GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

00727/12/FR
WP 192

Avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles

Adopté le 22 mars 2012

Le groupe de travail a été institué en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale de la justice de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

1. Introduction

Ces dernières années ont été marquées par une croissance rapide de la disponibilité et de la précision de la technologie de reconnaissance faciale. Cette technologie a, par ailleurs, été intégrée dans des services en ligne et mobiles à des fins d'identification, d'authentification/de vérification ou de catégorisation des personnes. Cette technologie, qui relevait naguère de la science-fiction, est désormais mise à la disposition d'organisations tant publiques que privées. Les réseaux sociaux et les téléphones intelligents offrent notamment des exemples de son utilisation dans les services en ligne et mobiles.

La capacité de collecter automatiquement des données et de reconnaître un visage à partir d'une image numérique a été examinée précédemment par le groupe de travail «article 29» dans son document de travail sur la biométrie (WP80) et dans l'avis 03/2012 (WP193) sur les progrès des technologies biométriques, récemment publié. La reconnaissance faciale est envisagée dans le contexte de la biométrie étant donné que, bien souvent, elle contient suffisamment de détails pour rendre possible l'identification univoque d'une personne.

L'avis 03/2012 observe que:

> *«[la biométrie] permet de localiser ou de suivre des personnes ou d'établir leur profil de façon automatisée et, à ce titre, son impact potentiel sur la vie privée et le droit à la protection des données est important.»*

Ce constat est particulièrement vrai dans le cas de la reconnaissance faciale dans les services en ligne et mobiles, dans le cadre desquels des images représentant une personne peuvent être collectées (sans que cette personne le sache nécessairement) et transmises ensuite à un serveur distant pour un traitement ultérieur. Les services en ligne, dont beaucoup appartiennent à des organisations privées qui en assurent l'exploitation, ont constitué de vastes collections d'images mises en ligne par les personnes concernées elles-mêmes. Dans certains cas, ces images peuvent aussi être obtenues illicitement en les récupérant sur d'autres sites publics comme les caches de moteurs de recherche. Les petits appareils mobiles équipés de caméras à haute résolution permettent aux utilisateurs de prendre des photos et de se connecter en temps réel à des services en ligne au moyen de connexions permanentes. De cette façon, les utilisateurs sont en mesure de partager ces images avec d'autres ou de procéder à une identification, authentification/vérification ou catégorisation pour accéder à des informations supplémentaires concernant la personne, connue ou inconnue, qui se tient devant eux.

La reconnaissance faciale dans les services en ligne et mobiles requiert donc une attention particulière du groupe de travail «article 29», étant donné que l'utilisation de cette technologie suscite un grand nombre de préoccupations en matière de protection des données.

Le présent avis a pour objectif d'examiner le cadre juridique et de formuler des recommandations appropriées applicables à la technologie de reconnaissance faciale utilisée dans le contexte des services en ligne et mobiles. Cet avis s'adresse aux autorités législatives européennes et nationales, aux responsables du traitement des données et aux utilisateurs de ces technologies. Il ne s'agit pas ici de répéter les principes auxquels il est fait référence dans l'avis 03/2012, mais plutôt de s'en inspirer dans le contexte des services en ligne et mobiles.

2. Définitions

La technologie de reconnaissance faciale n'est pas nouvelle et il existe toute une série de définitions et d'interprétations de la terminologie. Il est donc utile de définir clairement la technologie dont il est question dans le présent avis.

Image numérique: une image numérique est une représentation sous une forme numérique d'une image en deux dimensions. Toutefois, les récentes avancées dans la technologie de reconnaissance faciale requièrent l'intégration d'images tridimensionnelles, en plus d'images fixes et animées (à savoir des photographies et des vidéos enregistrées et en direct).

