EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

HELPING TO MAKE FUNDAMENTAL RIGHTS A REALITY FOR EVERYONE IN THE EUROPEAN UNION

Technologie de reconnaissance faciale: considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi

Focus de la FRA

La technologie de reconnaissance faciale permet de comparer des images faciales numériques afin de déterminer s'il s'agit d'une seule et même personne. La comparaison d'images obtenues à partir de caméras vidéo avec des images stockées dans des bases de données est appelée «technologie de reconnaissance faciale en temps réel». Les exemples d'autorités répressives nationales de l'Union européenne (UE) utilisant cette technologie sont rares, mais plusieurs d'entre elles testent actuellement son potentiel. Le présent document examine donc les implications en matière de droits fondamentaux de l'utilisation de la technologie de reconnaissance faciale en temps réel, en mettant l'accent sur son utilisation à des fins répressives et de gestion des frontières.

Le droit de l'UE reconnaît comme «données sensibles» les images faciales des personnes, qui sont une forme de données biométriques. Mais ces images sont également assez faciles à capturer dans les lieux publics. Malgré la précision croissante des correspondances, le risque d'erreur demeure réel, en particulier pour certains groupes minoritaires. En outre, les personnes dont les images sont capturées et traitées pourraient ne pas en être informées et, par conséquent, ne pas être en mesure de s'opposer à d'éventuelles utilisations abusives. Le document présente et analyse ces considérations ainsi que d'autres défis en matière de droits fondamentaux liés à la mise en place, par les autorités publiques, de la technologie de reconnaissance faciale en temps réel à des fins répressives. Il présente aussi succinctement les mesures à adopter pour éviter les violations des droits.

Table des matières

1. Technologie de reconnaissance faciale et droits fondamentaux: présentation du contexte

Ce document de réflexion explore les implications en matière de droits fondamentaux qui devraient être prises en compte lors du développement, du déploiement, de l'utilisation et de la réglementation des technologies de reconnaissance faciale. Il s'appuie sur des analyses et des données récentes (section 3 et section 4) et sur les résultats d'entretiens menés avec des experts et des représentants des autorités nationales qui testent les technologies de reconnaissance faciale (section 5) ([1]). Les dernières sections (section 6 et section 7) fournissent une brève analyse juridique résumant le droit applicable de l'Union européenne (UE) et du Conseil de l'Europe.

Ce document fait partie d'un projet de recherche plus vaste de l'Agence des droits fondamentaux de l'Union européenne (FRA) sur l'intelligence artificielle, les mégadonnées et les droits fondamentaux ([2]). Il s'agit du premier document portant sur les utilisations de la technologie de reconnaissance faciale. Il s'appuie sur les travaux antérieurs approfondis de l'Agence sur les implications en matière de droits fondamentaux de l'utilisation de données biométriques dans les systèmes d'information à grande échelle de l'UE dans le domaine de la migration, de l'asile et des frontières ([3]).

La technologie de reconnaissance faciale permet l'identification automatique d'une personne en faisant correspondre deux ou plusieurs visages présents dans des images numériques. Pour ce faire, elle détecte et mesure diverses caractéristiques faciales, les extrait de l'image, puis les compare à des caractéristiques d'autres visages ([4]).

Dans le secteur privé, la technologie de reconnaissance faciale est largement utilisée pour la publicité, le marketing et d'autres fins, le profilage et l'identification des clients individuels permettant de prédire leurs préférences pour des produits sur la base de leurs expressions faciales ([5]). Parmi d'autres exemples du secteur privé, citons: un club de football qui utilise la technologie de reconnaissance faciale dans son stade pour identifier les personnes non autorisées à assister aux matchs du club ([6]); l'utilisation de la technologie de reconnaissance faciale pour analyser les expressions faciales des candidats à l'embauche lors d'entretiens ([7]); et les grandes entreprises de l'internet et des réseaux sociaux, telles que Facebook, qui déploient des technologies de reconnaissance faciale pour améliorer leurs systèmes, en procédant à un étiquetage des visages ([8]).

L'évolution récente de la technologie de reconnaissance faciale fondée sur l'intelligence artificielle (IA) n'intéresse pas seulement le secteur privé. Elle ouvre également de nouvelles possibilités pour l'administration publique, notamment les services répressifs et de gestion des frontières. L'augmentation considérable de la précision obtenue au cours des dernières années a incité de nombreuses autorités publiques et entreprises privées du monde entier à commencer à utiliser, tester ou planifier l'utilisation des technologies de reconnaissance faciale.

Cela a donné lieu à un débat intense sur son impact potentiel sur les droits fondamentaux. Par exemple, l'utilisation à grande échelle de la technologie de reconnaissance faciale combinée à des caméras de surveillance en République populaire de Chine a suscité de nombreuses discussions et préoccupations quant aux violations potentielles des droits de l'homme, notamment en ce qui concerne

([1]) Entre mars et mai 2019, la FRA a mené onze entretiens dans des États membres de l'UE, tels que l'Allemagne, la France et le Royaume-Uni, afin de mieux comprendre les tests actuels et l'utilisation potentielle de la technologie de reconnaissance faciale.

([2]) Les documents publiés jusqu'à présent dans le cadre du projet de recherche sont les suivants: FRA (2018), *#BigData: Discrimination in data-supported decision making*, Office des publications, Luxembourg, mai 2018; FRA (2019), *Data quality and artificial intelligence — mitigating bias and error to protect fundamental rights*, Office des publications, Luxembourg, juin 2019. Pour en savoir plus sur le projet, consulter la page web de la FRA dédiée au projet.

([3]) Voir, par exemple, FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Office des publications, Luxembourg, mars 2018; FRA (2018), *Interoperability and fundamental rights implications — Opinion of the European Union Agency for Fundamental Rights*, avis de la FRA 1/2018 (Interopérabilité), Vienne, 11 avril 2018.

([4]) Pour plus de détails sur le fonctionnement de la technologie de reconnaissance faciale, voir, par exemple, Introna, L., et Nissenbaum, H. (2010), *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, document de travail 2010/030 de la Lancaster University Management School.

([5]) Voir, par exemple, Italy, *Garante per la protezione dei dati personali, Installazione di apparati promozionali del tipo «digital signage» (definiti anche Totem) presso una stazione ferroviaria*, 21 décembre 2017.

([6]) Voir European Digital Rights (EDRi), *Danish DPA approves Automated Facial Recognition*, 19 juin 2019.

([7]) Voir *The Telegraph*, «AI used for first time in job interviews in UK to find best applicants», 27 septembre 2019.

([8]) Voir Wired, *Facebook can now find your face, even when it's not tagged*, 19 décembre 2017.

la détection des membres de certaines minorités ethniques ([9]). À la suite d'une utilisation accrue de la reconnaissance faciale aux États-Unis, une enquête nationale publiée en septembre 2019 par le Pew Research Center révèle que, si un peu plus d'un Américain sur deux (56 %) fait confiance aux services répressifs pour utiliser ces technologies de manière responsable, une part plus faible de la population déclare accorder en revanche sa confiance aux entreprises technologiques (36 %) ou aux annonceurs (18 %) ([10]).

Dans un certain nombre de pays européens, les technologies de reconnaissance faciale sont testées ou utilisées dans différents contextes, que ce soit dans la sphère privée ou publique. Le présent document porte sur un aspect spécifique: la comparaison d'images obtenues à partir de caméras vidéo avec des images faciales stockées dans des bases de données (par exemple une liste de surveillance) à des fins répressives et de gestion des frontières. Souvent appelée «technologie de reconnaissance faciale en temps réel», elle constitue une forme spécifique de vidéosurveillance — et les analyses de ses implications en matière de droits fondamentaux font défaut.

À ce jour, il existe peu d'exemples d'utilisation par les autorités répressives nationales de la technologie de reconnaissance faciale en temps réel en Europe.

Définition des autorités répressives

Le terme «autorités répressives» se réfère aux «autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces».

Source: Directive en matière de protection des données dans le domaine répressif, article 1er, paragraphe 1.

Le Royaume-Uni a testé la technologie de reconnaissance faciale pour identifier en temps réel les personnes à l'aide de caméras installées dans les rues. D'autres États membres de l'UE se sont engagés à procéder à des tests et ont planifié d'utiliser la technologie de reconnaissance faciale. Par exemple, en Hongrie, un projet appelé «Szitakötő» (libellule) prévoit de déployer 35 000 caméras dotées de capacités de reconnaissance faciale à Budapest et dans tout le pays. Les caméras captureront les plaques d'immatriculation et les images faciales des conducteurs afin de maintenir l'ordre public, notamment la sécurité routière ([11]). Le gouvernement tchèque a approuvé un plan visant à étendre l'utilisation de caméras de reconnaissance faciale — de 100 à 145 — à l'aéroport international de Prague ([12]). En Allemagne et en France, la police a effectué de nombreux tests. L'autorité suédoise de protection des données a récemment autorisé l'utilisation de la technologie de reconnaissance faciale par la police pour aider à identifier des suspects criminels, ce qui permet à la police de comparer des images faciales provenant d'enregistrements de vidéosurveillance à une liste de surveillance contenant plus de 40 000 photos ([13]).

Le traitement des images faciales devrait être introduit plus systématiquement dans les systèmes d'information à grande échelle utilisés au niveau de l'UE dans le domaine de l'asile, de la migration et de la sécurité ([14]). Comme indiqué à la section 5, la plupart de ces systèmes européens traiteront à l'avenir les images faciales, une fois que les étapes juridiques et techniques nécessaires seront terminées. Ces images seront prises dans des environnements contrôlés — par exemple dans des postes de police ou à des points de passage frontaliers, où la qualité des images est supérieure à celle des caméras de vidéosurveillance. La FRA a déjà attiré l'attention, dans des publications antérieures, sur les risques en matière de droits fondamentaux liés au traitement des images faciales dans de tels systèmes d'information ([15]).

Malgré la forte pression exercée par l'industrie privée et d'autres parties prenantes pour utiliser la technologie de reconnaissance faciale, une forte opposition s'est manifestée, invoquant des défauts. Cela a conduit, par exemple, le plus grand fournisseur mondial de caméras piétons pour la police (Axon) à annoncer cette année qu'il ne

([9]) Conseil des droits de l'homme (2019), *Surveillance et droits de l'homme — Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, David Kaye, A/HRC/41/35; *New York Times*, «One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority», 14 avril 2019.

([10]) Pew Research Center (2019), *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, 5 septembre 2019.

([11]) Voir, par exemple, *Hungary Today*, «CCTV: Is it Big Brother or the Eye of Providence?», 18 janvier 2019. Concernant les multiples préoccupations juridiques — principalement liées à la protection des données — soulevées par l'autorité hongroise de protection des données dans le cadre de ce projet, voir la lettre disponible sur le site web de l'autorité.

([12]) Voir Biometriupdate.com, «Expanded use of facial recognition at Prague international airport approved», 10 mars 2019.

([13]) Voir, par exemple, Datainspektionen, «Polisen får använda ansiktsigenkänning för att utreda brott», 24 octobre 2019, et NewEurope, «Sweden authorises the use of facial recognition technology by the police», 28 octobre 2019.

([14]) Pour de plus amples informations, voir le tableau 2.

([15]) FRA (2018), *Interoperability and fundamental rights implications — Opinion of the European Union Agency for Fundamental Rights*, avis de la FRA 1/2018 (Interopérabilité), Vienne, 11 avril 2018; FRA (2018), *The revised Visa Information System and its fundamental rights implication — Opinion of the European Union Agency for Fundamental Rights*, avis de la FRA 2/2018 (VIS), Vienne, 30 août 2018; FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Office des publications, Luxembourg, mars 2018; FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Office des publications, Luxembourg, juin 2017.

déploierait la technologie de reconnaissance faciale dans aucun de ses produits, car elle est trop peu fiable pour le travail des autorités répressives et «pourrait exacerber les inégalités existantes dans les activités de la police, par exemple en pénalisant les communautés noires ou LGBTQ» ([16]). Dans le même ordre d'idées, la ville de San Francisco aux États-Unis, parmi d'autres villes, a interdit l'utilisation de cette technologie en raison de son caractère excessivement intrusif dans la vie privée des personnes et pour éviter d'éventuels abus par les services répressifs ([17]).

Dans ce contexte, un certain nombre de questions se posent du point de vue des droits fondamentaux: cette technologie est-elle appropriée à des fins répressives et de gestion des frontières — par exemple lorsqu'elle est utilisée pour identifier des personnes recherchées par les autorités répressives? Quels sont les droits fondamentaux les plus affectés par le déploiement de cette technologie — et quelles mesures les autorités publiques doivent-elles prendre pour garantir que ces droits ne sont pas violés?

Le risque d'erreurs dans la correspondance des visages est la préoccupation la plus fréquemment exprimée au sujet des droits fondamentaux. Toutefois, les préoccupations en matière de droits fondamentaux découlent également de la position de faiblesse des personnes dont les images faciales sont capturées et traitées. Les droits fondamentaux concernés sont, entre autres, la dignité humaine, le droit au respect de la vie privée, la protection des données à caractère personnel, la non-discrimination, les droits de l'enfant et des personnes âgées, les droits des personnes handicapées, la liberté de réunion et d'association, la liberté d'expression, le droit à une bonne administration et le droit à un recours effectif et à accéder à un tribunal impartial.

Par exemple, la technologie de reconnaissance faciale présente des taux d'erreur plus élevés lorsqu'elle est utilisée sur des femmes et des personnes de couleur, ce qui produit des résultats biaisés qui peuvent finalement entraîner une discrimination. L'utilisation de la technologie de reconnaissance faciale peut également avoir un impact négatif sur la liberté de réunion, si les personnes craignent que la technologie de reconnaissance faciale soit utilisée pour les identifier («effet dissuasif»).

En outre, il existe d'éventuelles implications à long terme, qui n'entrent pas dans le cadre de ce document de réflexion. Une entrave à la vie privée par le traitement de grandes quantités de données à caractère personnel, notamment les visages de personnes, peut finalement affecter le fonctionnement de la démocratie, puisque la vie privée est une valeur essentielle inhérente à une société démocratique libérale et pluraliste, et une pierre angulaire de la jouissance des droits fondamentaux.

La société civile et les entreprises privées ont préconisé un cadre réglementaire clair pour la technologie de reconnaissance faciale ([18]). En outre, le groupe d'experts de haut niveau sur l'intelligence artificielle de la Commission européenne recommande spécifiquement d'utiliser de manière proportionnée la technologie de reconnaissance faciale et suggère que son application soit clairement justifiée dans la législation applicable ([19]), étant donné sa croissance alimentée par la forte progression de l'utilisation de l'intelligence artificielle. La jurisprudence est encore pratiquement inexistante, avec une exception récente jugée au Royaume-Uni (jugement non définitif) ([20]).

([16]) Crawford, K. (2019), *Regulate facial-recognition technology*, Nature 572 (2019), 29 août 2019, p. 565.

([17]) *New York Times*, «San Francisco Bans Facial Recognition Technology», 14 mai 2019.

([18]) Voir, par exemple, Big Brother Watch, «Face Off Campaign», mai 2019; Microsoft, «Facial recognition: It's time for action», 6 décembre 2018. Big Brother Watch, soutenue par plusieurs députés britanniques et vingt-cinq organisations de défense des droits, de l'égalité raciale et de la technologie, ainsi que par des universitaires, des experts et des avocats spécialisés dans la technologie, a publié en septembre 2019 une déclaration commune sur l'utilisation par la police et les entreprises privées de la surveillance par reconnaissance faciale au Royaume-Uni («Joint statement on police and private company use of facial recognition surveillance in the UK»).

([19]) Commission européenne, groupe d'experts de haut niveau sur l'intelligence artificielle (2019), *Ethics guidelines for Trustworthy on AI*, avril 2019, p. 33-34.

([20]) Royaume-Uni, High Court of Justice (Queens' Bench Division — Divisional Court Cardiff), *The Queen (OTAO) Bridges and Chief Constable of South Wales Police and others*, (2019) EWCH 2341 (Admin), 4 septembre 2019.

2. Les images faciales comme identifiants biométriques uniques dans le droit de l'UE

Les images faciales des personnes constituent des données biométriques: elles sont plus ou moins uniques, ne peuvent être modifiées et ne peuvent être facilement cachées. Les images faciales sont également faciles à capturer: contrairement à d'autres identifiants biométriques, tels que les empreintes digitales ou l'ADN, une personne ne peut généralement pas éviter que son image faciale soit capturée et surveillée en public.

