44ème Session à huis clos de l'Assemblée mondiale sur la vie privée

Octobre 2022

Résolution sur les principes et les attentes concernant l'utilisation appropriée des informations personnelles dans la technologie de reconnaissance faciale

Cette résolution est soumise par les auteurs au nom du Groupe de travail sur la coopération internationale en matière d'application de la loi et du Groupe de travail sur l'éthique et la protection des données dans l'intelligence artificielle.

SPONSORS :

- Contrôleur européen de la protection des données, Union européenne
- Préposé fédéral à la protection des données et à la transparence, Suisse
- Commissaire à l'information et à la protection de la vie privée, Ontario (Canada)
- Le Bureau du commissaire à l'information, Royaume-Uni
- Bureau du commissaire australien à l'information, Australie
- Commissariat à la protection de la vie privée, Canada
- Commission de protection des informations personnelles, Japon

CO-SPONSORS :

- Autorité catalane de protection des données, Catalogne
- Commission de l'Informatique et des Libertés, Burkina Faso
- Autorité de protection des données, Pays-Bas
- Autorité de protection des données, Norvège
- Autorité réglementaire de Gibraltar, Gibraltar
- Commission d'accès à l'information, Québec (Canada)
- Bureau du commissaire à l'information de Jersey, Jersey
- Agence nationale d'accès à l'information publique, Argentine
- Commission nationale de l'informatique et des libertés, France
- Commission nationale de la vie privée, Philippines
- Commissariat à l'information et à la protection de la vie privée, Terre-Neuve-et-Labrador (Canada)
- Commissariat à l'information et à la protection de la vie privée, Nouvelle-Écosse (Canada)
- Bureau du commissaire à la protection de la vie privée, Nouvelle-Zélande
- Commission de protection des informations personnelles, Corée

- Surintendance de l'industrie et du commerce, Colombie
- Unité de régulation et de contrôle des données personnelles, Uruguay.

La 44ème Session annuelle à huis clos de l'Assemblée mondiale sur la protection de la vie privée :

Rappelant la Résolution sur la technologie de reconnaissance faciale (FRT), adoptée lors de la 42ème session à huis clos de l'Assemblée mondiale de la protection de la vie privée (GPA) en octobre 2020, qui a souligné les risques de FRT pour la vie privée et a mandaté le Groupe de travail sur la coopération internationale en matière d'application de la loi (IEWG) et le Groupe de travail sur l'éthique et la protection des données dans l'intelligence artificielle (AIWG) pour élaborer et promouvoir un ensemble de principes et d'attentes convenus pour l'utilisation appropriée des informations personnelles dans la FRT ;

Reconnaissant la création d'un sous-groupe de membres de l'IEWG et de l'AIWG et les efforts qu'ils déploient pour remplir le mandat défini dans la résolution sur le FRT : en menant des recherches, en effectuant une analyse documentaire, en faisant participer les membres de la GPA, en consultant les parties prenantes mondiales concernées et en élaborant les principes et les attentes ;

Admettant, suite à l'adoption de la résolution sur la FRT en octobre 2020, le développement et le déploiement continus de la FRT en direct et rétrospective par des entités des secteurs public et privé dans une variété de contextes tels que : les espaces publics, les lieux de travail, les magasins, les environnements éducatifs, en ligne et dans les zones de guerre ;

Tenir compte du débat mondial en cours sur le FRT parmi un ensemble diversifié de parties prenantes (notamment les régulateurs, les législateurs, les développeurs, les utilisateurs, le monde universitaire et la société civile), et de leurs points de vue respectifs sur les avantages et les risques du FRT, même qui sont exposés dans les résultats d'enquêtes, les livres blancs, les documents de synthèse, les avis, les blogs, les articles de journaux et autres communications publiques ;

Reconnaissant les contributions importantes des autorités chargées de la protection des données et de la vie privée, ainsi que des organismes internationaux, au débat mondial, par la publication de documents stratégiques et d'orientation, y compris, mais sans s'y limiter :

- les lignes directrices du Comité européen de protection des données (EDPB) sur l'utilisation de la technologie de reconnaissance faciale dans le domaine de l'application de la loi, et l'avis conjoint EDPB-EDPS sur la proposition de loi européenne sur l'intelligence artificielle ;

- Les directives des Commissaires à la protection de la vie privée fédéral, provinciaux et territoriaux du Canada sur la reconnaissance faciale pour les services de police ;

- Cadre juridique recommandé par les Commissaires à la protection de la vie privée fédéraux, provinciaux et territoriaux du Canada pour l'utilisation de la reconnaissance faciale par les services de police ;

- les avis du Bureau du commissaire à l'information du Royaume-Uni sur l'utilisation de la technologie de reconnaissance faciale dans les lieux publics et l'utilisation de la technologie de reconnaissance faciale en direct par les forces de l'ordre dans les lieux publics ;

- les lignes directrices du Conseil de l'Europe sur la reconnaissance faciale ; et

- la recommandation de l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO) sur l'éthique de l'intelligence artificielle.