Reconnaissance faciale: la reconnaissance faciale est le traitement automatique d'images numériques qui contiennent le visage de personnes à des fins d'identification, d'authentification/de vérification ou de catégorisation ([1]) de ces personnes. Le processus de reconnaissance faciale lui-même se compose de plusieurs sous-processus distincts:

a) acquisition d'image: le processus de capture des traits du visage d'une personne et de leur conversion au format numérique (l'image numérique). Dans le cadre d'un service en ligne ou mobile, l'image peut avoir été acquise dans un système différent, par ex. en prenant une photo avec un appareil numérique, avant de la transférer vers un service en ligne;

b) détection du visage: le processus de détection de la présence d'un visage dans une image numérique et de repérage de la zone concernée;

c) normalisation: le processus d'atténuation des variations entre les régions faciales détectées, par ex. conversion dans des dimensions standard, rotation ou alignement des répartitions des couleurs;

d) extraction de caractéristiques: le processus de détection et de restitution de lectures reproductibles et distinctives de l'image numérique représentant une personne. L'extraction de caractéristiques peut être holistique ([2]), se fonder sur les traits ([3]) ou combiner les deux méthodes ([4]). L'ensemble des caractéristiques essentielles peut être stocké en vue d'une comparaison ultérieure dans un modèle de référence ([5]);

e) inscription: s'il s'agit de la première fois qu'une personne est confrontée au système de reconnaissance faciale, l'image et/ou le modèle de référence peuvent être stockés sous la forme d'enregistrements en vue d'une comparaison ultérieure;

f) comparaison: le processus de mesure de la similarité entre un ensemble de caractéristiques (l'échantillon) et un autre précédemment enregistré dans le système. Les principales finalités de la comparaison sont l'identification et l'authentification/la vérification. Une troisième finalité de la comparaison est la catégorisation, qui

---

1 L'identification, l'authentification/la vérification et la catégorisation sont définies dans l'avis 03/2012.

2 Extraction holistique de caractéristiques: une représentation mathématique de l'image entière, telle qu'elle résulte de l'analyse des composantes principales.

3 Extraction de caractéristiques fondée sur les traits: identification des localisations de traits spécifiques du visage, comme les yeux, le nez et la bouche.

4 Aussi appelée méthode d'extraction hybride de caractéristiques.

5 Le modèle est défini dans l'avis 03/2012 comme des «*caractéristiques essentielles extraites de la forme brute des données biométriques (par ex., mesures faciales à partir d'une image) et enregistrées en vue d'un traitement ultérieur, plutôt que les données brutes elles-mêmes.*»

consiste à extraire des caractéristiques d'une image représentant une personne en vue de classer cette personne dans une ou plusieurs grandes catégories (par ex. l'âge, le sexe, la couleur des vêtements, etc.). Dans le cas d'un système de catégorisation, il n'est pas nécessaire de prévoir un processus d'inscription.

3. Exemples de reconnaissance faciale dans le cadre de services en ligne et mobiles

La reconnaissance faciale peut être intégrée dans les services en ligne et mobiles de plusieurs façons différentes et à des fins diverses. Dans le cadre du présent avis, le groupe de travail «article 29» retient un certain nombre d'exemples différents dans le but d'apporter un contexte supplémentaire à l'analyse juridique et d'inclure l'utilisation de la reconnaissance faciale à des fins d'identification, d'authentification/de vérification et de catégorisation.

3.1. La reconnaissance faciale comme moyen d'identification

Exemple 1: un service de réseautage social (SRS) ([6]) permet à ses utilisateurs d'associer une image numérique à leur profil. En outre, les utilisateurs ont la possibilité de mettre en ligne des images qu'ils partagent avec d'autres utilisateurs, enregistrés ou non. Les utilisateurs enregistrés peuvent identifier et marquer manuellement d'autres personnes (qu'il s'agisse ou non d'utilisateurs enregistrés) sur les images qu'ils mettent en ligne. Ces marquages peuvent être visibles pour leur créateur, partagés avec un groupe d'amis plus large ou avec tous les utilisateurs enregistrés ou non. Le SRS est en mesure d'utiliser les images marquées pour créer un modèle pour chaque utilisateur enregistré et, grâce à un système de reconnaissance faciale, proposer automatiquement de marquer les nouvelles images lorsqu'elles sont mises en ligne.

Ces images représentant des personnes qui sont rendues publiques par des utilisateurs pourraient ensuite être consultées et mises en cache par un moteur de recherche sur l'internet. Le moteur de recherche pourrait développer ses fonctions de recherche en permettant aux utilisateurs de charger l'image d'une personne et en affichant les résultats les plus ressemblants, avec un lien vers la page de profil du SRS. L'image de la requête pourrait être prise directement à l'aide de l'appareil photo d'un téléphone intelligent.