La législation de l'UE régit le traitement des images faciales dans le cadre de l'acquis de l'UE en matière de protection des données. Le tableau 1 donne une vue d'ensemble des instruments de l'UE relatifs à la protection des données, de leur objet et de la question de savoir s'ils régissent le traitement des images faciales en tant que données biométriques. Dans le domaine de la coopération policière et judiciaire en matière pénale, la directive en matière de protection des données dans le domaine répressif [directive (UE) 2016/680] ([21]) est l'instrument le plus pertinent. Elle établit un système complet de protection des données à caractère personnel dans le contexte de l'application de la loi ([22]). La directive en matière de protection des données dans le domaine répressif fait spécifiquement référence aux images faciales en tant que «données biométriques» lorsqu'elles sont utilisées pour une correspondance biométrique aux fins de l'identification ou de l'authentification unique d'une personne physique ([23]). Les instruments sectoriels de l'UE régissant les systèmes d'information à grande échelle de l'UE dans le domaine de la migration et de la sécurité, qui figurent dans le tableau 2 de la section 5.2, complètent l'acquis de l'UE en matière de protection des données.

Les données biométriques sont définies comme «les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques [empreintes digitales]» ([24]). La législation de l'UE sur la protection des données reconnaît deux catégories d'informations comme étant des données biométriques: 1) les «caractéristiques physiques/physiologiques», qui ont trait aux caractéristiques corporelles telles que les traits du visage, les empreintes digitales, les caractéristiques de la rétine et de l'iris; et 2) les «caractéristiques comportementales», comme les habitudes profondément ancrées, les actions, les traits de personnalité, les addictions, etc. ([25]). Cela inclut les caractéristiques comportementales qui pourraient permettre l'identification unique d'une personne, comme la signature manuscrite ou la façon de marcher ou de se déplacer. Les images faciales numériques appartiennent à la première catégorie.

Le considérant 51 du règlement général sur la protection des données (RGPD) fait une distinction entre la nature juridique des simples «photographies» et celle des «images faciales» biométriques. La définition des données biométriques s'applique aux photographies uniquement lorsque celles-ci sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique ([26]).

([21]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (directive en matière de protection des données dans le domaine répressif) (JO L 119 du 4.5.2016, p. 89-131).
Considérant 41 du RGPD.

([22]) Pour plus d'informations, voir FRA, Conseil de l'Europe et Contrôleur européen de la protection des données (CEPD) (2018), *Manuel de droit européen en matière de protection des données — Édition 2018*, Office des publications, Luxembourg, juin 2018, p. 31-33, et chapitre 8.

([23]) Directive en matière de protection des données dans le domaine répressif, article 3, paragraphe 13. Voir également le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1-88) (RGPD), article 4, paragraphe 14, ainsi que le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (PE/31/2018/REV/1) (JO L 295 du 21.11.2018, p. 39-98), article 3, paragraphe 18.

([24]) Directive en matière de protection des données dans le domaine répressif, article 3, paragraphe 13; RGPD, article 4, paragraphe 14; règlement (UE) 2018/1725, article 3, paragraphe 18.

([25]) Groupe de travail «article 29» sur la protection des données (2012), *Avis 3/2012 sur l'évolution des technologies biométriques*, 00720/12/FR, WP 193, Bruxelles, 27 avril 2012, p. 4; Misra, P. (2018), «Here's how face recognition tech can be GDPR compliant», *thenextweb.com*, 29 octobre 2018.

([26]) RGPD, considérant 51; voir également le règlement (UE) 2018/1725, considérant 29.

Tableau 1 — Instruments du droit européen relatifs à la protection des données: dispositions sur les images faciales et leur applicabilité

Instrument juridique de l'UE relatif à la protection des données	Définition des «données biométriques» (y compris les «images faciales»)	Champ d'application personnel	Champ d'application matériel
Directive en matière de protection des données dans le domaine répressif [directive (UE) 2016/680]	Oui (article 3, paragraphe 13)	Autorités répressives des États membres de l'UE	Traitement automatisé de données à caractère personnel dans les États membres Schengen et traitement de données à caractère personnel par tout autre moyen figurant dans un fichier à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales — dans le champ d'application du droit de l'UE
Règlement général sur la protection des données [règlement (UE) 2016/679]	Oui (article 4, paragraphe 14)	Tous les acteurs privés établis dans l'UE et les institutions publiques opérant dans l'UE ainsi que les responsables du traitement et les sous-traitants non établis dans l'UE qui proposent des biens ou des services aux personnes concernées dans l'UE	Traitement automatisé de données à caractère personnel dans l'Espace économique européen et traitement de données à caractère personnel par tout autre moyen figurant dans un fichier — dans le champ d'application du droit de l'UE (par exemple, le RGPD ne s'applique pas au traitement des données liées à la sécurité nationale)
Règlement sur la protection des données pour les institutions, organes et agences de l'UE [règlement (UE) 2018/1725]	Oui (article 3, paragraphe 18)	Institutions, organes et agences de l'UE	Traitement de données à caractère personnel par les institutions, organes et agences de l'UE
Directive «vie privée et communications électroniques» (directive 2002/58/CE, telle que modifiée par la directive 2009/136/CE)	Non	Toute personne dont les données à caractère personnel sont traitées dans le secteur des communications électroniques dans l'UE (par exemple, via l'internet et la téléphonie mobile et fixe, et les réseaux qui y sont associés)	Transmission de données à travers des services de communications électroniques publics — à l'exception des activités qui ne relèvent pas du champ d'application du droit de l'UE et des activités concernant la sécurité publique, la défense, la sûreté de l'État et les activités de l'État dans le domaine pénal

Source: FRA, 2019 (sur la base des instruments du droit européen figurant dans le tableau).

«Catégories particulières» de données à caractère personnel

«[D]onnées à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique».

Source: Directive en matière de protection des données dans le domaine répressif, article 10, paragraphe 1; RGPD, article 9, paragraphe 1; et règlement (UE) 2018/1725, article 10, paragraphe 1.

En raison de leur nature sensible, les images faciales relèvent des «catégories particulières de données à caractère personnel» ou des données sensibles. À ce titre, la législation de l'UE sur la protection des données prévoit une protection renforcée et des garanties supplémentaires par rapport aux autres données à caractère personnel ([27]).

([27]) Pour plus d'informations, voir FRA, Conseil de l'Europe et CEPD (2018), Manuel de droit européen en matière de protection des données — *Édition 2018*, Office des publications, Luxembourg, juin 2018.

3. Qu'est-ce que la technologie de reconnaissance faciale?

Les technologies de reconnaissance faciale sont des systèmes biométriques qui permettent l'identification et la mise en correspondance automatiques du visage d'une personne. La technologie extrait des données biométriques et les traite ultérieurement en créant un «modèle biométrique» ([28]). Pour les images faciales, un modèle biométrique détecte et mesure différentes caractéristiques faciales ([29]).

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 de ces personnes».

Source: Groupe de travail «article 29» sur la protection des données (2012), Avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles, 00727/12/EN, WP 192, Bruxelles, 22 mars 2012, p. 2.

La reconnaissance faciale fait référence à une multitude de technologies qui peuvent effectuer différentes tâches à des fins différentes. À cet égard, une distinction essentielle consiste à déterminer si la reconnaissance faciale est utilisée pour la vérification, l'identification ou la catégorisation. La vérification et l'identification consistent à faire correspondre des caractéristiques propres à des personnes afin de déterminer leur identité individuelle. La catégorisation consiste à déduire l'appartenance d'une personne à un groupe spécifique sur la base de ses caractéristiques biométriques — par exemple le sexe, l'âge ou la race.

Ces dernières années, les technologies de reconnaissance faciale ont fortement bénéficié d'une plus grande disponibilité de données, de l'augmentation de la puissance de calcul et du développement d'algorithmes d'apprentissage automatique sophistiqués.

3.1. Vérification (comparaison «un-à-un»)

La vérification ou l'authentification correspond souvent à une comparaison «un-à-un». Elle permet de comparer deux modèles biométriques, généralement supposés appartenir à la même personne ([30]). Deux modèles biométriques sont comparés pour déterminer si la personne qui figure sur les deux images est bien la même. Cette procédure est, par exemple, utilisée aux portiques de contrôle automatisé des passeports destinés aux vérifications aux frontières dans les aéroports. Un agent scanne l'image du passeport de la personne et une image en temps réel est prise sur place. La technologie de reconnaissance faciale compare les deux images faciales et si la probabilité que les deux images représentent la même personne est supérieure à un certain seuil, l'identité est vérifiée. La vérification n'exige pas que les caractéristiques biométriques soient déposées dans une base de données centrale. Elles peuvent être stockées, par exemple, sur une carte ou dans un document d'identité/de voyage d'une personne.

3.2. Identification (comparaison «un-à-plusieurs»)

L'identification signifie qu'une comparaison est effectuée entre le modèle de l'image faciale d'une personne et de nombreux autres modèles stockés dans une base de données afin de vérifier si l'image de cette personne y est stockée. La technologie de reconnaissance faciale renvoie un score pour chaque comparaison, indiquant la probabilité que deux images désignent la même personne. Parfois, les images sont comparées à des bases de données, s'il est avéré que la personne de référence figure dans la base de données (identification en série fermée), et parfois, lorsque ce n'est avéré (identification en série ouverte). Cette dernière opération serait appliquée lorsque les personnes sont comparées aux listes de surveillance. L'utilisation de la technologie de reconnaissance faciale

([28]) Groupe de travail «article 29» sur la protection des données (2012), *Avis 03/2012 sur l'évolution des technologies biométriques*, 00720/12/EN, WP 193, Bruxelles, 27 avril 2012.

([29]) «Modèle biométrique»: une représentation mathématique obtenue par l'extraction de caractéristiques des données biométriques, se limitant aux caractéristiques nécessaires pour procéder à des identifications et à des vérifications [voir article 4, paragraphe 12, du règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 (JO L 135 du 22.5.2019, p. 85-135)].

([30]) Voir également Kindt, E. (2013), *Privacy and Data Protection Issues of Biometric Applications A comparative legal analysis* (1st ed. Springer, Governance and Technology Series 12, 2013), et Iglezakis, I. (2013), *EU Data protection legislation and case-law with regard to biometric application*, université Aristote de Thessalonique, 18 juin 2013.

pour l'identification est parfois appelée «reconnaissance faciale automatisée» ([31]).

L'identification peut être basée sur des images faciales obtenues à partir de caméras vidéo. Dans ce cas, le système doit d'abord détecter la présence d'un visage sur des séquences vidéo. Les utilisateurs de smartphones ont sans doute remarqué que lorsqu'ils prennent des photos, l'appareil photo dessine parfois automatiquement des rectangles sur les visages.

Les visages qui apparaissent dans les séquences vidéo sont extraits puis comparés aux images faciales de la base de données de référence afin d'identifier si la personne présente dans la séquence vidéo se trouve dans la base de données d'images (par exemple sur la liste de surveillance). Ces systèmes sont désignés sous le nom de «technologie de reconnaissance faciale en temps réel» ([32]). La qualité des images faciales extraites des caméras vidéo ne peut être contrôlée: la lumière, la distance et la position de la personne capturée sur la séquence vidéo limitent les caractéristiques faciales. Par conséquent, les technologies de reconnaissance faciale en temps réel sont plus susceptibles de donner lieu à de fausses correspondances que les images faciales prises dans un environnement contrôlé, comme un point de passage frontalier ou un poste de police.

3.3. Catégorisation (correspondance des caractéristiques générales)

Outre la vérification et l'identification, la technologie de reconnaissance faciale est également utilisée pour extraire des informations sur les caractéristiques d'une personne. C'est ce qu'on appelle parfois «l'analyse faciale». Ainsi, elle peut également être utilisée pour le profilage des personnes, qui consiste à catégoriser les individus sur la base de leurs caractéristiques personnelles ([33]). Les caractéristiques couramment prédites à partir des images faciales sont le sexe, l'âge et l'origine ethnique. La catégorisation signifie que la technologie n'est pas utilisée pour identifier ou faire correspondre des personnes, mais seulement des caractéristiques individuelles, qui ne permettent pas nécessairement de les identifier. Toutefois, si plusieurs caractéristiques sont déduites d'un visage, et potentiellement liées à d'autres données (par exemple des données de localisation), cela pourrait permettre de facto l'identification d'une personne.

L'utilisation de la technologie de reconnaissance faciale ne s'arrête pas là. Des chercheurs et des entreprises ont mené des expériences visant à déduire d'autres caractéristiques à partir d'images faciales, comme l'orientation sexuelle ([34]). Ces tests sont très controversés d'un point de vue éthique. La technologie de reconnaissance faciale peut également être utilisée pour déduire des émotions, comme la colère, la peur ou le bonheur, et pour détecter si les personnes mentent ou disent la vérité. Cette utilisation a été expérimentée à certaines frontières extérieures de l'UE (Grèce, Hongrie et Lettonie) dans le cadre du projet iBorderCtrl, un système de contrôle des frontières intelligent et portable, qui intègre la reconnaissance faciale et d'autres technologies pour détecter si une personne dit la vérité ([35]).

Les graves implications en matière de droits fondamentaux de la catégorisation des personnes sur la base d'images faciales dépassent le cadre du présent document, qui porte sur l'utilisation de la technologie de reconnaissance faciale à des fins d'identification.

([31]) Voir, par exemple, Davies, B., Innes, M., et Dawson, A. (2018), *An Evaluation of South Wales Police's use of Automated Facial Recognition*, université de Cardiff, septembre 2018.

([32]) Fussey, P., et Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, université d'Essex, Human Rights Centre, juillet 2019.

([33]) FRA (2018), *Guide pour la prévention du profilage illicite aujourd'hui et demain*, Office des publications, Luxembourg, décembre 2018.

([34]) Wang, Y., et Kosinski, M. (2018), *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images*, *Journal of Personality and Social Psychology*, 114(2), p. 246-257.

([35]) Voir Commission européenne, «Smart lie-detection system to tighten EU's busy borders», 24 octobre 2018, et le site web d'iBorderCtrl.

4. Précision de la technologie de reconnaissance faciale: évaluation des risques d'identification erronée

4.1. Développements technologiques et évaluation des performances

Le niveau d'attention élevé prêté à la technologie de reconnaissance faciale ces derniers temps résulte d'importants gains de précision obtenus depuis 2014 ([36]). Ceux-ci sont principalement attribués à l'augmentation de la puissance de calcul, à des quantités massives de données disponibles (images numériques de personnes et de leurs visages) et à l'utilisation d'algorithmes modernes d'apprentissage automatique ([37]).

Déterminer le niveau de précision nécessaire d'un logiciel de reconnaissance faciale est un défi: il existe de nombreuses manières différentes d'évaluer et de déterminer la précision, qui dépendent également de la tâche, de la finalité et du contexte de son utilisation. Lorsque la technologie est appliquée dans des lieux fréquentés par des millions de personnes — comme les gares ou les aéroports —, une proportion relativement faible d'erreurs (par exemple 0,01 %) signifie que des centaines de personnes sont encore signalées à tort. En outre, certaines catégories de personnes risquent davantage de se voir attribuer à tort une correspondance que d'autres, comme le décrit la section 3. Il existe différentes façons de calculer et d'interpréter les taux d'erreur, la prudence est donc de mise ([38]). En outre, en ce qui concerne la précision et les erreurs, les questions relatives à la facilité avec laquelle un système peut être trompé, par exemple par de fausses images de visages (ce que l'on appelle la «mystification») sont importantes, en particulier à des fins répressives ([39]).

Les technologies de reconnaissance faciale, comme d'autres algorithmes d'apprentissage automatique, ont des résultats binaires, c'est-à-dire qu'il existe deux résultats possibles. Il convient donc de faire la distinction entre les faux positifs et les faux négatifs.

- Un «faux positif» désigne la situation dans laquelle une image correspond à tort à une autre image de la liste de surveillance. Dans un contexte répressif, cela signifierait qu'une personne serait identifiée à tort comme figurant sur la liste de surveillance par le système, ce qui aurait des conséquences majeures sur les droits fondamentaux de cette personne. Le «taux de fausses identifications positives» indique la proportion de correspondances détectées à tort (par exemple le nombre de personnes identifiées sur la liste de surveillance qui n'y figurent pas en réalité) parmi toutes les personnes qui ne figurent pas sur la liste de surveillance.

- Les «faux négatifs» désignent les personnes qui sont considérées comme ne présentant pas de correspondance (c'est-à-dire comme exclues de la liste de surveillance), mais qui présentent en réalité une correspondance. Le «taux de fausses identifications négatives» ou «taux d'échec» correspondant indique la proportion de personnes non identifiées à tort parmi celles qui devraient l'être.

La question des faux positifs et des faux négatifs est également liée à la qualité des données et à la précision de leur traitement. Pour y remédier, il faut corriger et mettre à jour régulièrement les images faciales stockées dans une liste de surveillance afin de garantir un traitement précis.

Lorsqu'on parle de taux d'erreur, il faut garder à l'esprit trois considérations importantes:

- Premièrement, un algorithme ne donne jamais un résultat définitif, mais uniquement des probabilités. Par exemple, avec 80 % de probabilité, la personne figurant sur une image est la personne figurant sur une autre image de la liste de surveillance. Cela signifie que des seuils ou des listes de classement doivent être définis pour prendre des décisions sur les correspondances.