Soulignant les interventions réglementaires formelles et des activités d'application des autorités chargées de la protection des données et de la vie privée, notamment les enquêtes, les amendes, les avis d'exécution ; les ordonnances de cessation et d'abstention, et les recommandations relatives au déploiement du FRT dans divers contextes par le secteur privé, le secteur public et les organismes chargés de l'application de la loi.

En tenant compte des réglementations existantes et des développements législatifs couvrant l'utilisation du FRT, notamment : la Loi sur la confidentialité des informations biométriques de l'Illinois ; la Loi sur l'intelligence artificielle proposée par l'Union européenne et la Loi sur l'intelligence artificielle et les données proposée par le Canada ;

Apprécier la contribution des membres de la GPA aux travaux du sous-groupe FRT, en partageant leurs points de vue sur les risques les plus importants pour la vie privée associés à des utilisations spécifiques de FRT ;

Accueillir la contribution des utilisateurs, des développeurs, des législateurs et des organisations de la société civile aux travaux du sous-groupe FRT, en contribuant à affiner le champ d'application, la terminologie, la clarté, la couverture et la facilité d'utilisation des principes et des attentes en matière d'utilisation appropriée des informations personnelles dans FRT

Soulignant que le respect des normes de protection des données et de la vie privée est essentiel pour le développement et le déploiement responsables et fiables de FRT, où que ce soit dans le monde ;

Réaffirmant les engagements du Plan stratégique 2021-23 de la GPA visant à renforcer la voix de l'Assemblée dans la politique numérique ; à renforcer la coopération réglementaire, et à œuvrer en faveur d'un environnement réglementaire avec des normes élevées de protection des données et de la vie privée qui sont appliquées de manière claire et cohérente dans le monde entier ;

Reconnaissant que le besoin de normes mondiales claires et cohérentes en matière de protection des données et de la vie privée est particulièrement important dans le contexte d'innovations technologiques complexes à haut risque, telles que le FRT, où

des avantages peuvent être apportés et où les différences de réglementation peuvent introduire une incertitude pour les parties prenantes ;

La 44ème Assemblée mondiale sur la vie privée approuve donc les principes et les attentes concernant l'utilisation appropriée des informations personnelles dans la technologie de reconnaissance faciale, résumés ici et fournis dans leur intégralité en annexe :

1. **BASE JURIDIQUE** : Les organisations qui utilisent la reconnaissance faciale doivent avoir une base légale claire pour la collecte et l'utilisation des données biométriques.

2. **RAISONNABILITÉ, NÉCESSITÉ ET PROPORTIONNALITÉ :** Les organisations doivent établir, et être en mesure de démontrer, le caractère raisonnable, la nécessité et la proportionnalité de leur utilisation de la technologie de reconnaissance faciale.

3. **LA PROTECTION DES DROITS HUMAINS :** Les organisations doivent en particulier évaluer et protéger les interférences illégales ou arbitraires avec la vie privée et les autres droits humains.

4. **TRANSPARENCE :** L'utilisation de la reconnaissance faciale doit être transparente pour les personnes et les groupes concernés.

5. **RESPONSABILITÉ :** L'utilisation de la reconnaissance faciale doit inclure des mécanismes de responsabilité clairs et efficaces.

6. **LES PRINCIPES DE PROTECTION DES DONNÉES :** L'utilisation de la reconnaissance faciale doit respecter tous les principes de protection des données, y compris ceux mentionnés ci-dessus.

La 44ème Assemblée mondiale sur la vie privée décide de travailler ensemble en 2022-23 pour :

1. Continuer à réaliser le mandat de la résolution 2020 de la GPA sur le FRT en élaborant et en mettant en œuvre un plan d'engagement pour :

    a. Promouvoir les principes avec une gamme de groupes de parties prenantes externes clés ; et

    b. Évaluer et examiner l'application des principes dans le monde réel par les développeurs et les utilisateurs de FRT.

2. Demande que l'IEWG et l'AIWG continuent à travailler ensemble pour mener à bien cette activité et aussi qu'ils rendent compte de leurs progrès à la 45ème session fermée de l'Assemblée mondiale sur la protection de la vie privée.

Annexe :

Principes et attentes pour une utilisation appropriée des informations personnelles dans la technologie de reconnaissance faciale

Global Privacy Assembly

GPA
Global Privacy Assembly

Introduction

Lors de la 42ème session fermée de l'Assemblée mondiale de la protection de la vie privée (GPA) en octobre 2020, les membres de la GPA ont adopté une résolution sur la technologie de reconnaissance faciale (la Résolution).