3.2. La reconnaissance faciale comme moyen d'authentification/de vérification

Exemple 2: un système de reconnaissance faciale est utilisé à la place du nom d'utilisateur/mot de passe pour contrôler l'accès à un service ou un dispositif en ligne ou mobile. Lors de l'inscription, un appareil photo équipant le dispositif est utilisé pour acquérir une image représentant un utilisateur autorisé du dispositif et un modèle de référence est créé, puis sauvegardé sur le dispositif ou à distance par le service en ligne. Pour accéder au service ou au dispositif, la personne est de nouveau photographiée et son visage est comparé avec l'image de référence. L'accès est autorisé si le système établi une correspondance positive.

[6] Les services de réseautage social sont définis, de manière générale, dans l'avis 05/2009 sur les réseaux sociaux en ligne, comme «des plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs».

3.3. La reconnaissance faciale comme moyen de catégorisation

Exemple 3: le SRS décrit dans l'exemple 1 peut accorder sous licence l'accès à sa bibliothèque d'images à une société tierce qui exploite un service de reconnaissance faciale en ligne. Le service autorise les clients de la société tierce à intégrer la technologie de reconnaissance faciale dans d'autres produits. Cette fonctionnalité permet à ces autres produits de soumettre des images de personnes dans le but de détecter et de catégoriser leurs visages en fonction d'un ensemble de critères prédéfinis, par ex. l'âge probable, le sexe et l'humeur.

Exemple 4: une console de jeux utilise un système de contrôle gestuel où les mouvements de l'utilisateur sont détectés de façon à contrôler le jeu. La/les caméra(s) utilisée(s) par le système de contrôle gestuel partage(nt) les images des personnes avec un système de reconnaissance faciale, qui prédit l'âge probable, le sexe et l'humeur des joueurs. Les données, couplées à celles obtenues au moyen d'autres facteurs multimodaux, permettent d'altérer le déroulement du jeu pour enrichir l'expérience de l'utilisateur ou de changer l'environnement pour refléter le profil supposé de l'utilisateur. De façon similaire, un système pourrait classer ses utilisateurs afin de leur autoriser/refuser l'accès à certains contenus en fonction de leur âge ou d'afficher dans le jeu des publicités ciblées.

4. Cadre juridique

Le cadre juridique applicable pour la reconnaissance faciale est la directive sur la protection des données (95/46/CE), qui a été examinée à cet égard dans l'avis 03/2012. Cette section a seulement pour but de donner un résumé du cadre juridique dans le contexte de la reconnaissance faciale dans le cadre des services en ligne et mobiles, sur la base des exemples fournis dans la section 3. D'autres exemples de reconnaissance faciale sont envisagés dans l'avis 03/2012.

4.1. Les images numériques en tant que données à caractère personnel

Quand une image numérique contient le visage, clairement visible, d'une personne qui peut ainsi être identifiée, elle peut être considérée comme relevant des données à caractère personnel. Cela déprendra de plusieurs paramètres comme la qualité de l'image ou la perspective. Dans le cas de scènes où figurent des personnes vues de loin ou lorsque les visages sont flous, il est peu probable que ces images soient considérées comme des données à caractère personnel. Il est important, cependant, de noter que les images numériques peuvent contenir des données à caractère personnel concernant plus d'une personne (ainsi, dans l'exemple 4, plusieurs joueurs peuvent apparaître dans le champ de prise de vue) et la présence d'autres personnes sur une photo peut suggérer une relation existante.

L'avis 04/2007 sur le concept de données à caractère personnel rappelle que si des données ont trait «*aux caractéristiques ou au comportement d'une personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée*», elles sont aussi considérées comme des données à caractère personnel.

Par définition, un modèle de référence créé à partir de l'image d'une personne relève aussi des données à caractère personnel, dès lors qu'il contient un ensemble de caractéristiques distinctives du visage, qui sont associées à un individu en particulier et conservées pour servir de référence en vue d'une comparaison ultérieure dans un processus d'identification et d'authentification/de vérification.

Un modèle ou un ensemble de caractéristiques distinctives qui sert uniquement dans un système de catégorisation ne devrait pas, en général, contenir suffisamment d'informations

pour identifier une personne. Il devrait contenir seulement des informations suffisantes pour procéder au classement dans une catégorie (par ex., homme ou femme). Dans ce cas, il ne s'agirait pas de données à caractère personnel, pour autant que le modèle (ou le résultat) ne soit pas associé au dossier d'une personne, à son profil ou à l'image originale (qui reste considérée comme relevant des données à caractère personnel).

