formés pour gérer les situations d'exception?)
  - Raisonnable ; à savoir qu'elle n'entraîne pas de conséquences négatives disproportionnées (par exemple, doubler le temps nécessaire pour passer le contrôle de sécurité)
- Y-a-t-il un processus alternatif pour les personnes qui n'acceptent pas l'utilisation de leur biométrie?

Conclusion

En raison des données sensibles qu'elle manipule, la reconnaissance faciale, peut quelque soit le cas d'usage, causer des dommages. Cela est vrai même lorsque la finalité première est de rendre service aux individus et à la communauté. Pour faire face à ce nouveau risque, il est urgent de bâtir une réponse à la hauteur des enjeux.

Celle-ci nécessite d'engager une démarche permettant de bâtir collégialement des règles applicables, de les tester grâce à une méthode robuste afin d'obtenir un cadre de gouvernance fiable, partagé et protecteur. Pour cela, nous avons réuni une communauté d'acteurs experts avec laquelle nous construisons un cadre d'action qui repose sur quatre piliers : (i) établir des principes d'action, (ii) proposer des bonnes pratiques pour les appliquer, (iii) mettre à disposition un questionnaire d'évaluation pour les vérifier et (iv) se soumettre à un audit indépendant pour valider le respect des principes d'action.

L'association de ces quatre piliers a pour ambition de non seulement établir des règles et de s'assurer de leur respect, mais également de guider les acteurs pour les respecter. Nous avons en effet la conviction que pour rendre effectif ces principes d'action, ils doivent pouvoir être intégrés au cœur des préoccupations des équipes métiers. Pour réussir cette transition, un travail de coopération entre industriels, chercheurs, acteurs publics, société civile et acteurs politiques doit être mis en œuvre. Si nous parvenons à créer un partenariat durable entre ces acteurs, nous serons alors en mesure de bâtir les fondations d'une approche qui positionne l'humain au cœur des préoccupations associées au développement technologique.

La prochaine étape de ce projet consiste à tester sur le terrain notre cadre d'action afin d'évaluer sa solidité et y apporter les mises à jour nécessaires. Ce test, réalisé pour le cas spécifique de la gestion des flux, permettra notamment à AFNOR Certification de tester le référentiel d'audit bâti à cet effet et ouvrir la voie vers une possible certification de l'usage responsable des systèmes de reconnaissance faciale.

Une fois le projet pilote réalisé, nous entrerons dans une phase de déploiement avec pour objectif de réunir une coalition d'acteurs engagés à respecter et promouvoir ce cadre d'action. Dans la mesure où le projet pilote sur lequel nous sommes engagés s'inscrit dans une démarche expérimentale et ouverte, nous encourageons les industriels, acteurs publics, acteurs de la société civile et chercheurs à contribuer à cette initiative pour enrichir les travaux et renforcer son impact.

Glossaire

Algorithme : série d'instructions d'exécution d'un calcul ou de résolution d'un problème, en particulier à l'aide d'un ordinateur. Ces instructions forment le fondement de toutes les opérations réalisables par un ordinateur et, par conséquent, constituent un aspect fondamental de tous les systèmes d'IA. Parmi les algorithmes de reconnaissance faciale les plus performants, on compte notamment DeepFace, créé en 2014 par Facebook, ou FaceNet, créé par Google en 2015.

Biométrie : la biométrie s'applique à diverses technologies qui utilisent à des fins d'identification et d'authentification les attributs identifiables uniques des personnes, y compris (mais sans s'y limiter) les empreintes digitales, l'empreinte de l'iris, l'empreinte de la main, le modèle de visage, l'empreinte vocale, la démarche ou la signature d'une personne.

Détection faciale : répond à la question « Cette image comporte-t-elle un ou plusieurs visages humains? » La détection identifie les visages humains.

Explicabilité : propriété des systèmes d'IA permettant de fournir une forme d'explication de la démarche empruntée pour parvenir à des conclusions, afin d'améliorer la compréhension des décisions prises ainsi que la confiance des opérateurs et utilisateurs de ces systèmes.

Faux négatif : résultat de test qui indique, de manière erronée, que la personne représentée dans l'image d'exploration n'est pas inscrite et qu'il n'y a pas de correspondance, alors même qu'elle est bien inscrite. Selon la situation d'utilisation de la reconnaissance faciale, les conséquences des faux positifs peuvent varier considérablement.