La Résolution a accepté que les applications potentielles de la technologie de reconnaissance faciale pourraient présenter des avantages pour la sécurité et la sûreté publique, mais elle souligne également que cette technologie peut permettre une surveillance arbitraire ou illégale et qu'elle peut être très intrusive, elle peut fournir des résultats biaisés et aussi elle peut porter atteinte à la protection des données, à la vie privée et aux droits humains.

Les organismes publics, les organisations privées et la société civile ont exprimé leur inquiétude quant au fait que la technologie de reconnaissance faciale pose des problèmes de vie privée, juridiques et éthiques qui doivent être résolus. En même temps, la GPA a précédemment identifié la nécessité de travailler à l'élaboration d'une politique mondiale, de normes et de modèles pour les questions ayant un impact important sur la vie privée. Cela permet de renforcer la coopération réglementaire, d'améliorer l'efficacité de la prévention, de la détection et de la résolution des problèmes de protection des données et de la vie privée, et aussi, de garantir la cohérence et la clarté du système de surveillance de l'économie numérique.

LA GPA a donc décidé d'élaborer un ensemble de principes et d'attentes convenus pour l'utilisation appropriée des informations personnelles dans la technologie de reconnaissance faciale, y compris des recommandations sur la manière d'atténuer les risques. Le présent document répond à cet objectif.

À propos de la reconnaissance faciale

La reconnaissance faciale est un processus dans lequel des outils logiciels analysent une image numérique du visage d'un individu, extraient ses caractéristiques distinctes dans un modèle biométrique et comparent ce modèle à un ou plusieurs modèles biométriques extraits au préalable. Cette comparaison peut être effectuée à des fins de **vérification** (p. ex. une comparaison un à un pour vérifier une demande d'identité faite par un individu) ou d'**identification** (p. ex. une comparaison un à plusieurs ou plusieurs à plusieurs d'une image d'un individu inconnu par rapport à une base de données de références biométriques). Elle peut s'effectuer selon différents modes, notamment des applications **en direct** ou **en temps quasi réel** (p. ex. comparaison en temps réel d'un ou de plusieurs visages avec une liste de surveillance) et des applications **rétrospectives** (p. ex. comparaison d'une image précédemment capturée d'un individu inconnu avec une base de données de références biométriques, comme cela lors d'une enquête policière).

Comme l'indique la Résolution, la technologie de reconnaissance faciale repose sur des informations biométriques sensibles qui sont uniques à l'individu et difficiles à modifier. Les décisions prises à l'égard des personnes à l'aide de ces identifiants, souvent faites à leur insu ou sans leur consentement, peuvent avoir des conséquences négatives sans qu'il existe des voies de recours appropriées. Outre les

impacts sur la vie privée, l'utilisation généralisée de la reconnaissance faciale peut également avoir des effets discriminatoires et affecter la capacité à exercer d'autres droits humains fondamentaux, tels que la liberté d'expression, de mouvement et d'association.

Application des principes

Ces principes s'appliquent à tous les types et à toutes les utilisations de la reconnaissance faciale par les organisations des secteurs privé et public (y compris les forces de l'ordre). Bien que, pour des raisons de commodité, nous ayons utilisé le terme << reconnaissance faciale >> tout au long de ce document, les principes énoncés ci-dessous s'appliquent également à toute analyse biométrique des images faciales et des modèles biométriques (comme la déduction de caractéristiques démographiques, de l'état émotionnel, etc.) Les principes sont destinés à s'appliquer aux utilisateurs, aux développeurs et aux fournisseurs de systèmes de reconnaissance faciale.

Il convient de noter que les principes énoncés ci-dessous sont d'importance équivalente et doivent être considérés de manière globale.

Enfin, nous reconnaissons que les gouvernements et les régulateurs de la protection des données ont un rôle important à jouer dans la technologie de reconnaissance faciale, notamment en ce qui concerne l'établissement et l'application de cadres réglementaires appropriés. Toutefois, ce sujet est hors du champ d'application du présent document.

Terminologie

Dans ce document, nous avons utilisé les termes suivants :

Biométrique : Une biométrie est la mesure d'une caractéristique physiologique (p. ex. l'empreinte digitale, l'iris, le visage ou la géométrie de la main d'une personne) ou d'un attribut comportemental (p. ex. la démarche ou les habitudes du clavier) d'un individu. Ces caractéristiques sont généralement persistantes, uniques à l'individu, et difficiles ou impossibles à modifier (c'est-à-dire, que la modification d'un élément biométrique nécessite une modification de la personne physique de l'individu). Ainsi, elles doivent être considérées comme sensibles.

Modèle biométrique : Représentation numérique ou mathématique des données biométriques d'une personne. Même si le format spécifique du modèle est modifiable, il représente une caractéristique unique, difficile à changer et indissociable d'une personne ; il doit donc être considéré comme sensible.