([36]) Voir Grother, P., Ngan, M., et Hanaoka, K. (2018), *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, NISTIR 8238*; ou Galbally, J., Ferrara, P., Haraksim, R., Psyllos, A., et Beslay, L. (2019), *Study on Face Identification Technology for its Implementation in the Schengen Information System*, Office des publications, Luxembourg, juillet 2019.

([37]) Le succès de la reconnaissance d'images faciales repose principalement sur l'utilisation de réseaux neuronaux convolutifs profonds. Ces algorithmes acquièrent des connaissances à partir de modèles génériques d'images en divisant les images en plusieurs zones.

([38]) Pour des discussions plus détaillées sur les paramètres d'évaluation, voir Grother, P., Ngan, M., et Hanaoka, K. (2018), *Ongoing Face Recognition Vendor Test (FRVT) Part 2:* Identification, NISTIR 8238; ou Galbally, J., Ferrara, P., Haraksim, R., Psyllos, A., et Beslay, L. (2019), *Study on Face Identification Technology for its Implementation in the Schengen Information System*, Office des publications, Luxembourg, juillet 2019.

([39]) Voir, par exemple, Parkin, A., et Grinchuk, O. (2019), *Recognizing Multi-Modal Face Spoofing with Face Recognition Networks*.

- Deuxièmement, en conséquence, il y a toujours un compromis entre les faux positifs et les faux négatifs du fait que la décision repose sur un seuil de probabilité. Lorsque le seuil est plus élevé, les faux positifs diminuent, mais les faux négatifs augmentent, et inversement. C'est pourquoi ces taux sont généralement rapportés conjointement, avec l'autre taux à un niveau fixe (par exemple, le taux d'échec est rapporté au taux de fausses identifications positives fixe de 0,01, c'est-à-dire 1 %) ([40]).

- Troisièmement, les taux doivent être évalués en tenant compte des quantités de cas réels. Si un grand nombre de personnes sont contrôlées en masse, un taux de fausses identifications positives potentiellement faible signifie qu'un nombre important de personnes sont encore incorrectement identifiées. Par exemple, un taux de fausses identifications positives de 0,01 signifie que, parmi 100 000 personnes, 1 000 seront signalées à tort. La précision est généralement déterminée sur la base d'ensembles de données d'apprentissage spécifiques et ne peut pas être facilement évaluée au cours du déploiement. L'une des raisons est que les personnes qui ne sont pas détectées dans le monde réel ne sont pas connues.

Enfin, la détermination de la précision doit être effectuée pour différents groupes de population, car les taux de précision généraux pourraient être trompeurs. Outre les questions liées aux performances variables de la technologie de reconnaissance faciale en fonction du sexe, de l'âge (enfants et personnes âgées) et du groupe ethnique des personnes, la précision de la technologie, lorsqu'elle est appliquée aux personnes handicapées, est un autre aspect important qui est rarement pris en compte.

4.2. Qualité des données et bases de données d'apprentissage

La précision de la technologie de reconnaissance faciale est fortement influencée par la qualité des données utilisées pour créer le logiciel et la qualité des données utilisées au cours du déploiement. En vertu du principe d'exactitude des données — énoncé à l'article 5, paragraphe 1, point d), du RGPD ainsi qu'à l'article 4, paragraphe 1, point d), de la directive en matière de protection des données dans le domaine répressif —, les autorités doivent utiliser des informations exactes et à jour.

Plusieurs facteurs influencent la qualité des images faciales, notamment la séparation du fond et des objets, l'éclairage et la luminosité, l'ergonomie, l'âge, le vieillissement, le sexe, la couleur de la peau et les affections cutanées ([41]). Les normes existantes relatives aux images faciales définissent les propriétés des images où figurent des visages afin de garantir une qualité élevée — par exemple le nombre de pixels entre les yeux d'un visage ([42]). Tandis que d'autres normes et méthodes de contrôle de qualité font encore l'objet de discussions et de recherches, la technologie de reconnaissance faciale établit souvent une distinction entre les images en fonction de leur qualité. Les images de haute qualité, prises dans des circonstances contrôlées, sont habituellement désignées sous le terme d'images faciales, portraits ou photos signalétiques. Les autres images sont considérées comme étant de moindre qualité et doivent être considérées avec plus de précaution. La qualité des images constitue un sérieux obstacle lorsque les technologies de reconnaissance faciale sont appliquées à des images obtenues à partir de caméras vidéo, car la qualité de l'image ne peut pas être facilement contrôlée.

Les logiciels de reconnaissance faciale sont basés sur des modèles préentraînés, ce qui signifie que le logiciel développe des règles d'identification des visages à partir d'une base de données d'images faciales. Cela a été possible grâce à la disponibilité croissante d'images faciales de meilleure qualité et à l'augmentation de la puissance de calcul pour traiter de grandes quantités de données. Du point de vue des droits fondamentaux, il est important de savoir quels ensembles de données ont été utilisés pour développer le logiciel de reconnaissance faciale, car ceux-ci influencent les performances du logiciel. Par exemple, bien que les logiciels préentraînés puissent être adaptés à un usage courant, des problèmes persistants ont été constatés en ce qui concerne le sexe et les groupes ethniques, car le logiciel de reconnaissance faciale a souvent été entraîné principalement sur des images faciales d'hommes blancs, et beaucoup moins sur des images faciales de femmes et de personnes appartenant à d'autres groupes ethniques ([43]). En raison de l'obligation de respecter les droits à la protection des données et des droits de propriété, les bases de données d'images faciales à grande échelle en vue de développer des logiciels ne sont pas accessibles à tous. Les grandes entreprises du secteur informatique ont donc un avantage certain lorsqu'elles développent leur logiciel de reconnaissance

([40]) Par exemple, Grother, P., Ngan, M., et Hanaoka, K. (2018), *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, NISTIR 8238.

([41]) Sanchez del Rio, J., Conde, C., et al. (2015), *Face-based recognition systems in the ABC e-gates;* FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Office des publications, Luxembourg, mars 2018.

([42]) L'Organisation de l'aviation civile internationale (OACI) a créé des normes relatives aux images faciales devant être insérées dans les documents de voyage [OACI (2018), Technical Report. Portrait Quality (Reference Facial Images for MRTD)]. L'Organisation internationale de normalisation (ISO), en collaboration avec la Commission électrotechnique internationale (CEI), a publié une norme relative aux meilleures pratiques applicables aux images faciales (ISO/IEC 19794-5).

([43]) Buolamwini, J., et Gebru, T. (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, *Proceedings of Machine Learning Research* 81:1-15, Conference on Fairness, Accountability, and Transparency.

faciale. Pourtant, même parmi ces grands fournisseurs de logiciels de reconnaissance faciale, des problèmes de performance persistent ([44]).

Cela souligne l'importance de disposer de données d'apprentissage de haute qualité pour le développement des technologies de reconnaissance faciale et d'autres systèmes d'IA en général, car l'utilisation de ces systèmes pourrait entraîner une discrimination à l'égard des personnes ayant certaines caractéristiques, notamment les femmes et les filles ([45]). En réalité, il peut être difficile d'obtenir des informations sur les données d'apprentissage utilisées pour le développement des logiciels. Les logiciels pourraient s'appuyer sur des algorithmes déjà existants (modèles préentraînés), ce qui rend difficile la recherche des données d'apprentissage originales. Plus important encore, les fournisseurs de logiciels de reconnaissance faciale pourraient ne pas vouloir divulguer d'informations sur les données d'apprentissage, comme l'a constaté un expert d'une organisation de la société civile. Les questions de droits d'auteur et de secrets d'affaire pourraient être utilisées pour empêcher l'accès aux informations nécessaires pour évaluer la qualité des systèmes employés ([46]).

Enfin, la qualité des images incluses dans les listes de surveillance à comparer aux images faciales est une discussion cruciale sur l'utilisation des technologies de reconnaissance faciale. Des images de mauvaise qualité contenues dans les listes de surveillance peuvent augmenter considérablement le nombre d'erreurs et de correspondances erronées.

([44]) Grother, P., Ngan, M., et Hanaoka, K. (2018), *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, NISTIR 8238.

([45]) FRA (2018), *#BigData:Discrimination and data-supported decision making*, Office des publications, Luxembourg, mai 2018; FRA (2019), *Data quality and artificial intelligence — mitigating bias and error to protect fundamental rights*, Office des publications, Luxembourg, juin 2019.

([46]) AI Now Institute (2018), *AI Now Report 2018*.

5. Utilisation de la technologie de reconnaissance faciale par les autorités publiques dans l'UE

On ne dispose pas à ce jour d'une vue d'ensemble de l'utilisation de la technologie de reconnaissance faciale dans l'UE. De nombreuses entreprises du secteur informatique proposent des technologies de reconnaissance faciale et leur utilisation par les administrations publiques à différentes fins suscite un vif intérêt. Cette section se concentre sur leur utilisation à des fins répressives ([47]). Ces dernières années, un certain nombre de tests sur les technologies de reconnaissance faciale ont été menés par les autorités répressives de différents États membres de l'UE, bien que les informations disponibles soient limitées. Outre des examens de déploiement des technologies de reconnaissance faciale en temps réel par les autorités publiques dans les États membres de l'UE, l'usage planifié des images faciales dans les bases de données européennes à grande échelle dans les domaines de la migration et de la sécurité est en augmentation (voir section 5.2). Entretemps, la recherche sur l'utilisation éventuelle des technologies de reconnaissance faciale se poursuit (voir section 5.3).

5.1. Tests sur les technologies de reconnaissance faciale par les autorités répressives dans les États membres de l'UE

La FRA a interrogé des représentants des autorités publiques en Allemagne, en France et au Royaume-Uni sur leur utilisation éventuelle et leurs projets d'utilisation des technologies de reconnaissance faciale en temps réel à des fins répressives.

Jusqu'à présent, c'est la police du Royaume-Uni qui a été la plus active dans l'examen des technologies de reconnaissance faciale en temps réel. Le Royaume-Uni est le seul État membre de l'UE à effectuer des tests sur les technologies de reconnaissance faciale en temps réel, sur le terrain avec des listes de surveillance réelles. Par exemple, la police du sud du Pays de Galles y a eu recours lors de grands événements ([48]), et la police métropolitaine de Londres a procédé à plusieurs essais en temps réel sur les technologies de reconnaissance faciale.

La police du sud du Pays de Galles a été la première à utiliser la technologie de reconnaissance faciale en temps réel au Royaume-Uni lors de grands événements sportifs. La police y a eu recours, en juin 2017, lors de la finale de la Ligue des champions de l'Union des associations européennes de football (UEFA), qui a rassemblé environ 310 000 personnes à Cardiff. Cette technologie a également été utilisée lors de plusieurs autres événements, notamment d'autres manifestations sportives ainsi que des concerts de musique. Plusieurs caméras de vidéosurveillance ont été placées à différents endroits présélectionnés. En fonction de l'ampleur des événements, la police a établi des listes de surveillance comprenant plusieurs centaines de personnes ciblées. Selon le rapport d'évaluation indépendant des essais, quatre listes de surveillance différentes ont été utilisées pour la finale de la Ligue des champions de l'UEFA, notamment:

- un petit nombre de personnes perçues comme présentant un risque sérieux pour la sécurité publique;
- des personnes condamnées antérieurement pour des types d'infractions graves;
- des personnes pouvant intéresser la police, dont la présence ne présentait pas de risque ou de menace immédiate pour la sécurité publique; et
- des images de policiers pour examiner l'efficacité du système.

Les listes de surveillance contenaient entre 400 et 1 200 personnes pour les différents événements. La sélection s'est faite sur la base de différents critères possibles. Cependant, aucune autre information sur la création de

([47]) Pour donner un autre exemple, une municipalité suédoise a utilisé la technologie de reconnaissance faciale pour contrôler l'assiduité des élèves dans les écoles. Cela a conduit l'autorité suédoise de protection des données à infliger une amende à la municipalité pour violation du RGPD. Voir comité européen de la protection des données, «Facial recognition school renders Sweden's first GDPR fine», 22 août 2019. Dans le même ordre d'idées, la Commission nationale de l'informatique et des libertés (CNIL) a également estimé que le recours à la reconnaissance faciale à l'entrée de deux lycées (à Marseille et à Nice), pour des raisons de sécurité, n'apparaît ni nécessaire ni proportionné pour atteindre les finalités poursuivies et constitue une violation du RGPD. Voir CNIL, «Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position», 20 octobre 2019.

([48]) La police du sud du Pays de Galles a également effectué des tests utilisant des caméras de vidéosurveillance à des fins d'enquête pénale, mais de manière rétrospective. Une liste complète des déploiements de ces technologies est disponible sur le site web de la police du sud du Pays de Galles.

listes de surveillance n'a été partagée avec les évaluateurs de l'essai ([49]). L'absence d'informations sur la manière dont les listes de surveillance ont été créées rend difficile l'évaluation de la finalité réelle, de la nécessité et du besoin social d'utiliser la technologie de reconnaissance faciale en temps réel. La première affaire sur cette question à être portée devant un tribunal de l'Union européenne (jugement non définitif) l'a été devant une chambre divisionnaire à Cardiff. Il a été statué, dans une affaire dirigée contre la police du sud du Pays de Galles, que le régime juridique national actuel est suffisant pour garantir l'utilisation appropriée et non arbitraire de la technologie de reconnaissance faciale appelée «AFR Locate», et que l'utilisation par la police du sud du Pays de Galles de l'«AFR Locate» était conforme aux exigences du Human Rights Act et de la législation sur la protection des données ([50]).

Entre 2016 et 2019, la police métropolitaine de Londres a effectué dix examens de déploiement des technologies de reconnaissance faciale en temps réel, afin d'examiner l'efficacité des technologies de reconnaissance faciale à identifier les personnes figurant sur des listes de surveillance. Ils ont eu lieu lors des carnavals de Notting Hill en 2016 et 2017, et dans d'autres lieux sélectionnés à Londres ([51]). Les tests ont été effectués en utilisant des listes de surveillance existantes et des images supplémentaires fournies par des policiers pour en expérimenter la précision. La création de listes de surveillance à partir de différentes sources et bases de données est décrite comme étant relativement complexe ([52]). Les listes de surveillance des tests comprenaient:

- des individus sous mandat d'arrêt;
- des individus considérés comme susceptibles de commettre des crimes violents; et
- des individus connus par les services de police, pouvant présenter un danger pour la sécurité des personnalités publiques.

Le comité d'éthique «London Policing Ethics Panel» a souligné l'importance capitale de la raison pour laquelle les listes de surveillance sont compilées et de la manière dont elles le sont. Il a exprimé des préoccupations quant à l'intégrité des bases de données à partir desquelles les images ont été extraites pour les listes de surveillance, et quant au fait que des images provenaient d'autres sources également ([53]). La société civile a critiqué le manque d'informations sur les personnes figurant sur les listes de surveillance, qui résulte de l'absence de dispositions législatives ou d'orientations.

En Allemagne, la police de Hambourg a utilisé des technologies de reconnaissance faciale dans le cadre du sommet du G20 en juillet 2017. Sur la base d'enregistrements vidéo de huit gares, ainsi que d'images et d'enregistrements vidéo provenant d'autres sources (par exemple bus, métro), les policiers ont identifié manuellement des activités criminelles et les personnes concernées. Dans un deuxième temps, ils ont tenté d'identifier ces personnes, potentiellement impliquées dans des activités criminelles, dans tous les enregistrements de l'événement disponibles en utilisant des technologies de reconnaissance faciale. Le commissaire à la protection des données de Hambourg (*Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*) a publié un rapport sur l'utilisation des technologies de reconnaissance faciale lors du G20 et a constaté que l'utilisation de cette technologie n'était pas conforme à la législation sur la protection des données. Il a considéré comme particulièrement problématique l'absence de base juridique pour son utilisation ([54]).

La police de Berlin a procédé à un vaste essai sur les technologies de reconnaissance faciale en temps réel dans une gare en 2017 et 2018. L'objectif principal de l'examen était d'évaluer les performances techniques lors de l'utilisation de trois systèmes logiciels de reconnaissance faciale différents. L'utilisation potentielle des technologies de reconnaissance faciale a été justifiée par l'impossibilité de pouvoir passer en revue les enregistrements vidéo de toutes les caméras de vidéosurveillance disponibles à Berlin lors de la recherche de personnes. La police a publié un rapport complet sur les résultats de l'examen en septembre 2018 ([55]). L'examen a été mené uniquement sur des sujets volontaires, inscrits sur une «liste de surveillance» artificielle. Les images faciales d'environ 300 volontaires ont été prises puis le logiciel a essayé de les identifier lorsque ceux-ci passaient dans une certaine zone de la gare. D'autres personnes, ne figurant pas sur la «liste de surveillance», pouvaient choisir de traverser ou non les zones signalées comme affectées à l'examen des technologies de reconnaissance faciale. En termes de

([49]) Davies, B., Innes, M., et Dawson, A., *An evaluation of South Wales Police's use of Automated Facial Recognition*, université de Cardiff, septembre 2018. Outre ces déploiements pour localiser des personnes, la police du sud du Pays de Galles a utilisé la technologie de reconnaissance faciale pour identifier des suspects à partir de scènes d'infraction antérieures. Les images capturées sur les scènes d'infraction par des caméras de vidéosurveillance ou de téléphonie mobile sont comparées à une base de données à grande échelle d'images de personnes placées en détention à des fins d'enquête.