De plus, étant donné que les images numériques représentant des personnes et les modèles se rapportent à «*des propriétés biologiques, des aspects comportementaux, des caractéristiques physiologiques, des caractéristiques vivantes ou des actions reproductibles lorsque ces caractéristiques et/ou actions sont à la fois propres à cette personne physique et mesurables* ([7])», elles doivent être considérées comme des données biométriques.

4.2. Les images numériques en tant que catégories particulières de données à caractère personnel

Les images numériques représentant des personnes peuvent aussi, dans certains cas, être considérées comme relevant d'une catégorie particulière de données à caractère personnel ([8]). Lorsque les images numériques en question ou les modèles font notamment l'objet d'un traitement complémentaire visant à obtenir des catégories particulières de données, il sera certainement considéré que ces images entrent dans cette catégorie. C'est le cas, par exemple, si elles sont destinées à être utilisées pour en extraire des informations relatives à l'origine ethnique, à la religion ou à la santé des personnes concernées.

4.3. Le traitement des données à caractère personnel dans le contexte d'un système de reconnaissance faciale

Ainsi qu'il a été expliqué précédemment, la reconnaissance faciale s'appuie sur plusieurs stades de traitement automatisé. La reconnaissance faciale constitue donc une forme automatisée de traitement de données à caractère personnel, y compris des données biométriques.

Du fait de l'utilisation de données biométriques, les systèmes de reconnaissance faciale peuvent être soumis, selon les États membres, à des contrôles supplémentaires ou à d'autres dispositions législatives, par exemple en matière d'autorisation préalable ou de droit du travail. L'utilisation de la biométrie dans le contexte de l'emploi est examinée de façon plus approfondie dans l'avis 03/2012.

4.4. Le responsable du traitement des données

Pour reprendre les exemples fournis, les responsables du traitement des données seront généralement les propriétaires de site web et/ou les prestataires de services en ligne, ainsi que les opérateurs d'applications mobiles qui pratiquent la reconnaissance faciale dans la mesure où ils déterminent les finalités et/ou les moyens du traitement ([9]). Cela englobe la conclusion formulée dans l'avis 05/2009 sur les réseaux sociaux en ligne, qui indique que «les fournisseurs de SRS sont responsables du traitement des données conformément à la directive sur la protection des données».

4.5. Motif légitime

La directive 95/46/CE énonce les conditions à respecter par le traitement des données à caractère personnel. Il en ressort que le traitement doit d'abord être conforme aux exigences de qualité des données (article 6). Dans le cas présent, les images numériques représentant

---

[7] Définition des données biométriques provenant de l'avis 03/2012.

[8] La jurisprudence de certains pays a classé les images numériques représentant des visages parmi les catégories particulières de données – LJN BK6331, Haute Cour des Pays-Bas, 23 mars 2010.

[9] Voir l'avis 01/2010 concernant les notions de «responsable» et de «sous-traitant».

des personnes et les modèles correspondants doivent être «pertinents» et «non excessifs» au regard des finalités du traitement de reconnaissance faciale. De plus, le traitement ne peut être effectué que si l'un des critères spécifiés à l'article 7 est satisfait.

En raison des risques particuliers associés aux données biométriques, le consentement informé de la personne sera donc requis avant le commencement du traitement des images numériques à des fins de reconnaissance faciale. Toutefois, dans certains cas, le responsable du traitement des données peut temporairement être amené à effectuer certaines opérations préliminaires de reconnaissance faciale dans le but, précisément, de vérifier si un utilisateur a donné ou non son consentement, qui doit servir de base juridique au traitement. Ce traitement initial (à savoir, acquisition d'image, détection du visage, comparaison, etc.) peut dans ce cas s'appuyer sur une base juridique distincte, notamment l'intérêt légitime du responsable du traitement des données à se conformer aux règles applicables en matière de protection des données. Les données traitées durant ces opérations devraient uniquement être utilisées dans le but strictement limité de vérifier le consentement de l'utilisateur et devraient donc être supprimées immédiatement après usage.