Sonde biométrique : Modèle biométrique extrait de l'image d'un individu inconnu ou non vérifié qui sera comparé à une référence biométrique (s'il y a une vérification) ou à une base de données de référence (dans le cas de l'identification).

Référence biométrique : Modèle biométrique extrait d'une image associée à une identité connue, auquel une sonde biométrique est comparée.

Base de données de référence : Une liste ou une base de données de références biométriques, contre chacune desquelles une sonde biométrique est comparée.

Considération juridique

Les principes ci-dessous sont formulés comme des recommandations (en utilisant le terme << devrait >>). Cependant, nombre d'entre eux sont des exigences légales explicites dans les juridictions des membres ou peuvent être interprétés comme tels par les tribunaux et les autorités de protection des données. Il incombe à toute organisation qui souhait d'utiliser la technologie de reconnaissance faciale de comprendre les exigences légales applicables dans sa juridiction.

PRINCIPES

1. BASE JURIDIQUE : Les organisations utilisant la reconnaissance faciale doivent avoir une base légale claire pour la collecte et l'utilisation des données biométriques.

1.1. Les organisations doivent documenter, et être prêtes à démontrer, la légalité de leur utilisation de la biométrie pour la reconnaissance faciale. Cela comprend à la fois la base légale pour capturer l'image d'une personne afin de créer une sonde biométrique et aussi pour créer, accéder ou modifier toute base de données de référence qui est, ou sera, utilisée. Cette base doit être réévaluée périodiquement pour tenir compte des changements de la loi ou de son interprétation.

1.2. Si les organisations opèrent dans une juridiction qui reconnaît plusieurs bases légales pour le traitement, elles doivent examiner si une autre base est plus appropriée que le consentement. Dans de nombreuses applications, notamment l'utilisation de la reconnaissance faciale dans les espaces accessibles au public et les contextes d'emploi, il peut être difficile pour une organisation de démontrer qu'elle a obtenu le consentement valable d'une personne.

1.3. Si le consentement est la base du traitement, les organisations doivent s'assurer et être en mesure de démontrer que le consentement est significatif. Cela signifie qu'il est informé, spécifique, actuel, donné librement et sans ambiguïté. Cela inclut la prise en compte de la capacité d'une personne à donner un consentement valable (comme dans le cas des jeunes ou des personnes vulnérables).

1.3.1. Le consentement explicite est préférable. Les organisations doivent savoir que le consentement implicite ne répond pas aux normes de consentement dans de nombreuses juridictions et qu'en général, il ne doit pas être utilisé pour la collecte d'informations personnelles sensibles. Toutefois, si une organisation considère qu'elle peut s'appuyer sur le consentement implicite pour la reconnaissance faciale, elle doit être en mesure de démontrer qu'il est (i) approprié dans les circonstances, et (ii) raisonnable de croire dans les circonstances qu'une personne a donné son consentement.

1.4. Les organisations doivent savoir que dans de nombreuses juridictions, le << scraping >> (capture) d'images à partir de plateformes en ligne accessibles au public (notamment de services de réseaux sociaux) pour créer une base de données de référence de reconnaissance faciale, n'est pas considéré comme légal ou équitable, ni comme un processus transparent.

2. RAISONNABILITÉ, NÉCESSITÉ ET PROPORTIONNALITÉ : Les organisations doivent établir, et être en mesure de démontrer, le caractère raisonnable, la nécessité et la proportionnalité de leur utilisation de la technologie de reconnaissance faciale.

2.1. Les organisations doivent établir la nécessité d'utiliser la technologie de reconnaissance faciale. Prenant en compte la sensibilité des informations concernées, le seuil pour établir la nécessité est élevé. Il faut élaborer clairement l'objectif visé : que la technologie de reconnaissance faciale peut être efficace pour atteindre cet objectif, et que l'objectif ne peut pas être raisonnablement atteint par des moyens moins intrusifs. La commodité ou le caractère souhaitable ne doivent pas être invoqués pour établir la nécessité.

2.2. Les organisations doivent établir, et être en mesure de démontrer, la proportionnalité de leur utilisation de la technologie de reconnaissance faciale. Là encore, le seuil de proportionnalité est élevé. Les avantages de l'utilisation de la reconnaissance faciale doivent clairement l'emporter sur le risque d'atteinte à la vie privée des personnes et aux autres droits humains. En établissant la proportionnalité :

2.2.1. Les organisations devraient documenter, et être en mesure de démontrer, les avantages attendus de l'utilisation de la technologie de reconnaissance faciale. Les organisations doivent également définir clairement comment elles mesureront si le système a réalisé ces avantages, et le niveau d'avantage en dessous duquel l'utilisation de la reconnaissance faciale serait arrêtée.