([50]) Royaume-Uni, High Court of Justice (Queen's Bench Division — Divisional Court Cardiff), *The Queen (OTAO) Bridges and Chief Constable of South Wales Police and others*, (2019) EWCH 2341 (Admin), 4 septembre 2019, paragraphe 159.

([51]) Fussey, P., et Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, université d'Essex, Human Rights Centre, juillet 2019, p. 24 et 31.

([52]) Ibid., p. 76-83.

([53]) London Policing Ethics Panel (2018), *Interim Report on Live Facial Recognition*.

([54]) Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg*, 2018. Jusqu'à présent, il n'y a eu aucune décision judiciaire allemande sur la légalité de l'utilisation de cette technologie par la police.

([55]) Polizeipräsidium Potsdam, *Biometrische Gesichtserkennung*, 2018.

précision, les résultats ont été jugés satisfaisants pour la police lorsque les trois systèmes logiciels étaient combinés. Cependant, l'utilisation potentielle du logiciel pour déterminer qui inclure sur une éventuelle liste de surveillance et dans quels cas il peut être déployé, n'a pas été déterminée par la police. La police a déclaré que le législateur doit prendre une décision à ce sujet en adoptant une loi sur le déploiement des technologies de reconnaissance faciale en temps réel. Il s'agit notamment de définir qui peut être inclus dans les listes de surveillance — par exemple les personnes recherchées pour terrorisme, les délinquants sexuels, les personnes qui se sont évadées de prison alors qu'elles purgeaient de longues peines, ou les enfants disparus. Selon les informations fournies par les experts, l'utilisation des technologies de reconnaissance faciale à des fins d'identification est également envisagée dans le cadre de la gestion des frontières en Allemagne. Cependant, elle n'a pas encore été mise en œuvre dans ce contexte.

La police de Nice (France) a mené un essai sur les technologies de reconnaissance faciale en temps réel lors du carnaval en 2018. Le but de l'examen était d'évaluer l'efficacité de la technologie. La «liste de surveillance» de l'essai était constituée d'images de volontaires. Les personnes présentes au carnaval pouvaient choisir d'entrer ou non dans la zone où les technologies de reconnaissance faciale en temps réel étaient déployées. La gendarmerie française utilise les technologies de reconnaissance faciale pour les enquêtes pénales, mais n'a pas recours aux technologies de reconnaissance faciale en temps réel en raison de l'absence de base juridique pour leur utilisation. Les experts interrogés par la FRA ont mentionné que l'utilisation potentielle future des technologies de reconnaissance faciale par la police pourrait cibler les grands événements et rassemblements ainsi que la sécurité quotidienne dans les lieux publics. Les experts ont déclaré que les technologies de reconnaissance faciale pourraient rendre plus efficaces les systèmes de contrôle actuels, comme l'identification des personnes recherchées.

En résumé, les autorités allemandes et françaises ont testé les technologies de reconnaissance faciale en temps réel uniquement sur des volontaires, sans indiquer clairement qui serait inclus dans les listes de surveillance si la technologie devait être utilisée pour des déploiements réels. En raison de l'absence de base juridique pour leur déploiement, les technologies de reconnaissance faciale en temps réel ne peuvent actuellement pas être utilisées légalement dans ces deux pays.

Seules des informations limitées sont actuellement disponibles sur l'utilisation éventuelle des technologies de reconnaissance faciale en temps réel ou les tests en la matière dans d'autres États membres de l'UE. En 2019, les autorités autrichiennes ont fait l'acquisition d'un logiciel destiné à appliquer les technologies de reconnaissance faciale pour effectuer des comparaisons de bases de données, dans le but d'identifier les auteurs inconnus d'infractions pénales pour lesquels des images sont disponibles à partir de caméras de vidéosurveillance ou d'autres sources ([56]). Aux Pays-Bas, des tests ont été lancés sur l'utilisation des technologies de reconnaissance faciale.

Ces tests montrent qu'un certain nombre d'États membres sont intéressés par l'utilisation potentielle des technologies de reconnaissance faciale, que ce soit en temps réel (c'est-à-dire à partir de caméras de vidéosurveillance) ou non. Dans certains cas, les tests sont évalués soit par des entités indépendantes sous contrat avec la police, soit par la police elle-même. La société civile, les autorités responsables de la protection des données et les universitaires ont soulevé plusieurs préoccupations concernant les droits fondamentaux quant à l'utilisation des technologies de reconnaissance faciale ([57]). La section 6 et la section 7 abordent les préoccupations en matière de droits fondamentaux liées à l'utilisation potentielle des technologies de reconnaissance faciale, en mettant l'accent sur les technologies de reconnaissance faciale en temps réel.

5.2. La reconnaissance faciale appliquée aux systèmes d'information à grande échelle de l'UE dans le domaine de la migration et de la sécurité

Ces dernières années, l'UE a développé ou mis à niveau plusieurs systèmes d'information à grande échelle dans le domaine de la migration et de la sécurité. Le processus est en cours, certaines propositions législatives étant encore en attente d'adoption finale.

([56]) Réponse à l'enquête parlementaire (*Anfragebeantwortung* 3403/J).

([57]) Voir, par exemple, au Royaume-Uni: Fussey, P., et Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, université d'Essex, Human Rights Centre, juillet 2019; Big Brother Watch (2019), «Joint statement on police and private company use of facial recognition surveillance in the UK»; et Big Brother Watch, «Face Off Campaign», mai 2019.

Tableau 2 — Systèmes d'information de l'UE dans le domaine de la migration et de la sécurité et traitement des images faciales

Système d'information de l'UE		Principales dispositions en matière de collecte et de traitement des images faciales	Finalité	Base juridique
Système d'information Schengen (SIS II)				
SIS II — police	√	Règles spécifiques pour l'introduction des données biométriques (article 42) Règles spécifiques pour les vérifications ou les recherches à l'aide de données biométriques (article 43) [...] Les images faciales et les photographies ne devraient être utilisées, dans un premier temps, à des fins d'identification que dans le contexte des points de passage frontalier habituels. [...] (considérant 22)	Introduire et traiter les signalements en vue d'une arrestation, concernant des personnes disparues, en vue de contrôles discrets et de contrôles spécifiques, concernant des objets, etc. afin de garantir la sécurité dans l'UE et les États membres de l'espace Schengen	Règlement (UE) 2018/1862, 28 novembre 2018
SIS II — vérifications aux frontières	√	Règles spécifiques pour l'introduction des données biométriques (article 32) Règles spécifiques pour les vérifications ou les recherches à l'aide de données biométriques (article 33) [...] Les images faciales et les photographies ne devraient être utilisées, dans un premier temps, à des fins d'identification que dans le contexte des points de passage frontalier habituels. [...] (considérant 20)	Introduire et traiter des signalements aux fins de non-admission ou d'interdiction de séjour dans les États membres Schengen pour soutenir la mise en œuvre des politiques de vérifications aux frontières et d'immigration	Règlement (UE) 2018/1861, 28 novembre 2018
SIS II — retour	√	Insertion d'une «image faciale» dans les signalements concernant un retour uniquement pour confirmer l'identité de la personne (article 4)	Introduire et traiter les signalements pour les ressortissants de pays tiers faisant l'objet d'une décision de retour pour soutenir la mise en œuvre des politiques de vérifications aux frontières et d'immigration	Règlement (UE) 2018/1860, 28 novembre 2018
Système d'entrée/de sortie (EES)	√	Image faciale de ressortissants de pays tiers (article 15) Utilisation des données à des fins de vérification aux frontières (article 23) Utilisation de l'EES aux fins de l'examen des demandes de visa et des décisions y afférentes (article 24) Utilisation de l'EES aux fins de l'examen des demandes d'accès aux programmes nationaux d'allègement des formalités (article 25) Accès aux données à des fins de vérification sur le territoire des États membres (article 26)	Calculer et surveiller la durée du séjour autorisé des ressortissants de pays tiers et identifier les personnes ayant dépassé la durée de séjour autorisée Finalité ajoutée: domaine répressif	Règlement (UE) 2017/2226, 30 novembre 2017
Système d'information sur les visas (VIS)				
VIS	–	Oui (article 5, paragraphe 1b)	Faciliter l'échange de données entre les États membres Schengen sur les demandes de visa Finalité ajoutée: domaine répressif	Règlement (CE) n° 767/2008, 9 juillet 2008
Proposition de VIS	√	Qualité des images faciales (article 9, paragraphe 8) Recherches à l'aide de données alphanumériques et d'images faciales (article 18) Règles particulières applicables à la saisie des données (article 29 *bis*)		*Proposition de révision* COM(2018) 302 final, 16 mai 2018

Système européen de comparaison des empreintes digitales (Eurodac)				
Eurodac	–	Aucun	Déterminer l'État membre responsable de l'examen d'une demande de protection internationale Finalité ajoutée: domaine répressif	Règlement (UE) n° 603/2013, 26 juin 2013
Eurodac Proposition de refonte	√	Obligation de relever les empreintes digitales et de capturer l'image faciale (article 2) Enregistrement des données à caractère personnel, y compris les images faciales (articles 12, 13 et 14) Comparaison et transmission de toutes les catégories de données (articles 15 et 16)	Nouvelle finalité: contribuer au contrôle de l'immigration irrégulière et des mouvements secondaires Finalité ajoutée: domaine répressif	*Proposition de révision* COM(2016) 272 final, 4 mai 2016
Système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN)	√	Image faciale uniquement pour confirmer l'identité d'une personne localisée à la suite d'une consultation alphanumérique ou d'une recherche sur la base des données dactyloscopiques (article 6, paragraphe 1) À terme, possibilité d'utiliser les images faciales pour l'établissement automatisé de correspondances biométriques, à condition que les critères de nécessité et de proportionnalité soient respectés et que la technologie soit prête à être employée (article 6, paragraphe 2)	Partager des informations sur les condamnations antérieures de ressortissants de pays tiers	Règlement (UE) 2019/816, 17 avril 2019
Interopérabilité des systèmes d'information de l'UE	√	Les requêtes basées sur des données alphanumériques et biométriques, y compris des images faciales, seront lancées avec le portail de recherche européen (ESP) [article 9, Interopérabilité (frontières et visas); article 9, Interopérabilité (coopération policière et judiciaire, asile et migration)] Modèles biométriques d'images faciales à stocker et à rechercher par le biais du service d'établissement de correspondances biométriques [articles 13 et 14, Interopérabilité (frontières et visas); articles 13 et 14, Interopérabilité (coopération policière et judiciaire, asile et migration)] Images faciales à stocker dans le répertoire commun de données d'identité [article 18, Interopérabilité (frontières et visas); article 17, Interopérabilité (coopération policière et judiciaire, asile et migration)]	Établir un cadre pour l'interopérabilité entre l'EES, le VIS, ETIAS, Eurodac, le SIS II et l'ECRIS-TCN afin de permettre leur communication pour la gestion des frontières, la sécurité, la protection internationale Finalité ajoutée: domaine répressif	Règlement (UE) 2019/817 — frontières et visas, 20 mai 2019 Règlement (UE) 2019/818 — coopération policière et judiciaire, asile et migration, 20 mai 2019

Notes: = *image faciale. Les propositions législatives qui n'ont pas encore été adoptées sont indiquées en italiques.*

Source: *FRA, 2019 (sur la base des instruments juridiques existants et proposés de l'UE).*

Tableau 3 — Identificateurs biométriques dans les systèmes d'information à grande échelle de l'UE dans le domaine de la migration et de la sécurité

				AUCUN
• Système d'information Schengen (SIS II) — police	• Système d'information Schengen (SIS II) — frontières • Système d'information Schengen (SIS II) — retour	• Système d'entrée/de sortie (EES) • Système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN) • Interopérabilité entre les systèmes d'information de l'UE • Système européen de comparaison des empreintes digitales (Eurodac) (2016, proposition de refonte) • Système d'information sur les visas (VIS) (2018, proposition)	• Système européen de comparaison des empreintes digitales (Eurodac) • Système d'information sur les visas (VIS)	• Système européen d'information et d'autorisation concernant les voyages (ETIAS)
Empreintes digitales	Empreintes palmaires	Image faciale	Profil ADN	Noir = adopté Bleu = non adopté

Source: FRA, 2019 (sur la base de la législation adoptée et en instance).

Le règlement relatif au système d'entrée/de sortie a introduit les images faciales en tant qu'identifiants biométriques et a prévu l'utilisation de la technologie de reconnaissance faciale à des fins de vérification pour la première fois dans le droit de l'UE ([58]). Comme le montre le tableau 2, le traitement des images faciales est pour l'instant inclus dans tous les systèmes d'information, à l'exception du système européen d'information et d'autorisation concernant les voyages (ETIAS). Le traitement des images faciales permet la vérification biométrique de l'identité d'une personne, par exemple lors d'une demande de visa, du franchissement d'une frontière ou d'une demande d'asile. Dans ces cas, la personne concernée est consciente que les autorités prennent son image faciale. Cette situation est différente de celle où la reconnaissance faciale en temps réel est appliquée à des fins d'identification, à l'insu de la personne concernée.

Le traitement des images faciales dans les systèmes d'information de l'UE à grande échelle complète le

([58]) Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) n° 767/2008 et (UE) n° 1077/2011 (JO L 327 du 9.12.2017, p. 20-82) (règlement EES), article 3, paragraphes 1 et 18, article 15 et articles 23 à 26.

traitement d'autres identifiants biométriques, notamment les empreintes digitales. Le tableau 3 donne un aperçu du type de données biométriques qui seront traitées dans les six systèmes d'information de l'UE une fois que la nouvelle base juridique de deux d'entre eux, le système européen de comparaison des empreintes digitales (Eurodac) et le système d'information sur les visas (VIS), sera en place. Cinq des six systèmes traiteront les images faciales.

Dans les systèmes d'information à grande échelle de l'UE, la collecte et le traitement des images faciales, ainsi que d'autres données biométriques, sont strictement réglementés par la loi ([59]). Des garanties limitent la collecte et le traitement des données à caractère personnel à ce qui est strictement nécessaire sur le plan opérationnel. L'accès à ces données est restreint aux personnes qui en ont un besoin opérationnel. Les instruments juridiques sur lesquels reposent les systèmes d'information garantissent les droits des personnes concernées, conformément à l'acquis de l'UE en matière de protection des données ([60]).

En outre, les instruments juridiques des systèmes d'information de l'UE mis à niveau renforcent les garanties en matière de qualité des données. Ils exigent que ces conditions soient remplies pour que des recherches biométriques au moyen d'images faciales puissent être effectuées ([61]). En règle générale, ils prévoient que le traitement automatisé des images faciales ne doit être effectué que dès que ce sera techniquement possible pour garantir un recoupement fiable des données et que la Commission européenne doit présenter un rapport indiquant si la technique requise est disponible. Comme garantie supplémentaire, l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) ([62]) est responsable des garanties d'assurance qualité et fait régulièrement rapport sur les mécanismes et procédures automatisés de contrôle de la qualité des données ([63]).

En ce qui concerne le système d'entrée/de sortie, la Commission européenne a adopté des spécifications techniques relatives à la qualité, à la résolution et à l'utilisation des données biométriques, y compris les images faciales ([64]). En ce qui concerne le système d'information Schengen, le Centre commun de recherche de la Commission européenne a évalué si la technologie de reconnaissance faciale est suffisamment mature pour être intégrée dans le contexte du système d'information Schengen ([65]). L'étude présente dix-neuf recommandations pour le déploiement de la technologie, dont différentes mesures visant à garantir la meilleure qualité possible des données stockées.

Il est particulièrement important de disposer de ces garanties, étant donné que l'évolution de l'interopérabilité des systèmes d'information de l'UE à grande échelle permet, sous un contrôle strict, aux autorités nationales, y compris les autorités répressives, d'accéder à des données d'identité supplémentaires stockées dans le répertoire commun de données d'identité auxquelles elles ne pourraient pas accéder autrement, notamment aux fins de la lutte contre l'immigration clandestine, les formes graves de criminalité et le terrorisme, telles que des images faciales — consultables. Ces contrôles stricts doivent toujours respecter le principe de la limitation de la finalité et l'accès doit être nécessaire et proportionné aux objectifs définis par la loi ([66]).