Dans l'exemple 1, le responsable du traitement des données a déterminé que toutes les nouvelles images mises en ligne par des utilisateurs enregistrés du SRS devraient faire l'objet d'une détection du visage, d'une extraction des caractéristiques et d'une comparaison. Il n'y aura de correspondances possibles, et donc de propositions automatiques de marquage des nouvelles images, qu'avec les utilisateurs enregistrés pour qui un modèle de référence est inscrit dans la base de données d'identification. Si le consentement de la personne devait être considéré comme la seule base légitime acceptable pour tout traitement, le service entier serait bloqué, dans la mesure où, par exemple, il n'est pas possible d'obtenir le consentement d'utilisateurs non enregistrés dont les données à caractère personnel pourraient être traitées aux stades de la détection du visage et de l'extraction des caractéristiques. De plus, il ne serait pas possible de faire la distinction entre les visages des utilisateurs enregistrés qui ont ou n'ont pas marqué leur consentement sans effectuer au préalable une reconnaissance faciale. Ce n'est qu'après l'identification (ou l'échec de l'identification) qu'un responsable du traitement des données peut déterminer s'il dispose ou non du consentement nécessaire pour ce traitement spécifique.

Avant de mettre en ligne des images sur le SRS, un utilisateur enregistré doit être clairement informé que ces images seront soumises à un système de reconnaissance faciale. Surtout, les utilisateurs enregistrés doivent aussi avoir la possibilité d'indiquer s'ils consentent ou non à ce que leur modèle de référence soit inscrit dans la base de données d'identification. Il ne sera dès lors pas proposé automatiquement de marquer des images avec les noms des utilisateurs non enregistrés et des utilisateurs enregistrés qui n'auront pas consenti au traitement, étant donné que les images les représentant ne produiront aucune correspondance.

Le consentement donné par l'utilisateur qui met une image en ligne ne devrait pas être confondu avec la base légitime qu'il est nécessaire d'obtenir pour le traitement de données à caractère personnel d'autres personnes susceptibles d'apparaître sur l'image. À cet effet, le responsable du traitement des données pourra s'appuyer sur un motif légitime différent pour procéder aux stades intermédiaires du traitement (détection du visage, normalisation et comparaison), effectués dans l'intérêt légitime du responsable du traitement des données, pour autant que des restrictions et des contrôles suffisants soient en place afin de protéger les libertés et les droits fondamentaux des personnes concernées, autres que l'utilisateur qui met l'image en ligne. Ces contrôles incluraient la vérification qu'aucune donnée résultant du traitement n'est conservée dès lors que ce traitement n'a pas produit de correspondance (à savoir que tous les modèles et les données associées ont bien été supprimés). Le responsable

du traitement des données pourra aussi envisager de fournir des outils aux utilisateurs qui mettent en ligne des images pour leur permettre de «flouter» les visages des personnes pour lesquelles aucune correspondance n'a été trouvée dans la base de données de référence. L'inscription du modèle représentant une personne dans une base de données d'identification (de façon à permettre ultérieurement l'obtention d'une correspondance et des propositions de marquage) ne serait possible qu'avec le consentement informé de la personne concernée.

Dans l'exemple 2, il existe, de toute évidence, une possibilité d'obtenir le consentement de la personne à qui l'accès est autorisé lors du processus d'inscription. Pour que ce consentement soit valable, un autre système de contrôle d'accès, tout aussi sécurisé, doit être mis en place (comme l'authentification au moyen d'un mot de passe sûr). Cette autre option, respectueuse de la vie privée, devrait être proposée par défaut. De cette façon, quand un utilisateur se présente devant une caméra connectée au dispositif dans le but explicite d'obtenir l'accès à ce dispositif, nous pouvons considérer que cette personne a marqué son consentement pour le traitement résultant des données faciales à des fins d'authentification, même si cette personne n'est pas un utilisateur autorisé du dispositif. Le niveau d'information fourni devra cependant être suffisant pour garantir la validité du consentement.

L'exploitation ultérieure de la bibliothèque photographique du SRS décrite dans l'exemple 3 constituerait un cas manifeste de violation du principe de limitation des finalités et il faut donc qu'un consentement valable soit obtenu avant l'introduction d'une telle fonctionnalité, en indiquant clairement que ce traitement des images sera effectué. C'est aussi le cas du moteur de recherche décrit dans l'exemple 1. Les images collectées par le moteur de recherche ont été affichées dans un but de consultation et non à des fins d'acquisition par un système de reconnaissance faciale. L'exploitant du moteur de recherche devrait être tenu de demander leur consentement aux personnes concernées avant de procéder à leur inscription dans le second système de reconnaissance faciale.