Faux positif : résultat de test qui indique, de manière erronée, que la personne représentée dans la photo d'exploration est inscrite dans le système, alors même qu'elle ne l'est pas. Selon la situation d'utilisation de la reconnaissance faciale, les conséquences des faux positifs peuvent varier considérablement.

Identification faciale (ou un pour plusieurs) : répond à la question « Cette personne inconnue peut-elle être mise en correspondance avec un gabarit inscrit? » Cette identification compare un gabarit d'exploration avec tous les gabarits d'inscription stockés dans un référentiel, d'où sa deuxième dénomination de correspondance « un pour plusieurs », ou one-to-many en anglais. Les correspondances entre candidats sont produites en fonction du degré de concordance entre le gabarit d'exploration et chacun des gabarits inscrits.

Image d'exploration : une image d'exploration est une image soumise à un système de reconnaissance faciale pour être comparée à des personnes inscrites. Les images d'exploration sont également converties en gabarits d'exploration. Comme pour les gabarits d'inscription, des images de bonne qualité donnent lieu à des gabarits de bonne qualité.

Inscription : l'inscription désigne le processus d'inscription d'images de personnes de manière à créer des gabarits permettant de les reconnaître. Lorsqu'une personne est inscrite dans un système de vérification utilisé à des fins d'authentification, son gabarit est également associé à un identifiant principal qui servira à déterminer le gabarit à comparer avec le gabarit d'exploration.

Gabarit : les images des personnes sont converties en gabarits, qui servent ensuite à la reconnaissance faciale. Des caractéristiques pouvant être interprétées par ordinateur sont extraites d'une ou plusieurs images d'une personne pour créer le gabarit de cette personne.

Précision de la reconnaissance faciale : la précision d'un système de reconnaissance faciale repose sur l'association de deux éléments : la fréquence à laquelle le système identifie correctement une personne inscrite dans le système et la fréquence à laquelle le système ne trouve aucune correspondante concernant une personne non inscrite. Ces deux conditions, appelées « vraies » conditions, s'associent à deux « fausses » conditions pour décrire toutes les conséquences possibles d'un système de reconnaissance faciale (cf. définitions des termes Vrai positif, Vrai négatif, Faux positif et Faux négatif).

Reconnaissance faciale : application logicielle biométrique capable d'opérer une identification ou vérification exclusive d'une personne en comparant et en analysant les caractéristiques de cette personne fonction de ses lignes faciales.

Vérification faciale (ou un pour un) : répond à la question « Ces deux images représentent-elles la même personne ? ». En situation de sécurité ou d'accès, cette vérification s'appuie sur l'existence d'un identifiant principal (tel que la pièce d'identité d'un client) et la reconnaissance faciale est utilisée en second lieu pour vérifier l'identité de la personne. Cette vérification est également appelée correspondance « un pour un » ou one-to-one en anglais, car le gabarit d'exploration (une personne) est comparé uniquement au gabarit stocké pour la (une) personne associée à l'identification présentée.

Vision par ordinateur : la vision par ordinateur est un domaine de science informatique qui vise à permettre aux ordinateurs de voir, d'identifier et de traiter des images à la manière d'un humain, puis de produire un résultat approprié.

Vrai négatif : la personne représentée dans l'image d'exploration n'est pas inscrite et il n'y a pas de correspondance.

Vrai positif : la personne représentée dans l'image d'exploration est inscrite et il y a une correspondance correcte.

Remerciements

Nous tenons à remercier nos organisations et experts participants pour leurs multiples contributions et leur engagement actif :

Hicham Alaoui Fdili, Expert vidéo, SNCF

Didier Baichère, Député des Yvelines et Vice-Président de l'OPECST

Charlotte Baylac, Responsable affaires publiques chez AWS, Amazon

Xavier Blondeau, AMOA Video-protection, SNCF

Vincent Bouatou, Directeur du Laboratoire d'innovation, IDEMIA

Pascal Briand, Manager IT, Traitement des passagers et Automatisation, Groupe ADP

Marine Dunoguier, Directeur des systèmes embarqués, Alcatraz.ai

Natasha Crampton, Head of Office of Responsible AI, Microsoft

Gokce Cobansoy Hizel, Juriste principale, Turkcell

Laurent Dahmani, Directeur-Général adjoint, AFNOR Certification

Jean-Luc Dugelay, Professeur d'ingénierie et de sécurité numérique, EURECOM

Valéria Faure-Muntian, Députée de la Loire

Louis-Thomas Fernandes, Expert LAF, SNCF

Romain Galesne-Fontaine, Directeur des relations institutionnelles et de la communication externe, IN Groupe