2.2.2. Les organisations doivent documenter, et être en mesure de démontrer, qu'elles ont évalué les risques ou connus de préjudice que présente l'utilisation proposée de la reconnaissance faciale. Cela doit inclure l'examen des risques de préjudice pour les individus et les groupes. Les organisations doivent également documenter clairement les mesures qu'elles ont mises en œuvre pour atténuer les risques identifiés.

2.2.3. Dans le cas de l'identification, une organisation doit démontrer un intérêt public évident dans l'utilisation de la technologie. En général, le bénéfice commercial ne sera pas considéré comme un intérêt public évident.

2.2.4. Le seuil de proportionnalité peut être plus facilement atteint dans les cas d'utilisation de la technologie de reconnaissance faciale à des fins de vérification lorsque l'organisation peut démontrer que les personnes ont consenti de manière significative à l'utilisation du système, comme est indiqué au principe 1.3.

2.3. Les organisations doivent établir le caractère raisonnable de leur utilisation de la technologie de reconnaissance faciale. Le seuil pour établir le caractère raisonnable est élevé. Ce qui est raisonnable est une question de fait dans chaque cas individuel. Le caractère raisonnable peut être influencé par les attentes de la communauté, ainsi que par les normes et pratiques actuelles de la technologie de reconnaissance faciale.

2.4. Pour éviter que les décisions ne soient influencées par des coûts ou des engagements irrécupérables ; l'évaluation du caractère raisonnable, de la nécessité, et de la proportionnalité doit être entreprise avant l'achat, le développement ou le déploiement d'un système de reconnaissance faciale.

2.5. Les organisations doivent être informées de toute décision de leurs autorités de protection des données respectives que les inconvénients connus ou potentiels de certaines applications de la reconnaissance faciale sont tellement importants qu'ils ne peuvent être proportionnels aux avantages escomptés.

> 2.5.1. En particulier, les organisations doivent savoir que le préjudice potentiel associé à la reconnaissance des caractéristiques humaines dans les espaces publics (y compris par reconnaissance faciale) a conduit de multiples autorités nationales, régionales et locales de protection des données à proposer des interdictions de cette pratique, notamment toutes les autorités de protection des données de l'EEE,
>
> 2.5.2. Les organisations doivent également savoir que de nombreuses autorités de protection des données ont demandé l'interdiction d'autres formes d'analyse faciale non liées à la vérification et à l'identification, telles que la déduction de l'état émotionnel.

2.6. L'évaluation par une organisation du caractère raisonnable, de la nécessité et de la proportionnalité doit être régulièrement réexaminée. Il s'agit notamment de déterminer si le besoin auquel il est répondu existe toujours, si les avantages escomptés de l'utilisation de la reconnaissance faciale se sont concrétisés et si des inconvénients non identifiés auparavant sont apparus ; ou bien si les inconvénients identifiés ont été pires que prévu, de sorte que ces inconvénients l'emportent désormais sur les avantages.

3. PROTECTION DES DROITS HUMAINS : Les organisations doivent en particulier évaluer et protéger contre toute ingérence illégale ou arbitraire dans la vie privée et les autres droits humains.

3.1. En général, les organisations doivent partir du principe que l'utilisation de la technologie de reconnaissance faciale peut interférer indûment avec la protection des données et le droit à la vie privée des individus.

> 3.1.1. Cette interférence est généralement plus importante lorsque ces technologies sont utilisées dans un espace accessible au public. Les organisations doivent prendre note que la présence d'une personne dans un lieu public ne signifie pas nécessairement qu'elle a renoncé à toute attente raisonnable en matière de vie privée ou de contrôle des renseignements

personnels. Conformément au principe 2.5.1, de nombreuses autorités de protection des données ont proposé d'interdire telles utilisations.

3.1.2. Les interférences seront également accrues par toute utilisation de la reconnaissance faciale qui suit les mouvements, les actions ou les comportements d'une personne au fil du temps (dans le même endroit ou dans des endroits multiples et, en particulier, dans des endroits qui peuvent révéler des informations sensibles sur une personne).

3.2. Les organisations ne doivent pas supposer que les images de personnes accessibles au public sur Internet (y compris sur les sites de réseaux sociaux) peuvent être collectées et transformées pour être utilisées comme sondes ou références biométriques, ou pour entraîner un système de reconnaissance faciale, sans la connaissance et le consentement de ces personnes ou une autre base légale pour cette collecte et cette utilisation.

3.3. Lorsqu'elles déterminent les impacts potentiels sur la protection des données et le droit à la vie privée, les organisations doivent :

3.3.1. Réaliser des analyses d'impact appropriées (telles qu'une analyse d'impact sur la vie privée, une analyse d'impact sur la protection des données ou une analyse d'impact sur les droits humains).