([59]) Voir, par exemple, articles 32 et 33 du règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006 (JO L 312 du 7.12.2018, p. 14-55) (SIS II — vérifications aux frontières).

([60]) Voir, par exemple, articles 51, 52 et 53 du règlement relatif au SIS II — vérifications aux frontières (énumérant les droits des personnes concernées).

([61]) Voir, par exemple, article 33, paragraphe 4, du règlement relatif au SIS II — vérifications aux frontières.

([62]) Pour une vue d'ensemble du rôle et des tâches de l'agence eu-LISA, voir le chapitre II du règlement (UE) 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), modifiant le règlement (CE) n° 1987/2006 et la décision 2007/533/JAI du Conseil et abrogeant le règlement (UE) n° 1077/2011 (JO L 295 du 21.11.2018, p. 99-137) (règlement eu-LISA).

([63]) Voir le règlement eu-LISA, articles 2 et 12.

([64]) Annexe de la décision d'exécution de la Commission établissant les spécifications relatives à la qualité, à la résolution et à l'utilisation des empreintes digitales et de l'image faciale aux fins de vérification et d'identification biométriques dans le système d'entrée/de sortie (EES), C(2019) 1280 final, Bruxelles, 25 février 2019.

([65]) Galbally, J., Ferrara, P., Haraksim, R., Psyllos, A., et Beslay, L. (2019), *Study on Face Identification Technology for its Implementation in the Schengen Information System*, Office des publications, Luxembourg, juillet 2019, p. 9.

([66]) Pour plus d'informations sur l'accès des autorités répressives nationales aux systèmes d'information de l'UE: FRA (2018), *Interoperability and fundamental rights implications — Opinion of the European Union Agency for Fundamental Rights*, avis de la FRA 1/2018 (Interopérabilité), Vienne, 11 avril 2018; FRA (2018), *The revised Visa Information System and its fundamental rights implications — Opinion of the European Union Agency for Fundamental Rights*, avis de la FRA 2/2018 (VIS), Vienne, 30 août 2018; FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Office des publications, Luxembourg, juin 2017; FRA (2016), *Opinion on the impact of the proposal for a revised Eurodac Regulation on fundamental rights*, avis de la FRA 6/2016 (Eurodac), Vienne, 22 décembre 2016.

5.3. Projets de recherche financés par l'UE dans le domaine de la technologie de reconnaissance faciale

L'UE finance, dans le cadre du programme européen «Horizon 2020» sur les sociétés sûres pour la période 2018-2020 ([67]), plusieurs projets de recherche sur l'application potentielle de la technologie de reconnaissance faciale dans le domaine de la sécurité et de la gestion des frontières, comme le montrent les exemples suivants.

Dans le domaine de la gestion des frontières, le projet Protect (Pervasive and UseR Focused BiomeTrics BordEr ProjeCT) a exploré l'application des technologies de reconnaissance faciale dans le développement d'un «système amélioré d'identification sans contact des personnes basé sur la biométrie» lors du franchissement des frontières extérieures. Les exigences en matière de protection de la vie privée et les préoccupations qu'une telle technologie pourrait susciter ont également été examinées dans le cadre de ce projet. D'autres projets se sont concentrés sur de nouveaux concepts de mobilité pour la sécurité des frontières terrestres**.** Dans ce cadre, le projet iBorderCtrl a étudié un système multi-modules qui pourrait accélérer les procédures de contrôle aux frontières et les exigences d'identification. S'appuyant sur une combinaison de technologies de pointe, telles qu'un outil de mise en correspondance des visages et un système de détection automatique du mensonge, les recherches visent à déterminer si cette technologie peut aider les gardes-frontières à détecter les voyageurs qui sont de bonne foi, mais aussi les passagers qui font des déclarations mensongères.

En outre, des recherches sont en cours pour comprendre l'acceptation sociale des technologies de reconnaissance faciale et l'attitude du public à leur égard. Le projet Persona relatif à l'acceptation des solutions de franchissement des points de passage sans contact du point de vue du respect de la vie privée, éthique, réglementaire et sociétal (Privacy, ethical, regulatory and social no-gate crossing point solutions acceptance), par exemple, vise à concevoir des méthodes d'analyse d'impact adaptées pour évaluer correctement les effets des nouvelles technologies de contrôle sans contact lors du franchissement des frontières, y compris les technologies de reconnaissance faciale. Elles examineront également leur acceptabilité, en tenant compte du comportement humain, du sexe, des cadres juridiques, des préoccupations relatives au respect de la vie privée, du point de vue sociétal et du risque potentiel de discrimination ([68]).

En matière de sécurité, dans le cadre de l'évaluation de la mise en œuvre décennale des décisions de Prüm ([69]), la Commission européenne réalise une étude de faisabilité sur l'amélioration des capacités du système afin optimiser l'échange d'informations ([70]). Les États membres de l'UE discutent également de l'extension du système pour y inclure davantage de données biométriques. L'Autriche est chef de file du groupe de discussion sur la «reconnaissance faciale» ([71]).

La Commission européenne finance également un projet de recherche intitulé «Towards the European Level Exchange of Facial Images» (Telefi), qui examinera «comment la reconnaissance faciale est actuellement utilisée pour les enquêtes pénales dans les États membres de l'UE». Elle accordera également une attention particulière aux possibilités de mise en œuvre de l'échange d'images faciales dans le cadre Prüm ([72]). Le projet est mis en œuvre par les départements de médecine légale de Finlande, de Lettonie, de Suède et des Pays-Bas, sous la direction du ministère estonien de la justice.

([67]) Le nom officiel du programme est «Des sociétés sûres — protéger la liberté et la sécurité de l'Europe et de ses citoyens». Pour des informations supplémentaires, voir la page web de la Commission sur la recherche en matière de sécurité.

([68]) Projet financé au titre du programme H2020-EU.3.7.6 — Garantir le respect de la vie privée et de la liberté, y compris sur l'internet, et renforcer la compréhension, du point de vue sociétal, juridique et éthique, de tous les domaines de la sécurité, du risque et de la gestion, thématique: SEC-18-BES-2017 — Acceptance of no gate crossing point solutions.

([69]) Les décisions de Prüm permettent l'échange à grande échelle de données relatives aux empreintes digitales, aux profils ADN et à l'immatriculation des véhicules entre les parties contractantes du traité de Prüm et d'autres États membres de l'UE à des fins de répression et de sécurité nationale. Voir la décision 2008/615/JAI du Conseil relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, et la décision 2008/616/JAI du Conseil concernant la mise en œuvre de la décision 2008/615/JAI, 23 juin 2008.

([70]) Conseil de l'Union européenne, 10911/199, 8 juillet 2019.

([71]) Ibid.; Monroy, M., «European Union plans borderless query of facial images», 22 juillet 2019.

([72]) Voir le site web du projet «Towards the European Level Exchange of Facial Images» (Telefi).

6. Implications en matière de droits fondamentaux de l'utilisation de la reconnaissance faciale en temps réel: considérations d'ordre général

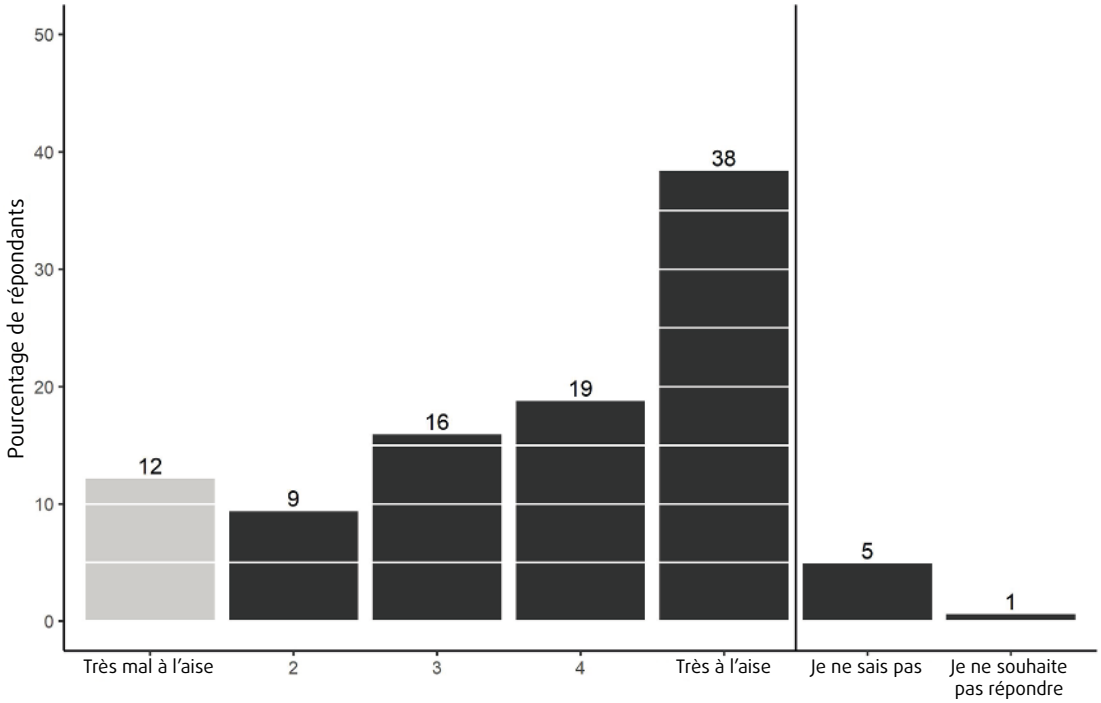
L'utilisation de la technologie de reconnaissance faciale comporte à la fois des risques et des possibilités en ce qui concerne les droits fondamentaux. Elle entraîne de nombreux défis en matière de droits fondamentaux qui résultent de la position de faiblesse des personnes dont les images faciales sont capturées et ensuite comparées à une «liste de surveillance». En parallèle, la technologie de reconnaissance faciale peut offrir une protection plus rapide — par exemple en aidant à retrouver des enfants disparus — et peut contribuer à la détection des fraudes et à l'usurpation d'identité.

Avec de nombreuses questions sans réponse liées à l'utilisation et à la précision de la technologie, la société civile a exprimé de grandes inquiétudes quant à l'utilisation des technologies de reconnaissance faciale, et en particulier des technologies de reconnaissance faciale en temps réel. Cette section présente la manière dont la reconnaissance faciale est perçue et analyse les implications de cette technologie en matière de droits fondamentaux en général. La section 7 examine les droits fondamentaux individuels qui sont les plus affectés.

6.1. Perceptions du public

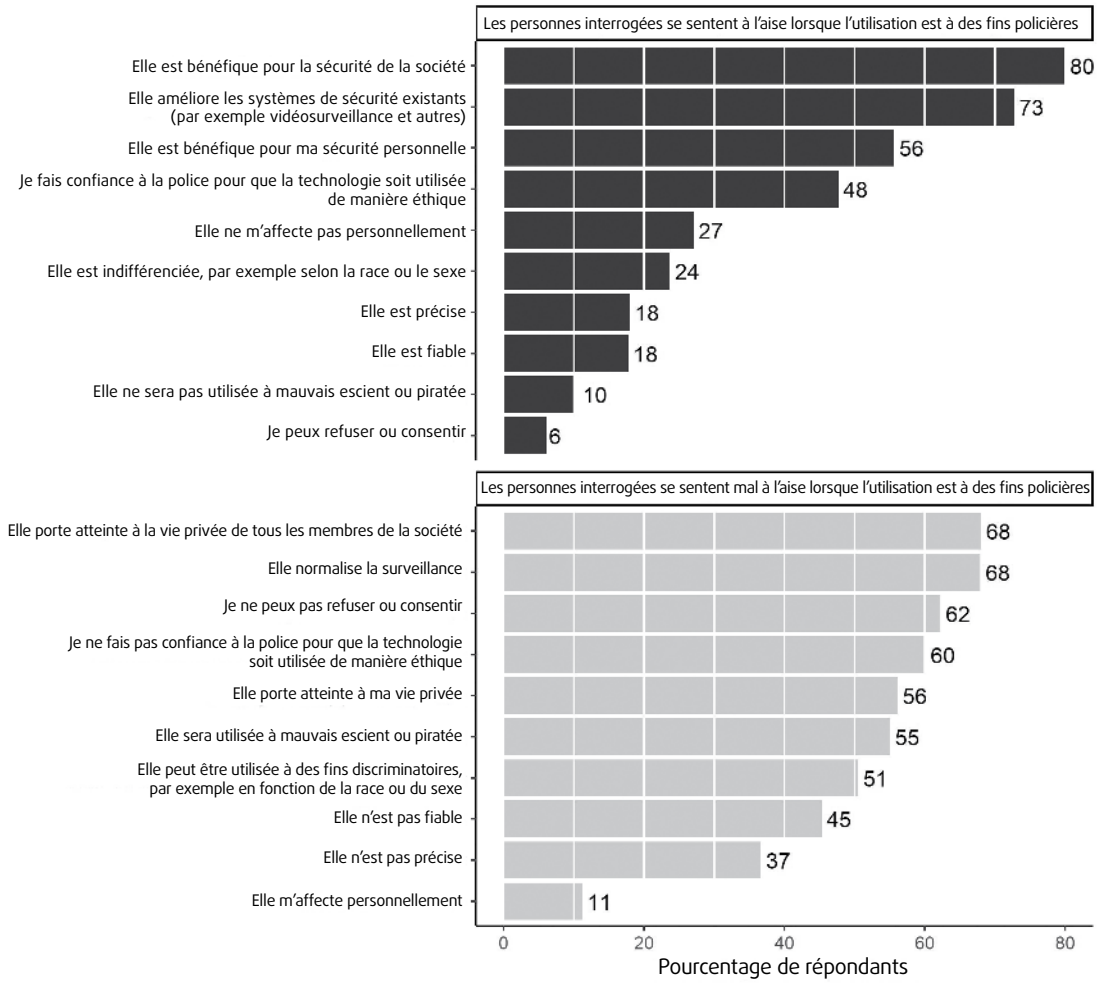
Aucune évaluation détaillée de la mesure dans laquelle les personnes jugent l'utilisation des technologies de reconnaissance faciale intrusive n'a été réalisée au niveau de l'UE. Toutefois, il semble qu'une partie de la population s'oppose fermement à l'utilisation de la reconnaissance faciale. Dans une enquête menée par la FRA en 2015 — portant sur 1 227 ressortissants de pays tiers à sept points de passage frontaliers —, 12 % de tous les répondants ont indiqué se sentir très mal à l'aise lorsque leur image faciale était utilisée lors du franchissement de la frontière (voir la figure 1), 18 % ont considéré que le fait de fournir une image faciale à une frontière était très intrusif pour leur vie privée, et 26 % ont déclaré que cet acte était humiliant. Il existe des différences entre les

Figure 1 — Degré d'aisance des voyageurs face au fait de fournir des images faciales aux frontières, 2015



Notes: *Question: «Que ressentez-vous vis-à-vis de l'utilisation des images faciales lors du franchissement de la frontière?»; N = 1 227.*
Source: *FRA, 2015 (d'après une enquête réalisée à sept points de passage frontaliers).*

Figure 2 — Raisons pour lesquelles les personnes se sentent à l'aise ou mal à l'aise lorsque la reconnaissance faciale est utilisée au Royaume-Uni, 2019



Notes: *Le graphe supérieur comprend les répondants qui ont indiqué des valeurs de 6 à 10 à la question sur le fait de se sentir à l'aise avec l'utilisation de la technologie de reconnaissance faciale à des fins policières (sur une échelle de 1 à 10, où 1 signifie pas à l'aise, n = 2 757). Le graphe inférieur comprend les répondants qui ont indiqué ne pas se sentir à l'aise (valeurs 1 à 5, n = 1 180).*

Source: *Données provenant de l'institut Ada Lovelace, 2019, d'après une enquête en ligne au Royaume-Uni.*

nationalités, les Russes et les citoyens des États-Unis étant moins préoccupés, tandis que les citoyens chinois et les personnes originaires d'autres régions du monde le sont davantage. L'enquête n'a pas fait apparaître de différences nettes en ce qui concerne le degré d'humiliation en fonction de l'âge et du sexe ([73]). Les résultats d'une telle enquête pourraient vite évoluer compte tenu du développement rapide de la technologie et du fait que les personnes sont plus fréquemment exposées à cette technologie.

Selon les experts interrogés par la FRA, dans une autre enquête menée dans le cadre de tests sur les technologies de reconnaissance faciale en temps réel menés à Nice (France), seuls 3 % des 900 répondants se sont opposés à l'utilisation de la technologie de reconnaissance faciale.