Herve Genty, Responsable de la sécurité des données retail, SNCF

Meeri Haataja, PDG et co-fondateur, Saidot.AI

Bruce Hedin, Directeur Scientifique, H5

Mihael Krauth, Ingénieur, OPECST

Jacquelyn M. Krones, Directeur en charge des études IA, Microsoft

Jarrett Lane, Affaires publiques chez AWS, Amazon

Gautier Martin, Chef de projets, Développement de Services et Produits Aéroportuaires, Groupe ADP

Franck Maurin, Directeur des produits et solutions de facilitation du traitement des passagers et des contrôles aux frontières, IDEMIA

Jérémie Mella, Responsable projet, AFNOR Certification

Mickael Mesure, Directeur LAF, SNCF

Cédric Maziere, Responsable du programme de vidéosurveillance, SNCF

Jean-Michel Mis, Député de la Loire

Dana Rivera, Responsable des affaires publiques chez AWS, Amazon

Mathieu Rondel, Directeur Expertise et Performance Opérationnelle, Direction des Opérations Aéroportuaires, Groupe AD

Frank Torres, Directeur principal de la réglementation, Microsoft

Isabelle Valverde, Responsable de la gestion des flux, SNCF

Camille Vaziaga, Responsable des affaires publiques, Microsoft

Philippe Weiss, Responsable des Opérations et de la Vision Clients, SNCF

Nous tenons également à remercier la CNIL et le CNNum pour leur intervention en qualité d'observateurs indépendants, et plus particulièrement :

Theodore Christakis, Membre, CNNum

Karine Dognin-Sauze, Membre, CNNum

Marie Duboys Fresney, Juriste, CNIL

Salwa Toko, Présidente, CNNum

Felicien Vallet, Ingénieur, CNIL

Auteurs principaux :

Sebastien Louradour, French Government Fellow, Forum Économique Mondial

Lofred Madzou, Directeur de projet AI/ML, Forum Économique Mondial

Bibliographie

- *Future of Privacy Forum, Privacy Principles for Facial Recognition Technology in Commercial Applications*, September 2018
- Li Stan Z., Jain Anil K., *Handbook of Face Recognition*, March 2011
- Mitchell Mitchell, *Artificial Intelligence : A Guide for Thinking Humans*, September 2019
- CNIL, *Reconnaissance faciale : pour un débat à la hauteur des enjeux*
- OPECST, Didier Baichere, *La reconnaissance faciale, Les notes scientifiques de l'office*, juillet 2019
- Independent High-level expert group on Artificial Recognition set up by the European Commission, *Ethics guidelines for trustworthy AI*, April 2019
- OECD, *Artificial intelligence in society*, 2019
- Darell M. West, *10 actions that will protect people from facial recognition*, in Brookings website, Nov. 2019
- IDEO, *How can we use AI to make things better for humans? ACLU, The dawn of robot surveillance*, June 2019
- Pew Research Center, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, Sept. 2019
- Rachel German, K. Suzanne Barber, *Current Biometric Adoption and Trends*, The University of Texas at Austin, Center for identity, Sept. 2017
- Claude Castelluccia, Daniel Le Métayer, *Analyse des impacts de la reconnaissance faciale - Quelques éléments de méthode*, Inria Grenoble Rhône-Alpes, Nov. 2019

Notes de fin de document

1. https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp
2. Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf
3. https://www.aclu.org/report/dawn-robot-surveillance
4. http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html
5. https://www.wired.com/story/delicate-ethics-facial-recognition-schools/
6. https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/
7. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
8. NISTIR 8280, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf
9. https://www.reuters.com/article/usa-crime-face/us-government-study-finds-racial-bias-in-facial-recognition-tools-idUSL1N28T29H
10. https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf
11. https://hal.inria.fr/hal-02373093
12. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018- reform-eu-data-protection-rules/eu-data-protection-rules_en
13. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680
14. https://www.cnet.com/news/tokyo-2020-olympics-using-facial-recognition-system-from-nec-intel/
15. https://www.usatoday.com/story/travel/airline-news/2019/08/16/biometric-airport-screening-facial-recognition-everything-you-need-know/1998749001/