3.3.1.1. Les organisations doivent faire preuve de transparence à l'égard de toutes les personnes potentiellement préoccupées en ce qui concerne leur évaluation et leur atténuation des risques d'atteinte à la vie privée.

3.3.2. Tenir compte des différences démographiques (c'est-à-dire, des préjugés) en ce qui concerne à la fois le fonctionnement du système (p. ex. les différences de performance pertinentes entre les groupes) et l'application du système (p. ex. les différences dans la façon dont le déploiement du système aura un impact sur les individus ou les groupes). Les organisations doivent également envisager la manière dont elles mesureront, sur une base continue, tout impact différentiel de l'utilisation du système de reconnaissance faciale sur les groupes.

3.3.3. Tenir compte du << chilling effect >> potentiel sur des droits tels que la liberté d'expression et la liberté d'association, ainsi que du risque de discrimination, lié à l'utilisation de systèmes de reconnaissance faciale dans les espaces accessibles au public, indépendamment de la finalité de ces systèmes.

3.3.4. Lorsque des groupes marginalisés risquent d'être particulièrement touchés par l'utilisation d'un système, il faut consulter des représentants de ces groupes au sujet des impacts prévus et des stratégies visant à réduire les préjudices.

3.4. Si possible, en employant la reconnaissance faciale pour la vérification, une méthode alternative qui ne repose pas sur la biométrie doit être mise à disposition, y

compris pour les personnes qui refusent ou retirent leur consentement. Les personnes ne doivent pas être pénalisées pour l'utilisation de cette méthode alternative.

4. TRANSPARENCE : L'utilisation de la reconnaissance faciale doit être transparente pour les individus et les groupes concernés.

4.1. Les organisations doivent s'assurer que les personnes sont informées (dans un langage clair et simple) de :

4.1.1. Chaque fois que leur image faciale capturée peut être ou sera soumise à un système de reconnaissance faciale, ou que leur modèle biométrique peut être ou sera inclus dans une base de données de référence pour un système de reconnaissance faciale. Il est préférable et de bonne pratique - et dans certaines circonstances, la loi l'exige - que les personnes soient informées de cela avant ou au moment où leur image faciale est capturée.

4.1.2. Leurs droits en matière de données concernant les systèmes de reconnaissance faciale, ainsi que la manière de les exercer. Il s'agit notamment de la possibilité de demander que leur image faciale ne soit pas soumise à un système de reconnaissance faciale, que leur modèle biométrique soit supprimé d'une base de données de référence (le cas échéant), ou que leurs informations dans un système de reconnaissance faciale soient corrigées (p. ex. en mettant à jour leur référence biométrique).

4.1.3. Toute autre information devant être fournie aux individus en vertu de la loi de leur juridiction. Il s'agit notamment de savoir comment et où les informations seront stockées, à quelles fins elles seront traitées, combien de temps elles seront conservées et avec quelles entités elles pourront être partagées.

4.2. Les organisations doivent réfléchir comment elles s'assureront qu'un avis adéquat est fourni à toutes les personnes, y compris les jeunes et les personnes vulnérables.

4.3. Les organisations doivent savoir que la signalisation de l'utilisation d'un système de reconnaissance faciale, généralement, ne suffira pas par soi même à assurer la conformité au principe 4.1.

4.3.1. Bien que le traitement repose sur le consentement et que la signalisation est un élément de ce processus de consentement, la signalisation doit être bien visible avant qu'une personne accède à une zone surveillée. Cette signalisation doit inclure une indication de toute alternative disponible pour accéder à l'espace. La signalisation doit également indiquer clairement que la reconnaissance faciale est utilisée, par opposition à une caméra de sécurité standard.

4.3.2. Lorsque la signalisation est un élément clé de la stratégie de notification d'une organisation, il convient de réfléchir à la manière dont la notification sera fournie aux personnes qui peuvent avoir des difficultés à lire ou à comprendre les signalisations.

4.4. Au cas de la reconnaissance faciale rétrospective, les organisations doivent prendre des mesures proactives pour s'assurer que les personnes sont informées de l'utilisation et de la finalité du système. Cela comprend la publication de ces informations avant l'utilisation du système, ainsi que (dans la mesure du possible) l'envoi d'un avis spécifique aux personnes dont les images ont été traitées par le système.

5. RESPONSABILITÉ : L'utilisation de la reconnaissance faciale doit inclure des mécanismes de responsabilité clairs et efficaces.

5.1. Les organisations doivent établir des politiques claires de gouvernance et d'atténuation des risques pour toutes les utilisations de la reconnaissance faciale, et aussi doivent être prêtes à démontrer l'existence et l'efficacité de ces politiques.

5.1.1. Les organisations doivent établir et maintenir un moyen de détecter la non-conformité aux politiques de gouvernance et de gestion des risques pour la reconnaissance faciale (y compris par les acteurs internes), et les conséquences de cette non-conformité.