Une enquête plus importante a été menée au Royaume-Uni auprès de la population générale pour connaître l'opinion des personnes sur la reconnaissance faciale ([74]). Les résultats de l'enquête montrent que, parmi la population générale du Royaume-Uni, seuls 9 % des personnes se sentent complètement mal à l'aise lorsque la reconnaissance faciale est utilisée à des fins policières, et 10 % lorsqu'elle est utilisée dans les aéroports. Cependant, 24 % ne se sentent pas à l'aise avec l'utilisation de la reconnaissance faciale dans les transports publics, 28 % dans

([73]) D'après FRA (2015), *Fundamental Rights Agency Survey results*, joint au document de l'eu-LISA (2015), *Smart Borders Pilot Project — Technical Report Annexes — Volume 2.*

([74]) Institut Ada Lovelace (2019), *Beyond face value: public attitudes to facial recognition technology*.

les écoles, 37 % dans les supermarchés et 37 % sur le lieu de travail. Il apparaît que, si les personnes ont généralement tendance à se sentir plus à l'aise avec l'utilisation des technologies de reconnaissance faciale à des fins policières, beaucoup ne sont pas satisfaits de l'utilisation de ces technologies dans la vie quotidienne. La figure 2 montre que, selon cette enquête menée au Royaume-Uni, les principales raisons de se sentir à l'aise sont liées à un renforcement de la sécurité, tandis que les principales raisons de se sentir mal à l'aise sont liées à des ingérences dans la vie privée des personnes.

6.2. Exigences d'une ingérence justifiée dans les droits fondamentaux

Le plein respect des droits fondamentaux est une condition préalable à toute activité répressive, quelles que soient les technologies utilisées. Le droit européen et international des droits de l'homme fournit un cadre normatif pour la conception, le développement et le déploiement des technologies de reconnaissance faciale. Il aide à déterminer si une utilisation spécifique de la technologie de reconnaissance faciale est conforme ou non aux droits de l'homme ([75]).

La section 7 porte sur les principaux droits fondamentaux affectés par les technologies de reconnaissance faciale. Ces droits ne sont généralement pas absolus et peuvent donc être soumis à des limitations ([76]). Cette sous-section présente les étapes à suivre pour déterminer si un droit de la Charte peut être restreint ou non. Les exigences spécifiques à un droit individuel (en particulier celles relatives aux atteintes au droit au respect de la vie privée et à la protection des données à caractère personnel) sont analysées dans la section 7.

Jusqu'à présent, les tests et les déploiements des technologies de reconnaissance faciale dans les États membres de l'UE par les autorités publiques se sont principalement concentrés sur la précision technique et n'ont pas évalué les implications en matière de droits fondamentaux de manière plus large. L'accent a été mis sur la qualité des images et les taux d'erreur. Ces résultats sont importants, mais ne sont qu'un aspect. Si la technologie de reconnaissance faciale était parfaite en termes de précision, d'autres questions subsisteraient néanmoins. Par exemple, la technologie de reconnaissance faciale en temps réel, qui consiste à soumettre des personnes à une reconnaissance faciale sans nécessairement leur consentement éclairé, les place dans une position de faiblesse et potentiellement humiliante.

L'utilisation des technologies de reconnaissance faciale en temps réel est donc aussi liée plus largement au droit à la dignité humaine. La dignité humaine est le fondement de tous les droits fondamentaux garantis par la Charte des droits fondamentaux de l'UE ([77]). L'article 1 de la Charte stipule que la dignité humaine est inviolable et qu'elle doit être respectée et protégée. La Cour de justice de l'Union européenne (CJUE) a confirmé dans sa jurisprudence que le droit fondamental à la dignité fait partie du droit européen ([78]).

Les données biométriques, y compris les images faciales, doivent être traitées de manière à respecter la dignité humaine. Le traitement des images faciales peut affecter la dignité humaine de différentes manières, comme l'illustrent les exemples suivants:

- Les personnes peuvent se sentir mal à l'aise de se rendre dans des lieux publics sous surveillance. Elles peuvent modifier leur comportement, se retirer de la vie sociale, ne pas se rendre dans les lieux centraux sous surveillance, éviter les gares ou refuser d'assister à des événements culturels, sociaux ou sportifs. Selon la mesure dans laquelle les technologies de reconnaissance faciale en temps réel sont appliquées, l'impact de ce que les personnes peuvent percevoir comme des technologies de surveillance sur leur vie peut être si important qu'il affecte leur capacité à vivre dignement.

- La FRA a documenté des exemples où les autorités ont fait un usage excessif de la force pour prendre les empreintes digitales de personnes arrivant à la frontière ([79]). Des situations similaires peuvent aussi hypothétiquement se produire pour forcer les personnes à passer par des endroits où des images faciales sont capturées. L'interdiction de l'usage excessif de la force découlant de l'article 4 de la Charte, qui interdit la torture, les traitements inhumains et dégradants, est une garantie essentielle lorsque des données biométriques sont prélevées sur des personnes ([80]).

([75]) Voir également Fussey, P., et Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, université d'Essex, Human Rights Centre, juillet 2019, p. 31; McGregor, L., Murray, D., et Ng, V. (2019), «International Human Rights Law as a Framework for Algorithmic Accountability», *International and Comparative Law Quarterly* 68, p. 309-343.

([76]) Scheinin, M., et Sorell, T. (2015), *SURVEILLE Deliverable D4.10 — Synthesis report from WP4, merging the ethics and law analysis and discussing their outcomes*, p. 8.

([77]) Barak, A. (2015), «Human dignity as a framework right (mother-right)», *Human Dignity: The Constitutional Value and the Constitutional Right*, chapitre 9, Cambridge University Press, Cambridge, 2015, p. 156-169.

([78]) Arrêt de la Cour de justice du 9 octobre 2001, *Pays-Bas/Parlement et Conseil*, C-377/98, ECLI:EU:C:2001:523, points 70 à 77.

([79]) FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Office des publications, Luxembourg, mars 2018, p. 52-55; FRA (2019), *Fundamental Rights Report 2019*, Office des publications, Luxembourg, juin 2019, p. 133.

([80]) FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Office des publications, Luxembourg, février 2018.

- Dans le cas où les autorités répressives obtiennent de nombreuses concordances lors du déploiement de technologies de reconnaissance faciale (par exemple à l'occasion d'un grand événement public), elles peuvent être amenées à arrêter et à contrôler un plus grand nombre de personnes. Cela nécessite des ressources importantes en termes de personnel de police, en particulier lorsque de nombreuses personnes sont arrêtées à tort en raison de correspondances erronées, comme cela peut être le cas lorsque les images faciales sont extraites de caméras de vidéosurveillance. Le risque d'un comportement inapproprié de la police dû au stress augmente, ce qui peut porter atteinte à la dignité de la personne arrêtée. L'interaction avec des personnes ayant fait l'objet d'une correspondance requiert une attention particulière. Les agents doivent recevoir une formation adéquate sur la nécessité de garantir le plein respect du droit à la dignité humaine et sur la manière d'éviter le risque de tensions, y compris lorsqu'ils ont affaire à des personnes vulnérables. Les médias du Royaume-Uni ont rapporté une affaire concernant une personne qui a évité des caméras utilisant la technologie de reconnaissance faciale à Londres et qui a ensuite été condamnée à une amende pour atteinte à l'ordre public. Les circonstances concrètes de l'incident sont toutefois contestées ([81]).

Le contrôle par des organismes indépendants constitue un moyen important de promouvoir le respect des droits fondamentaux. Cela s'applique à de nombreux domaines différents, notamment le contrôle par les autorités responsables de la protection de l'enfance dans le cas d'enfants exposés à des risques d'exploitation, de maltraitances ou de négligence mais aussi les organes de surveillance internationaux établis pour prévenir la torture et les traitements inhumains ou dégradants. Le contrôle indépendant est également une composante essentielle du droit européen en matière de protection des données ([82]), l'article 8, paragraphe 3, de la Charte y faisant expressément référence. Compte tenu des enjeux relatifs aux droits fondamentaux et de leur complexité, un contrôle indépendant est essentiel pour protéger effectivement les personnes dont les droits peuvent être affectés par la technologie de reconnaissance faciale.

En ce qui concerne les droits fondamentaux qui peuvent faire l'objet de restrictions, l'article 52, paragraphe 1, de la Charte fixe le cadre. Les ingérences dans les droits fondamentaux ne peuvent être justifiées que si elles respectent les exigences de la Charte et de la Convention européenne des droits de l'homme (CEDH), dans le cas de droits de la Charte correspondant à des droits garantis par la CEDH (article 52, paragraphe 3, de la Charte) ([83]).

En vertu de l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits fondamentaux doit:

- être prévue par la loi;
- répondre effectivement à des objectifs d'intérêt général reconnus par l'Union et au besoin de protection des droits et libertés d'autrui;
- respecter le contenu essentiel du droit; et
- être proportionnée ([84]).

La CJUE a insisté sur le fait que toutes ces exigences doivent être respectées. La Cour a également souligné que toute limitation de l'exercice des droits et libertés reconnus par la Charte doit respecter le contenu essentiel desdits droits et libertés ([85]). Cela signifie que les droits fondamentaux peuvent être limités, dans une certaine mesure, mais pas entièrement ignorés. Une fois qu'il a été établi que le caractère inaliénable et essentiel d'un droit n'est pas violé par une mesure, l'examen de la nécessité et de la proportionnalité décrites dans la Charte doit être effectué dans une prochaine étape au regard des aspects non fondamentaux de ce droit ([86]).

Un objectif d'intérêt général — tel que la prévention de la criminalité ou la sécurité publique — n'est pas, en soi, suffisant pour justifier une ingérence. Toute ingérence dans un droit garanti par la Charte doit être examinée afin de déterminer si l'objectif légitime donné ne pourrait

([81]) Fussey, P., et Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, université d'Essex, Human Rights Centre, juillet 2019, p. 104.

([82]) Directive en matière de protection des données dans le domaine répressif, chapitre VI; RGPD, chapitre VI.

([83]) Charte, article 52, paragraphe 3: «Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention.»

([84]) Comme l'a également réitéré et expliqué la CJUE, voir par exemple: l'arrêt de la Cour de justice du 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia*, C-73/07, ECLI:EU:C:2008:727, point 56; l'arrêt de la Cour de justice du 9 novembre 2010, *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, ECLI:EU:C:2010:662, point 77; l'arrêt de la Cour de justice du 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.*, C-293/12 et C-594/12, ECLI:EU:C:2014:238, point 52; l'arrêt de la Cour de justice du 6 octobre 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, point 92; et l'arrêt de la Cour de justice du 17 décembre 2015, *WebMindLicenses*, C-419/14, ECLI:EU:C:2015:832, points 69 et 80 à 82.

([85]) Voir l'arrêt de la Cour de justice du 6 octobre 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, points 94 et 95, qui fait référence à l'article 52, paragraphe 3, de la Charte. Voir également Scheinin, M., et Sorell, T. (2015), *SURVEILLE Deliverable D4.10 — Synthesis report from WP4, merging the ethics and law analysis and discussing their outcomes*, 7 avril 2015, p. 9.

([86]) Voir, par exemple, Brkan, M. (2019), «The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning», *German Law Journal* 20, p. 867.

pas être atteint à l'aide d'autres moyens portant moins atteinte au droit garanti ([87]).

Des exigences similaires sont également imposées par la CEDH, tel qu'interprété par la Cour européenne des droits de l'homme (CouEDH). Selon un examen en trois volets élaboré par la CouEDH, toute ingérence dans les droits doit: poursuivre un objectif légitime; être conforme à la loi, c'est-à-dire nécessiter une base juridique appropriée répondant à des exigences qualitatives (publique, précise et prévisible) ([88]); et être nécessaire dans une société démocratique (examen de la nécessité et de la proportionnalité) ([89]). Un quatrième examen mené par la CouEDH a également utilisé le concept de «contenu essentiel», qui peut être déduit de l'objet et du but de la CEDH dans sa globalité ([90]). La jurisprudence de la CouEDH a identifié les éléments suivants pour déterminer si une mesure est «nécessaire dans une société démocratique» — par exemple, que l'ingérence doit correspondre à un besoin social impérieux, qu'elle doit être proportionnée, et que les raisons invoquées pour justifier l'ingérence doivent être pertinentes et suffisantes ([91]). En ce qui concerne l'utilisation des nouvelles technologies, la CouEDH a observé, dans l'affaire *S. et Marper c. Royaume-Uni*, que les États doivent «trouver un juste équilibre» entre la protection des droits fondamentaux et le développement des nouvelles technologies ([92]). Cela s'applique également à l'introduction des technologies de reconnaissance faciale pour soutenir les autorités répressives et la gestion des frontières.

Cette évaluation doit être effectuée pour chaque mode d'utilisation de la technologie. Elle doit couvrir tous les droits fondamentaux pertinents et prendre en compte tous les éléments, depuis l'objectif légitime que la technologie veut atteindre et la manière dont les images faciales sont capturées (par exemple caméras de vidéosurveillance, caméras piétons, applications de téléphonie mobile, etc.) jusqu'au degré d'erreur qu'elle entraîne, afin de permettre une évaluation éclairée de la nécessité et de la proportionnalité de son utilisation. Plus la technologie est intrusive, plus l'examen doit être strict.

En ce qui concerne son objectif légitime, les résultats de l'examen de la nécessité et de la proportionnalité seront différents selon qu'il facilite la vérification de l'identité d'une personne — comme lors des vérifications aux frontières dans les aéroports (comparaison «un-à-un») — ou qu'il est utilisé dans le cadre d'enquêtes pénales pour comparer l'image faciale d'une personne à une liste de surveillance (comparaison «un-à-plusieurs»). Dans ce deuxième cas, la gravité de l'infraction faisant l'objet de l'enquête joue un rôle important. Les exemples d'utilisation mentionnés dans la section 5 indiquent que, d'une manière générale, les autorités ont déployé ou testé la technologie pour améliorer l'efficacité du travail de la police, notamment réussir à identifier plus facilement les personnes recherchées et réduire les coûts. Les autorités ont également mentionné l'incapacité de la main-d'œuvre humaine à passer en revue toutes les séquences vidéo produites par les caméras de vidéosurveillance pour justifier les tests sur les technologies de reconnaissance faciale. La FRA n'a pas été en mesure d'obtenir une vision complète des types d'infractions pour lesquelles les autorités répressives ont utilisé ou testé la technologie.

En ce qui concerne la précision, il a été rapporté que les tests effectués à Nice ont parfaitement, fonctionné, sans aucune erreur. Toutefois, l'utilisation des technologies de reconnaissance faciale s'accompagne généralement d'erreurs. L'examen de plus grande envergure portant sur la précision des technologies de reconnaissance faciale est disponible auprès de l'Institut national des normes et des technologie (NIST) du ministère du commerce des États-Unis, qui réalise en continu un test comparatif auprès des fournisseurs portant sur la vérification et l'identification. Les résultats montrent une forte augmentation des taux de précision, avec un taux d'erreur actuellement inférieur à 0,2 % pour des galeries comptant 12 millions de personnes ([93]). Pourtant, il existe une relation complexe entre les faux positifs (c'est-à-dire le fait d'arrêter des personnes innocentes) et les faux négatifs (c'est-à-dire le fait de ne pas pouvoir identifier la personne d'intérêt). Une évaluation de la proportionnalité doit équilibrer le compromis entre les faux positifs et les faux négatifs, comme illustré ci-après. La question est de savoir quel nombre de personnes innocentes signalées par le système et arrêtés par la police est acceptable dans le but de réussir à identifier une personne d'intérêt. Le résultat de cette évaluation varie en fonction de l'importance de l'identification d'une personne spécifique et du préjudice causé par l'arrestation de personnes innocentes.

Un exemple frappant nous vient de l'examen effectué en Allemagne. En utilisant en parallèle trois systèmes logiciels de reconnaissance faciale différents, et en analysant les correspondances dans les cas où au moins un des trois systèmes a établi une correspondance, les tests effectués à Berlin ont eu un taux d'échec moyen (faux négatifs parmi tous les négatifs) de 8,8 %, avec un taux de

([87]) Arrêt de la Cour de justice du 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.*, C-293/12 et C-594/12, ECLI:EU:C:2014:238.

([88]) Concernant les exigences de la «qualité du droit», voir CouEDH, *Gorlov et autres c. Russie*, n°s 27057/06, 56443/09 et 25147/14, 2 juillet 2019, paragraphe 97.

([89]) Voir, par exemple, CouEDH, *S. et Marper c. Royaume-Uni* (GC), n°s 30562/04 et 30566/04, 4 décembre 2008, paragraphes 95 à 104.

([90]) Scheinin, M., et Sorell, T. (2015), *SURVEILLE Deliverable D4.10 — Synthesis report from WP4, merging the ethics and law analysis and discussing their outcomes*, 7 avril 2015, p. 9.

([91]) Voir par exemple: CouEDH, *Khelili c. Suisse*, n° 16188/07, 18 octobre 2011; CouEDH, *S. et Marper c. Royaume-Uni* (GC), n°s 30562/04 et 30566/04, 4 décembre 2008; CouEDH, *K & T c. Finlande*, n° 25702/94, 12 juillet 2001; CouEDH, *Z c. Finlande*, n° 22009/93, 25 février 1997; CouEDH, *Huvig c. France*, n° 11105/84, 24 avril 1990; CouEDH, *Leander c. Suède*, n° 9248/81, 26 mars 1987.