Il en irait de même aussi dans l'exemple 4, étant donné que l'utilisateur ne s'attend pas nécessairement à ce que les images acquises à des fins de contrôle gestuel fassent l'objet d'un traitement complémentaire. Si le responsable du traitement des données demande le consentement des utilisateurs en vue d'un traitement à plus long terme (dans le temps ou d'une partie à l'autre du jeu), il doit leur rappeler régulièrement que le système est activé et veiller à ce que le traitement soit désactivé par défaut.

L'avis 15/2011 sur la définition du consentement prend en considération la qualité, l'accessibilité et la visibilité des informations relatives au traitement de données à caractère personnel. Il précise notamment que:

> *«les informations doivent être communiquées directement à la personne concernée. Il ne suffit pas que les informations soient "disponibles" quelque part.»*

Il convient donc que les informations relatives à la fonction de reconnaissance faciale d'un service en ligne ou mobile ne soient pas cachées, mais au contraire présentées de façon aisément accessible et compréhensible. Il faut notamment veiller à ce que les caméras elles-mêmes ne fonctionnent pas de manière dissimulée. Les responsables du traitement des données doivent tenir compte des attentes raisonnables du public et répondre de façon appropriée à ses préoccupations lorsqu'ils mettent en place une technologie de reconnaissance faciale.

Dans ce contexte, le consentement au processus d'inscription ne saurait découler de l'acception par l'utilisateur des conditions générales du service de base, à moins que la finalité première dudit service ne soit censée inclure la reconnaissance faciale. La raison en est que, dans la plupart des cas, l'inscription constituera une fonctionnalité supplémentaire et ne sera pas directement liée au fonctionnement du service en ligne ou mobile. Les utilisateurs ne s'attendent pas nécessairement à ce que cette fonctionnalité soit activée quand ils ont recours au service. Il convient donc de donner explicitement aux utilisateurs la possibilité de marquer leur consentement à l'égard de cette fonctionnalité, lors de leur enregistrement ou à une date ultérieure, selon le moment où la fonctionnalité est introduite.

Pour que le consentement puisse être considéré comme valable, des informations adéquates sur le traitement des données doivent avoir été communiquées. Les utilisateurs devraient toujours avoir la possibilité de retirer leur consentement de façon simple. Dès le retrait du consentement, le traitement des images à des fins de reconnaissance faciale devrait cesser immédiatement.

5. Risques spécifiques et recommandations

Les risques d'atteinte à la vie privée présentés par un système de reconnaissance faciale dépendront entièrement du type de traitement appliqué et des finalités. Il existe cependant certains risques qui méritent davantage d'attention à des stades spécifiques de la reconnaissance faciale. La section suivante souligne les principaux risques et formule des recommandations de meilleures pratiques.

5.1. Traitement illicite à des fins de reconnaissance faciale

Dans un environnement en ligne, l'acquisition d'images par le responsable du traitement des données peut s'opérer de diverses façons, selon qu'elles proviennent, par exemple, des utilisateurs du service en ligne ou mobile, de leurs amis et collègues ou d'un tiers. Les images peuvent contenir les visages des utilisateurs eux-mêmes et/ou d'autres utilisateurs enregistrés ou non, ou avoir été prises à l'insu de la personne concernée. Quels que soient les moyens par lesquels ces images peuvent être obtenues, il est nécessaire de disposer d'une base juridique pour procéder à leur traitement.

Recommandation 1: Si le responsable du traitement des données effectue directement l'acquisition d'image (comme dans les exemples 2 et 4), il lui incombe de veiller à obtenir le consentement valable des personnes concernées avant l'acquisition d'images et d'indiquer de façon suffisamment claire quand une caméra est utilisée à des fins de reconnaissance faciale.

Recommandation 2: Si des personnes prennent des images numériques et les envoient à des services en ligne et mobiles à des fins de reconnaissance faciale, les responsables du traitement des données doivent s'assurer que les utilisateurs qui mettent en ligne les images ont consenti au traitement qui peut être effectué aux fins de la reconnaissance faciale.