5.2. Tous les utilisateurs d'un système de reconnaissance faciale doivent suivre une formation régulière sur les politiques internes de protection de la vie privée, les exigences légales de leur juridiction, les limites et les biais potentiels des systèmes de reconnaissance faciale, la manière de procéder à la comparaison des visages, et les moyens d'atténuer les risques connus tels que le biais d'automatisation (c'est-à-dire, la tendance des humains à accorder plus de poids aux suggestions faites par un système automatisé).

5.3. Partout où cela est raisonnable, les conclusions tirées sur l'identité d'une personne doivent être évaluées par une personne qui a suivi une formation appropriée. C'est particulièrement le cas lorsqu'une personne sera affectée de manière significative par une telle conclusion.

5.3.1. Les personnes doivent avoir la possibilité de défier et de demander réparation pour toute décision prise à leur sujet sur la base d'une identification en utilisant la reconnaissance faciale.

5.3.2. Les organisations doivent s'assurer que le seuil pour un << match >> est raisonnable pour l'application proposée du système, si ce seuil soit déterminé par l'organisation elle-même ou par le développeur du système.

5.3.3. Les organismes doivent établir des stratégies d'atténuation pour gérer les risques associés aux non-concordances (à la fois faux positifs et faux négatifs) et aux erreurs d'enregistrement (c'est-à-dire, les inexactitudes dans la base de données de référence).

5.4. Les organisations doivent reconnaître les limites des systèmes de reconnaissance faciale et interpréter les résultats produits par ces systèmes en conséquence. Par exemple, dans le contexte d'un système de reconnaissance faciale rétrospectif utilisé par les forces de l'ordre, un << match >> doit être considérée comme une piste potentielle et non comme une preuve concluante ou admissible.

5.5. Les organisations doivent entreprendre des audits périodiques de l'efficacité du système de reconnaissance faciale, des mesures d'atténuation des risques mises en place et de la conformité interne aux politiques de gouvernance.

5.6. Les organisations devraient surveiller et évaluer régulièrement toute différence démographique dans l'efficacité de leur utilisation d'un système de reconnaissance faciale.

5.7. Les organisations développant des systèmes de reconnaissance faciale doivent documenter les mesures prises pour mesurer et protéger leurs produits contre les différentiels démographiques, ainsi que l'efficacité de ces mesures (c'est-à-dire, toute différence de performance connue entre les groupes démographiques).

5.8. Les organisations qui envisagent d'acheter ou d'utiliser d'une autre manière des systèmes de reconnaissance faciale devraient :

> 5.8.1. Obtenir des informations sur la mesure des différentiels démographiques et les protections contre ceux-ci, documentées par le principe 5.7.
>
> 5.8.2. Obtenir des informations sur les caractéristiques démographiques des ensembles de données de formation, de test et d'évaluation du produit, afin de s'assurer qu'ils ont inclus un éventail suffisamment diversifié d'individus pour le contexte prévu.
>
> 5.8.3. Assurer que le produit a été conçu et testé d'une manière compatible avec l'utilisation prévue ; par exemple, un produit de reconnaissance faciale conçu pour la vérification dans un environnement bien éclairé et contrôlé peut ne pas être suffisamment précis pour l'identification dans un environnement très dynamique, sombre ou à angle élevé (p. ex. une foule en mouvement).
>
> 5.8.4. En faisant appel à un prestataire de services tiers, il faut mettre en place un cadre solide de gestion des risques liés aux fournisseurs pour évaluer la conformité au principe 5.10, ainsi que des protections contractuelles associées pour garantir que la conformité sera permanente.

5.9. Les organisations doivent établir des procédures et des politiques pour identifier, atténuer, répondre et notifier à l'autorité de protection des données compétente toute violation de données liée au système de reconnaissance faciale.

5.10. Les organisations doivent s'assurer que les tiers qu'elles engagent respectent les principes énoncés dans le présent document (dans la mesure où ils s'appliquent au tiers), ainsi que toute exigence législative.

6. PRINCIPES DE PROTECTION DES DONNÉES : L'utilisation de la reconnaissance faciale doit respecter tous les principes de protection des données, notamment ceux mentionnés ci-dessus.

Les organisations doivent tenir compte de *tous* les principes de protection des données tout au long du cycle de vie d'un système de reconnaissance faciale. En plus de ceux décrits ci-dessus, ceux-ci comprennent :

6.1. Le respect de la vie privée dès la conception. (<< Privacy by design >>)

6.1.1. Lors du développement d'un système de reconnaissance faciale, les organisations doivent adopter une approche de protection de la vie privée dès la conception pour s'assurer que des protections sont intégrées dès le départ dans les systèmes de reconnaissance faciale.