([92]) CouEDH, *S. et Marper c. Royaume-Uni* (GC), n°s 30562/04 et 30566/04, 4 décembre 2008, paragraphe 112.

([93]) Grother, P., Ngan, M., et Hanaoka, K. (2018), *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, NISTIR 8238.

fausses identifications positives de 0,34 %. Cela signifie que, dans un peu moins d'un cas sur dix — en moyenne et à long terme —, une personne d'intérêt ne serait pas détectée (ou, dans un peu plus de neuf cas sur dix, serait identifiée). Dans le même temps, sur 1 000 personnes traversant le système, entre trois et quatre personnes seraient identifiées à tort comme présentant une correspondance par le système. Selon les autorités allemandes, ce n'est pas acceptable, car, compte tenu du nombre de personnes qui traversent les gares chaque jour, cela conduirait à un grand nombre de personnes arrêtées à tort (ou du moins signalées à la police). Le système peut également être utilisé pour établir une correspondance uniquement lorsque les trois systèmes logiciels concordent. Cela porterait le taux d'échec à 31,9 % (ce qui signifie que, dans un cas sur trois — à long terme —, une personne d'intérêt ne serait pas détectée) et réduirait le taux de fausses identifications positives à 0,00018 %. Ce chiffre est considéré comme très faible par les autorités qui procèdent à l'examen ([94]). Utilisé dans une gare traversée par 100 000 personnes chaque jour, un tel taux signifierait que, sur une période de dix jours, environ deux personnes seraient signalées alors qu'elles ne figurent pas dans le système ([95]).

([94]) Polizeipräsidium Potsdam, *Biometrische Gesichtserkennung*, 2018.

([95]) Il est important de mentionner que les résultats des tests sont soumis à des incertitudes découlant du fait qu'il existe des écarts statistiques et que les valeurs ne sont pas réelles.

7. Droits fondamentaux les plus affectés

Cette section examine les droits fondamentaux spécifiques qui sont les plus affectés par l'utilisation des technologies de reconnaissance faciale dans le contexte de l'application de la loi. Elle se concentre sur les technologies de reconnaissance faciale en temps réel, lorsque les images faciales sont extraites de caméras de vidéosurveillance et comparées à une base de données ou à une liste de surveillance. Cette section ne constitue pas une analyse exhaustive de tous les droits fondamentaux affectés par les technologies de reconnaissance faciale, mais fournit plutôt des exemples pertinents.

7.1. Respect de la vie privée et protection des données à caractère personnel

Le droit au respect de la vie privée et le droit à la protection des données sont essentiels au déploiement de la technologie de reconnaissance faciale dans les lieux publics. Bien qu'ils soient étroitement liés, ces droits sont distincts et autonomes. Ces deux droits distincts ont également été décrits comme un droit classique (la protection de la vie privée) et un droit plus moderne (le droit à la protection des données) ([96]). Tous deux tendent à protéger des valeurs similaires, à savoir l'autonomie et la dignité humaine des individus, en leur accordant une sphère privée dans laquelle ils peuvent librement développer leur personnalité, penser et se forger des opinions. Ils constituent donc une condition essentielle à l'exercice d'autres droits fondamentaux, tels que la liberté de pensée, de conscience et de religion (article 10 de la Charte), la liberté d'expression et d'information (article 11 de la Charte), et la liberté de réunion et d'association (article 12 de la Charte) ([97]).

L'utilisation de technologies de reconnaissance faciale en temps réel implique la collecte, la comparaison et/ou le stockage d'images faciales dans un système d'information à des fins d'identification. Elle constitue donc une ingérence dans le droit à la protection des données à caractère personnel énoncé à l'article 8 de la Charte (qui reprend la législation de l'UE préexistante sur la protection des données) et dans le droit à la vie privée garanti par l'article 7 de la Charte et l'article 8 de la CEDH. Les images faciales constituent des données à caractère personnel, comme l'ont également confirmé la CJUE ([98]) et la CouEDH ([99]). La CouEDH a également précisé que l'image faciale d'une personne constitue l'un des principaux attributs de sa personnalité, car elle révèle les caractéristiques uniques de cette personne et la distingue de ses pairs. Le droit de la personne à la protection de son image faciale constitue ainsi l'une des conditions essentielles de son épanouissement personnel ([100]).

La notion de «vie privée» est une notion large, qui ne se prête pas à une définition exhaustive. Elle recouvre l'intégrité physique et morale d'une personne ainsi que de multiples aspects de son identité physique et sociale ([101]). Il existe en effet une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la vie privée ([102]). Dans d'autres contextes, la CouEDH a utilisé le concept «d'attente raisonnable en matière de respect de la vie privée» — qui fait référence à la mesure dans laquelle les personnes peuvent s'attendre au respect de leur vie privée dans les espaces publics sans être soumises à une surveillance — comme l'un des facteurs, bien qu'il ne soit pas nécessairement concluant, pour décider d'une violation du droit au respect de la vie privée. La pertinence et le champ d'application de ce concept semblent toutefois limités ([103]). De même, selon les experts de l'Organisation des Nations unies (ONU), le simple fait qu'un rassemblement se déroule en public ne signifie pas que la vie privée des participants ne peut pas être violée ([104]). Le traitement d'images faciales figurant dans des bases de données à grande échelle peut, au fur et à mesure du développement de la technologie de reconnaissance faciale, soulever des problèmes jusqu'à présent inconnus en ce qui concerne les droits à la protection de la vie privée et à la protection des données à caractère personnel. Étant donné que ces deux droits ne sont pas des droits absolus, ils peuvent être soumis à des limitations, mais toute ingérence doit être justifiée de manière adéquate ([105]) et ne peut en aucun cas compromettre le

([96]) Arrêt de la Cour de justice du 9 novembre 2010, *Volker und Markus Schecke et Eifert*, C-92/09 et C-93/09, ECLI:EU:C:2010:662, *Conclusions de l'avocat général Sharpston*, 17 juin 2010, point 71.

([97]) FRA, Conseil de l'Europe et CEPD (2018), *Manuel de droit européen en matière de protection des données — Édition 2018*, Office des publications, Luxembourg, juin 2018, p. 19.

([98]) Arrêt de la Cour de justice du 17 octobre 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670, points 22, 48 et 49.

([99]) CouEDH, *Szabó et Vissy c. Hongrie*, n° 37138/14, 12 janvier 2016, paragraphe 56.

([100]) CouEDH, *Guide sur l'article 8 de la Convention européenne des droits de l'homme — Droit au respect de la vie privée et familiale, du domicile et de la correspondance*, Conseil de l'Europe, Strasbourg, mis à jour le 31 août 2019, paragraphe 138.

([101]) CouEDH, *López Ribalda et autres c. Espagne*, n°s 1874/13 et 8567/13, 17 octobre 2019, paragraphe 87.

([102]) Ibid., paragraphe 88.

([103]) Vermeulen, M. (2015), *SURVEILLE Deliverable D4.7 — The scope of the right to private life in public places*, juillet 2014, p. 2.

([104]) ONU, Comité des droits de l'homme, *Observation générale n° 37 sur le droit de réunion pacifique (art. 21)*, projet préparé par le rapporteur, Christof Heyns, juillet 2019, paragraphe 69.

([105]) Voir également FRA, Conseil de l'Europe et CEPD (2018), *Manuel de droit européen en matière de protection des données — Édition 2018*, Office des publications, Luxembourg, juin 2018, p. 35-52.

caractère essentiel et inaliénable de ces droits, comme expliqué dans la section 6.2 ([106]).

La technologie de reconnaissance faciale en temps réel implique le traitement biométrique d'images faciales prises dans un lieu public, dans le but de déterminer l'identité d'une personne (identification «un-à-plusieurs»), et la conservation potentielle de ces images. Par conséquent, le traitement biométrique initial des images faciales, la conservation ultérieure des séquences vidéo et la comparaison des données à une «liste de surveillance» — et le fait d'alimenter cette liste avec des images faciales — constituent des ingérences dans les droits au respect de la vie privée et à la protection des données à caractère personnel ([107]). Étant donné que le traitement des données à caractère personnel constitue une limitation de ces droits, il doit être soumis à un examen strict de la nécessité et de la proportionnalité, avoir une base juridique claire et poursuivre un objectif légitime. Un tel examen doit tenir compte du contexte et de toutes les circonstances. Par conséquent, la sensibilité des données ou la manière dont elles sont utilisées sont importantes pour le contexte ([108]).

Outre les garanties en matière de droits fondamentaux et les principes clés de la protection des données découlant de l'article 8 de la Charte, tel qu'interprété par la CJUE, les garanties spécifiques prévues par l'acquis de l'UE en matière de protection des données corroborent encore le test de la nécessité et de la proportionnalité décrit à la section 6.2. En vertu de l'article 9, paragraphe 2, point g), du RGPD, le traitement des données biométriques n'est autorisé que lorsque le traitement est «nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée». L'article 10 de la directive en matière de protection des données dans le domaine répressif prévoit des conditions similaires, bien qu'un peu plus permissives ([109]).

([106]) Cour européenne des droits de l'homme (2019), *Guide sur l'article 8 de la Convention européenne des droits de l'homme — Droit au respect de la vie privée et familiale, du domicile et de la correspondance*, Conseil de l'Europe, Strasbourg, mis à jour le 31 août 2019, paragraphes 133 et 136.

([107]) Fussey, P., et Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, université d'Essex, Human Rights Centre, juillet 2019, p. 36.

([108]) CEPD (2017), *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*.

([109]) Pour une présentation plus élaborée et détaillée du test de la nécessité et de la proportionnalité au titre du droit européen, consulter FRA (2018), *Guide pour la prévention du profilage illicite aujourd'hui et demain*, Office des publications, Luxembourg, décembre 2018, p. 35-38.

La collecte et le traitement des images faciales à des fins de reconnaissance faciale doivent être strictement conformes au droit européen en matière de protection des données. Conformément aux grands principes juridiques de la protection des données, le traitement des images faciales doit être:

a) licite, loyal et transparent;

b) avoir une ou des finalités déterminées, explicites et légitimes (clairement définies dans le droit de l'État membre ou le droit de l'Union); et

c) se conformer aux exigences de minimisation des données, d'exactitude des données, de limitation de la conservation, de sécurité des données et de responsabilité ([110]).

Licite, loyal et transparent

La fourniture transparente et claire d'informations est de la plus haute importance dans le contexte des technologies de reconnaissance faciale en temps réel, étant donné que les images faciales des personnes sont généralement capturées par des caméras dans des lieux publics à leur insu et sans leur consentement. Le RGPD et la directive en matière de protection des données dans le domaine répressif comportent des dispositions garantissant le principe de transparence et le droit à l'information. Le droit à la protection des données à caractère personnel exige un traitement loyal, ce qui implique d'informer de manière adéquate les personnes dont les images faciales sont prises. L'article 5, paragraphe 1, du RGPD stipule que «les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée». Le considérant 26 de la directive en matière de protection des données dans le domaine répressif reprend les mêmes exigences. De même, le droit à l'information est une condition préalable à l'exercice par l'enfant de son droit à être entendu dans les procédures judiciaires ou administratives qui l'intéressent, qui est protégé par l'article 12 de la Convention des Nations unies relative aux droits de l'enfant (CNUDE) et l'article 24, paragraphe 1, de la Charte. La communication d'informations est non seulement une exigence de transparence en vertu de la législation de l'UE sur la protection des données, mais elle promeut également le respect de la dignité de l'individu.

Les responsables du traitement doivent prendre des mesures appropriées pour fournir des informations en ce qui concerne «le traitement à la personne concernée d'une forme concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples» ([111]).

([110]) Directive en matière de protection des données dans le domaine répressif, article 4; RGPD, article 5.

([111]) Directive en matière de protection des données dans le domaine répressif, article 12; RGPD, article 12, paragraphe 1.

Les articles 13 et 14 du RGPD et l'article 13 de la directive en matière de protection des données dans le domaine répressif exigent que les personnes soient informées de l'identité et des coordonnées du responsable du traitement, de la finalité du traitement des données, des durées de conservation, du droit de demander l'accès aux données stockées et leur effacement ou leur rectification, ainsi que du droit d'introduire une réclamation auprès d'une autorité de contrôle. Toutefois, la directive en matière de protection des données dans le domaine répressif prévoit certaines exceptions possibles à cette obligation à l'article 13, paragraphe 3, pour éviter de gêner ou de nuire à des enquêtes en cours, ou pour protéger la sécurité publique et la sécurité nationale. Ces scénarios sont d'une importance majeure lorsque des technologies de reconnaissance faciale sont envisagées. Les finalités potentielles actuellement discutées et invoquées pour l'utilisation des technologies de reconnaissance faciale pourraient ne fonctionner qu'en l'absence de consentement éclairé ou de possibilité de se soustraire (par exemple, en cas de recherche de terroristes ou d'autres criminels présumés). Par conséquent, cette limitation du droit fondamental d'être informé et du consentement au traitement des données, associée aux restrictions du droit d'accès aux données stockées, doit être solidement justifiée.

Le comité européen de la protection des données précise que les États membres ont l'obligation d'informer les personnes concernées des dispositifs de vidéosurveillance existants. Ces informations doivent être fournies au moyen d'un avertissement situé à une distance raisonnable des lieux surveillés, et d'informations accessibles sans avoir à entrer dans la zone surveillée. Il peut s'agir d'une fiche d'information, d'un lien vers un site web détaillant les informations sur la surveillance, d'un numéro de téléphone pour recevoir des informations complémentaires ou d'une application permettant de localiser les dispositifs vidéo ([112]).

Le processus d'extraction des caractéristiques biométriques d'un visage, qui rend le visage disponible pour d'autres traitements, modifie le niveau d'intrusion du fait de la disponibilité de nouveaux moyens technologiques. Par conséquent, la disponibilité d'une image faciale dans une base de données est différente de l'application d'un logiciel qui extrait des caractéristiques uniques d'une image faciale, indépendamment du fait que les caractéristiques extraites sont en fait comparées à une liste de surveillance. À la suite de l'argumentation du commissaire à la protection des données de la ville de Hambourg, un équilibre précédemment spécifié par la loi entre l'ingérence des autorités à des fins répressives et le droit à l'autodétermination informationnelle est significativement modifié au détriment de ce droit. En outre, le commissaire à la protection des données considère que les technologies de reconnaissance faciale offrent des possibilités de persécution et un mode d'intrusion entièrement nouveaux, qui nécessitent une réglementation autonome et spécifique ([113]).

Finalités déterminées, explicites et légitimes

Le principe de la limitation de la finalité est l'un des principes fondamentaux du droit européen en matière de protection des données ([114]). Ce principe se retrouve à l'article 8, paragraphe 2, de la Charte, ainsi qu'à l'article 5, paragraphe 1, point b), du RGPD et à l'article 4, paragraphe 1, point b), de la directive en matière de protection des données dans le domaine répressif. Il exige que les données à caractère personnel ne soient traitées qu'à des fins déterminées, qui doivent être explicitement définies par la loi. La personne concernée doit être en mesure de prévoir la finalité du traitement de ses données ([115]). Ces principes s'appliquent de la même façon dans le cadre du traitement des données via les technologies de reconnaissance faciale. Le principe de la limitation de la finalité implique également l'interdiction de la conservation illimitée de ces données.

Dans ce contexte, la finalité du traitement des images faciales via les technologies de reconnaissance faciale doit être strictement déterminée — avec un seuil élevé, consistant essentiellement en la finalité de lutter contre le terrorisme et d'autres formes graves de criminalité, qui est la limitation de la finalité bien établie en vertu du droit de l'UE pour l'accès des autorités répressives à diverses bases de données de l'UE à grande échelle. Une autre finalité est que le traitement pourrait également être utilisé pour identifier les personnes disparues et les victimes de la criminalité, y compris les enfants.

En concevant des systèmes d'information, y compris des systèmes de reconnaissance faciale, pour lutter contre les formes graves de criminalité et le terrorisme, améliorer la sécurité publique et lutter contre l'immigration clandestine, il existe un risque d'évolution progressive des fonctions — ce qui signifie que les données à caractère personnel (les images faciales) peuvent être utilisées à des fins qui n'étaient pas envisagées initialement. Dans le cas de l'interopérabilité des bases de données de l'UE à grande échelle, des garanties doivent être mises en œuvre pour s'assurer que la technologie de reconnaissance faciale

([112]) Comité européen de la protection des données (2019), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, Bruxelles, 10 juillet 2019, p. 21-23.

([113]) *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* (2018).