Recommandation 3: Si les responsables du traitement des données obtiennent des images numériques représentant des personnes auprès de tiers (par ex. des images copiées sur un site web ou achetées à un autre responsable du traitement des données), ils doivent en examiner soigneusement la source, vérifier le contexte dans lequel a eu lieu l'acquisition des images originales et s'assurer que le traitement n'a pas été effectué sans le consentement préalable des personnes concernées.

Recommandation 4: Les responsables du traitement des données doivent veiller à ce que les images numériques et les modèles soient utilisés uniquement dans le but spécifié pour lequel les images ont été fournies. Il leur revient de mettre en place des contrôles techniques en vue de réduire le risque que les images numériques soient traitées ultérieurement par des tiers à des fins pour lesquelles l'utilisateur n'a pas marqué son consentement. Les responsables du traitement des données devraient mettre à la disposition des utilisateurs des outils permettant de contrôler la visibilité des images qu'ils ont mises en ligne, en proposant par défaut un accès restreint.

Recommandation 5: Les responsables du traitement des données doivent veiller à ne traiter les images numériques représentant des personnes qui ne sont pas des utilisateurs enregistrés ou qui n'ont pas marqué leur consentement d'une autre façon, que dans la mesure où un tel traitement relève d'un intérêt légitime. Il peut s'agir notamment, dans le cas de l'exemple 1, d'une mesure visant à arrêter le traitement et à supprimer toutes les données si aucune correspondance n'est trouvée.

Atteinte à la sécurité des données lors du transfert

Dans le cas de services en ligne et mobiles, il est probable que des données seront transférées entre l'acquisition d'images et les autres stades de traitement (par ex., mise en ligne d'une image provenant d'un appareil photo sur un site web à des fins d'extraction des caractéristiques et de comparaison).

Recommandation 6: Le responsable du traitement des données doit prendre des mesures appropriées pour garantir la sécurité du transfert des données. Ces mesures peuvent notamment consister à crypter les canaux de communication ou l'image acquise elle-même. Dans la mesure du possible, et en particulier dans le cas d'un processus d'authentification/de vérification, un traitement local devrait être privilégié.

5.2. Détection du visage, normalisation, extraction de caractéristiques

Minimisation des données

Les modèles créés par un système de reconnaissance faciale peuvent contenir plus de données que nécessaire pour la réalisation des finalités spécifiées.

Recommandation 7: Les responsables du traitement des données doivent veiller à ce que les données extraites d'une image numérique pour constituer un modèle ne soient pas excessives et ne contiennent que les informations requises aux fins spécifiées, de façon à éviter tout autre traitement éventuel. Les modèles ne devraient pas être transférables entre différents systèmes de reconnaissance faciale.

Atteinte à la sécurité des données lors du stockage

Il est probable que les processus d'identification et d'authentification/de vérification nécessiteront le stockage du modèle à des fins de comparaison ultérieure.

Recommandation 8: Le responsable du traitement des données doit privilégier l'endroit le plus approprié pour le stockage des données. Il peut s'agir de l'appareil de l'utilisateur ou des systèmes du responsable du traitement des données. Le responsable du traitement des données doit prendre des mesures appropriées pour garantir la sécurité des données conservées. Ces mesures peuvent notamment consister à crypter le modèle. Il ne devrait

pas être possible d'accéder sans autorisation au modèle ou à l'endroit où il est stocké. Lorsque la reconnaissance faciale est utilisée à des fins de vérification, notamment, des techniques de cryptage biométrique peuvent être utilisées; avec ces techniques, la clé cryptographique est directement liée aux données biométriques et elle n'est recréée que si l'échantillon biométrique correct est présenté en direct lors de la vérification, sans qu'aucune image ni aucun modèle ne soit stocké (formant ainsi un type de «biométrie intraçable»).

Accès des personnes concernées

Recommandation 9: Le responsable du traitement des données devrait mettre à la disposition des personnes concernées des mécanismes appropriés pour exercer, le cas échéant, leur droit d'accès aussi bien aux images originales qu'aux modèles créés dans le contexte de la reconnaissance faciale.

Fait à Bruxelles, le 22 mars 2012

Pour le groupe de travail
Le président
Jacob KOHNSTAMM