6.1.2. Dans la mesure du possible, les organisations doivent éviter le stockage central des modèles biométriques et de toute donnée biométrique brute. Par exemple, dans le cas d'une vérification, la référence biométrique pourrait être stockée sur un dispositif ou un artefact (tel qu'un permis de conduire, un passeport ou un badge d'identification d'employé) détenu par la personne vérifiée. Si les modèles biométriques sont stockés de manière centralisée (lorsque des objectifs spécifiques sont identifiés pour ce faire), ils doivent être protégés par des mesures cryptographiques fortes et appropriées.

6.1.3. Les organisations qui utilisent un système de reconnaissance faciale doivent s'assurer que des mesures de protection appropriées sont appliquées à chaque étape du cycle de vie des informations du système.

6.2. Spécification de l'objectif et limitation de l'utilisation**.**

6.2.1. Les organisations doivent définir clairement les objectifs pour lesquels les systèmes de reconnaissance faciale seront utilisés, et ne pas s'écarter de ces objectifs, sauf autorisation légale.

6.3. Minimisation, conservation et suppression des données.

6.3.1. Les organisations doivent définir des périodes de conservation pour les données biométriques brutes et les modèles biométriques (y compris ceux utilisés comme sondes biométriques ou références biométriques, ou bien, ceux stockés dans des bases de données de référence), et supprimer les modèles biométriques lorsqu'il n'est plus nécessaire de les conserver. Cette période doit tenir compte de la diminution de l'utilité d'un modèle biométrique au fil du temps.

6.3.2. En général, les sondes biométriques qui ne correspondent pas à une référence biométrique doivent être supprimées immédiatement. Une conservation limitée de ces images peut être acceptable si elle est raisonnablement nécessaire, par exemple pour des tests du système qui ont une base juridique claire et sont conformes à la finalité définie pour le traitement en question, lorsqu'une politique de conservation appropriée est en place. Les sondes biométriques appariées peuvent être conservées pendant une période déterminée, mais ne doivent être utilisées qu'en relation avec cette correspondance (c'est-à-dire, à des fins de preuve ou pour permettre aux personnes de contester une décision prise à leur sujet).

6.3.3. Sauf si cela est nécessaire pour un objectif défini (et légal), les organisations doivent éviter de créer un profil des activités ou des comportements d'une personne en corrélant les << matches >> de reconnaissance faciale dans le temps.

6.3.4. Les organisations doivent mettre en place des mécanismes accessibles permettant aux personnes de demander le retrait de leur modèle biométrique

d'une base de données de référence lorsqu'elles ne consentent plus à leur inclusion ou lorsqu'elles ont d'autres motifs légitimes de demander et d'obtenir ce retrait. Ces suppressions doivent être rapides et intervenir le plus tôt possible (et dans les délais légaux).

6.4. Sauvegardes.

6.4.1. Les organisations devraient mettre en œuvre des mesures de sécurité proportionnelles à la grande sensibilité des informations contenues dans un système de reconnaissance faciale.

6.4.2. Les organisations doivent mettre en œuvre les politiques, procédures, normes de sécurité et contrôles nécessaires pour garantir que ni le système de reconnaissance faciale ni les informations personnelles qu'il collecte ou stocke, ne sont soumis à un accès, une utilisation abusive, une interférence ou une perte non autorisée ou non intentionnelle.

6.4.3. Les organisations doivent s'assurer que les systèmes de reconnaissance faciale qu'elles déploient (y compris ceux développés par des tiers) comprennent des mesures appropriées de protection des modèles biométriques et que ces protections sont utilisées. Dans la mesure du possible, ces mesures doivent être conformes aux normes internationales reconnues en matière de protection des données biométriques.

6.4.4. Les organisations devraient revoir régulièrement leurs mesures de sécurité pour s'assurer qu'elles restent suffisantes dans un contexte de menaces en constante évolution.

6.5. Qualité des données.

6.5.1. Les organisations doivent s'assurer que les références biométriques, ainsi que toute autre information personnelle recueillie, générée et stockée par le système de reconnaissance faciale, sont suffisamment précises et à jour pour l'objectif pour lequel elles sont utilisées.

6.5.2. Les organisations doivent prendre des mesures raisonnables pour corriger ou supprimer les informations personnelles qui sont inexactes par rapport à la finalité pour laquelle elles sont utilisées.

6.5.3. Les organisations doivent s'assurer que seules les images bien adaptées pour être utilisées par des systèmes de reconnaissance faciale sont incluses dans les bases de données de référence biométriques ou utilisées comme sondes biométriques. Les évaluations de la qualité doivent, au moins, tenir compte des caractéristiques de l'image, notamment la pose, l'éclairage, l'expression, la taille et la résolution de l'image, ainsi que l'occlusion du visage (c'est-à-dire, la présence de lunettes, de chapeaux, des écharpes, ou de masques).