([114]) FRA, Conseil de l'Europe et CEPD (2018), *Manuel de droit européen en matière de protection des données — Édition 2018*, Office des publications, Luxembourg, juin 2018, p. 122; groupe de travail «article 29» sur la protection des données (2013), *Avis 03/2013 relatif à la limitation des finalités*, WP 2013, 00569/13/EN, Bruxelles, 2 avril 2013.

([115]) Arrêt de la Cour de justice du 29 janvier 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, *Conclusions de l'avocate générale Kokott*, 18 juillet 2007, point 53.

n'est pas utilisée illégalement pour accéder aux bases de données de l'UE à grande échelle ([116]).

Minimisation des données, exactitude des données, limitation de la conservation, sécurité des données et responsabilité

Les données doivent également être collectées, traitées et conservées en toute sécurité et le traitement illicite des données doit être évité et détecté ([117]). Une question connexe est la prévention de l'accès et de l'utilisation non autorisés des données à caractère personnel traitées par les technologies de reconnaissance faciale. L'article 32 du RGPD et l'article 29 de la directive en matière de protection des données dans le domaine répressif exigent des États membres qu'ils prennent les mesures nécessaires pour éviter que des données à caractère personnel ne soient communiquées ou consultées par des personnes ou organes non autorisés. Si, à l'avenir, les systèmes de reconnaissance faciale sont rendus interopérables avec d'autres systèmes d'information, il sera particulièrement difficile de garantir la limitation de la finalité dans un tel scénario. Pour éviter les fuites de données potentielles, des recherches en cours portent sur les moyens de protéger la confidentialité des données biométriques et ainsi d'accroître la sécurité des données. Les recherches actuelles évaluent les solutions technologiques pour protéger les identifiants biométriques (modèles) ([118]).

Le droit de l'UE exige que les responsables du traitement des données protègent les données dès la conception, ce qui signifie que des mesures doivent être mises en place pour intégrer des garanties visant à protéger les droits de la personne concernée ([119]). Par conséquent, lorsqu'il est envisagé d'utiliser des technologies de reconnaissance faciale, il convient de mettre en œuvre, dès le départ, une analyse exhaustive, un plan et un processus pour protéger les droits. Conformément au RGPD et à la directive en matière de protection des données dans le domaine répressif, l'utilisation d'images faciales nécessite une analyse d'impact relative à la protection des données (AIPD), y compris une consultation préalable de l'autorité de protection des données (APD) ([120]). Les analyses d'impact relatives à la protection des données sont des outils importants pour évaluer de manière exhaustive la licéité et les risques liés à l'utilisation des technologies de reconnaissance faciale, et elles doivent être réalisées de manière approfondie. Le rôle des APD est crucial à cet égard pour la sauvegarde des droits fondamentaux, en tant qu'organes établis par la loi agissant de manière indépendante ([121]).

En effet, des efforts ont été déployés dans le cadre des tests sur les technologies de reconnaissance faciale pour réaliser une analyse d'impact. Le test allemand comprenait un plan de protection des données qui a été mis en place avec l'APD aux fins du test. L'analyse d'impact relative à la protection des données de la police du sud du Pays de Galles a également été publiée ([122]), ainsi que l'analyse de la police métropolitaine de Londres ([123]). En France, la police a informé l'APD quelques semaines avant l'essai de son intention de réaliser le test.

([116]) Pour en savoir plus sur les implications en matière de droits fondamentaux de l'interopérabilité des systèmes d'information à grande échelle, voir FRA (2018), *Interoperability and fundamental rights implications — Opinion of the European Union Agency for Fundamental Rights*, avis de la FRA 1/2018 (Interopérabilité), Vienne, 11 avril 2018.

([117]) Pour une vue d'ensemble du cadre juridique de l'UE sur la protection des données, voir FRA, Conseil de l'Europe et CEPD (2018), *Manuel de droit européen en matière de protection des données — Édition 2018*, Office des publications, Luxembourg, juin 2018.

([118]) Gomez-Barrero, M., et al. (2018), «General Framework to Evaluate Unlinkability in Biometric Template Protection Systems», *IEEE Transactions on Information Forensics and Security*, vol. 13(6), p. 1406-1420.

([119]) Directive en matière de protection des données dans le domaine répressif, article 20, paragraphe 1; RGPD, article 25, paragraphe 1.

([120]) Directive en matière de protection des données dans le domaine répressif, articles 27 et 28; RGPD, articles 35 et 36.

([121]) Des informations supplémentaires sur la manière de réaliser des analyses d'impact relatives à la protection des données, y compris dans le contexte de la vidéosurveillance, figurent dans le document du groupe de travail «article 29» sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248 rev.01, Bruxelles, telles que modifiées et adoptées en dernier lieu le 4 octobre 2017.

([122]) South Wales Police Data Protection Impact Assessment, Version 5.4, octobre 2018.

([123]) London Policing Ethics Panel, *Interim Report on Live Facial Recognition*, 2018.

Prise de décision automatisée et droit à une vérification par un être humain

L'article 22 du RGPD et l'article 11 de la directive en matière de protection des données dans le domaine répressif interdisent de manière générale la prise de décision automatisée, c'est-à-dire que la personne concernée a le droit de ne pas faire l'objet d'une «décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire». Il existe une exception à cette interdiction lorsque cela est autorisé par le droit de l'UE ou des États membres, qui prévoit des garanties appropriées pour les droits et libertés de la personne concernée, au moins le droit d'obtenir une intervention humaine de la part du responsable du traitement. Lorsque des données particulières sont concernées, telles que des images faciales, des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée doivent être mises en place.

Tous les essais et déploiements envisagés dans les États membres de l'UE prévoient une intervention humaine. Cela signifie que les correspondances basées sur les technologies de reconnaissance faciale sont signalées à des humains (par exemple des policiers), qui évalueront la correspondance et trancheront en se fondant sur cette évaluation. De nombreux faux positifs sont déjà écartés à ce stade.

Toutefois, le concept de prise de décision «automatisée» est difficile à définir et de plus amples discussions et recherches sont nécessaires. Par exemple, dans certains cas, l'intervention humaine pourrait consister à simplement «approuver» tous les résultats du système, ce qui le rend virtuellement automatisé *(*)*. À l'inverse, un autre exemple serait la situation dans laquelle des humains examineraient et ignoreraient potentiellement les résultats du système, ce qui doit également être évalué. Les recherches indiquent que les humains ne tiennent pas compte des résultats des algorithmes principalement lorsque l'issue est conforme à leurs stéréotypes (par exemple en désavantageant les groupes minoritaires). Ce comportement menace l'éventuelle valeur ajoutée du traitement automatisé, en ce sens qu'il est potentiellement plus précis ou même, dans certains cas, plus loyal que les humains *(**)*.

(*) *Veale, M., et Edwards, L. (2018), «Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling», Computer Law & Security Review, Vol 34 (2), avril 2018, p. 398-404.*

(**) *Green, B., et Chen, Y. (2019), «Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments», FAT* '19: Conference on Fairness, Accountability, and Transparency (FAT* '19), 29-31 janvier 2019.*

7.2. Non-discrimination

Il y a discrimination «lorsqu'une personne est traitée de manière moins favorable qu'une autre ne l'est, ne l'a été ou ne le serait dans une situation comparable» sur la base d'une caractéristique personnelle perçue ou réelle ([124]) (appelée «caractéristique protégée»). L'article 21 de la Charte interdit toute discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle. Cette interdiction par la Charte recoupe les droits correspondants de la CEDH (article 14) et du protocole n° 12 à la CEDH (article 12), mais elle est encore plus large. Cette formulation a permis d'établir une liste non exhaustive et ouverte étendant la protection à un large éventail de nouveaux motifs; et contrairement à l'article 14 de la CEDH, le droit à la non-discrimination prévu par la Charte est un droit autonome, qui s'applique à des situations ne devant pas nécessairement être couvertes par une autre disposition de la Charte ([125]). L'article 20 de la Charte dispose que toutes les personnes sont égales en droit.

La justification d'un traitement différent ou moins favorable est possible en vertu de la CEDH et du droit de l'UE. Une différence de traitement peut être justifiée si elle poursuit un but légitime et si les moyens mis en œuvre pour atteindre ce but sont nécessaires et proportionnés ([126]). Ces limites peuvent varier au cas par cas, en fonction des circonstances propres à chaque cas. Par exemple, dans la jurisprudence de la CouEDH, les différences de

([124]) Directive 2000/43/CE du Conseil du 29 juin 2000 relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique (JO L 180 du 19.7.2000, p. 22-26), article 2; et directive 2000/78/CE du Conseil du 27 novembre 2000 portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail (JO L 303 du 2.12.2000, p. 16-22), article 2.

([125]) FRA et Conseil de l'Europe (2018), *Manuel de droit européen en matière de non-discrimination — Édition 2018*, Office des publications, Luxembourg, juin 2018, p. 35.

([126]) Voir par exemple: CouEDH, *Burden c. Royaume-Uni* (GC), n° 13378/05, 29 avril 2008, paragraphe 60; CouEDH, *Guberina c. Croatie*, n° 23682/13, 22 mars 2016, paragraphe 69. Concernant le critère de justification dans le droit de l'UE, voir l'arrêt de la Cour de justice du 22 mai 2014, *Glatzel*, C-356/12, ECLI:EU:C:2014:350, et l'arrêt de la Cour du 13 mai 1986, *Bilka/Weber von Hartz*, 170/84, ECLI:EU:C:1986:204.

traitement considérées comme ayant une incidence sur un élément fondamental de la dignité personnelle (par exemple la race ou l'origine ethnique, le sexe, la vie privée) sont plus difficiles à justifier que les différences de traitement dans d'autres domaines ([127]).

La discrimination dans la prise de décision algorithmique fondée sur des données peut se produire pour plusieurs raisons. La discrimination peut survenir lors de la conception, des tests et de la mise en œuvre des algorithmes utilisés pour la reconnaissance faciale, par l'intermédiaire de préjugés qui sont incorporés — sciemment ou non — dans l'algorithme lui-même, et lorsque les agents décident des mesures à mettre en place suite à la détection d'une correspondance. S'il existe des différences dans les performances des algorithmes, il est généralement très difficile, voire impossible, de supprimer le préjugé par des solutions mathématiques ou programmatiques ([128]). Une cause importante de discrimination est la qualité des données utilisées pour développer les algorithmes et les logiciels ([129]). Pour être efficaces et précis, les logiciels de reconnaissance faciale doivent être alimentés par de grandes quantités d'images faciales. Un plus grand nombre d'images faciales conduit, en principe, à des prédictions plus précises. Cependant, la précision n'est pas seulement déterminée par la quantité d'images faciales traitées, mais aussi par la qualité de ces images. La qualité des données exige également un ensemble représentatif de visages représentant différents groupes de personnes ([130]). Pourtant, à ce jour, les images faciales utilisées pour développer des algorithmes dans le monde occidental surreprésentent souvent les hommes blancs, avec un nombre plus faible de femmes et/ou de personnes d'autres origines ethniques. En conséquence, les systèmes de reconnaissance faciale fonctionnent bien pour les hommes blancs, mais pas pour les femmes noires ([131]).

Les caractéristiques phénotypiques — c'est-à-dire l'expression des gènes de manière observable, comme la couleur des cheveux ou de la peau — pourraient influencer le résultat des correspondances biométriques dans les systèmes de reconnaissance faciale: la luminosité affecte la qualité des images faciales des personnes à la peau très claire, et une lumière insuffisante affecte la qualité pour les personnes à la peau très foncée ([132]). Ainsi, lors de la comparaison de leurs images faciales avec une base de données ou une liste de surveillance, ces personnes ont une plus grande probabilité de se voir attribuer à tort une correspondance en tant que faux positifs. Cela peut conduire à ce que certains groupes de personnes soient plus souvent arrêtés à tort en raison de leur couleur de peau.

L'article 26 de la Charte garantit les droits des personnes handicapées. Le handicap ne doit pas entraîner une inégalité de traitement ou une discrimination interdite par l'article 20 (égalité en droit) et l'article 21 (non-discrimination) de la Charte. Peu d'études et de discussions sont consacrées à la façon dont les technologies de reconnaissance faciale (et plus largement l'intelligence artificielle) affectent les personnes handicapées. Les types de handicaps sont multiples. On ne dispose pas de beaucoup d'informations sur la précision des technologies de reconnaissance faciale pour les différentes formes de handicaps ou de blessures au visage, c'est-à-dire les personnes dont le visage a été modifié à la suite d'un accident ou d'une paralysie, les personnes qui ont subi une chirurgie faciale ou les personnes présentant des dysmorphies craniofaciales ([133]). Des recherches supplémentaires sont nécessaires pour comprendre si les technologies de reconnaissance faciale peuvent être discriminatoires envers les personnes atteintes de certains handicaps.

Bien que la sensibilisation au risque de discrimination par les technologies de reconnaissance faciale ait considérablement augmenté au cours des dernières années, de nombreux professionnels n'y voient toujours pas d'inconvénient. Certains fonctionnaires interrogés par la FRA ont indiqué que la discrimination n'était pas un problème parce que la «technologie est neutre» ou étaient convaincus que le système fonctionne de la même manière pour les différents groupes parce que des personnes de différents groupes ont été incluses lors des tests. En fait, aucun des tests décrits dans ce document n'a analysé les résultats en termes de différences de performance selon l'origine ethnique, le sexe ou l'âge. Certains des tests ne comptaient pas suffisamment de personnes à la peau foncée parmi les volontaires pour tester les différences de performance. Par conséquent, un échantillon de personnes beaucoup plus important aurait été nécessaire pour tester une éventuelle discrimination. Le test de plus grande envergure sur les technologies de reconnaissance faciale aux États-Unis montre que les taux d'erreur diffèrent selon les caractéristiques démographiques, notamment l'âge, le sexe et le pays d'origine. En outre, les résultats en termes

([127]) FRA et Conseil de l'Europe (2018), *Manuel de droit européen en matière de non-discrimination — Édition 2018*, Office des publications, Luxembourg, juin 2018, p. 93.

([128]) FRA (2018), *Guide pour la prévention du profilage illicite aujourd'hui et demain*, Office des publications, Luxembourg, décembre 2018, p. 26; FRA (2018), *#BigData: Discrimination in data-supported decision making*, Office des publications, Luxembourg, mai 2018. Toutefois, des recherches sont en cours pour examiner cet aspect, notamment du point de vue de la vie privée et de la non-discrimination. Voir, par exemple, le site web SensitiveNets, et Morales, A., Fierrez, J., et Vera-Rodriguez, R. (2019), *SensitiveNets: Learning Agnostic Representations with Application to Face Recognition*, arXiv:1902.00334.

([129]) FRA (2019), *Data quality and artificial intelligence — mitigating bias and error to protect fundamental rights*, Office des publications, Luxembourg, juin 2019.

([130]) Ibid.

([131]) Center on Privacy and Technology at Georgetown Law (2016), *The Perpetual Line-Up*; et Buolamwini, J., et Gebru, T. (2018), «Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification», *Proceedings of Machine Learning Research* 81:1-15, 2018, Conference on Fairness, Accountability, and Transparency.

([132]) FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Office des publications, Luxembourg, mars 2018, p. 17.

([133]) Voir Medium, *Disability and AI-Bias*, 11 juillet 2019.

de différences par caractéristiques diffèrent également selon les systèmes logiciels ([134]).

La discrimination liée aux technologies de reconnaissance faciale pourrait avoir un effet négatif sur la cohésion de groupe, si les personnes issues de groupes ethniques particuliers sont arrêtées à tort avec une fréquence disproportionnée. Cela peut affecter de manière significative leur confiance envers les fonctionnaires de la police et de la gestion des frontières ([135]).

7.3. Droits de l'enfant et des personnes âgées

Les systèmes de reconnaissance faciale affectent les droits de l'enfant de différentes manières. L'article 24 de la Charte (droits de l'enfant) souligne que l'intérêt supérieur de l'enfant doit être une considération primordiale dans toutes les décisions qui concernent les enfants prises par des autorités publiques ou des acteurs privés. Les États membres doivent fournir à l'enfant la protection et les soins nécessaires à son bien-être et à son développement. L'intérêt supérieur de l'enfant est l'un des quatre principes essentiels de la CNUDE ([136]). L'intérêt supérieur de l'enfant doit également être une considération primordiale dans le contexte de l'utilisation de la technologie de reconnaissance faciale à des fins de répression et de gestion des frontières. La CJUE a également reconnu expressément la nécessité de respecter les droits de l'enfant et exige des États membres qu'ils tiennent dûment compte de la CNUDE lors de la mise en œuvre du droit de l'UE ([137]). L'acquis de l'UE en matière de protection des données offre une protection spéciale pour les enfants en ce qui concerne leurs données à caractère personnel ([138]).

En raison de la vulnérabilité particulière des enfants, le traitement de leurs données biométriques, y compris leurs images faciales, doit être soumis à un test de la nécessité et de la proportionnalité plus strict que pour les adultes.

En outre, à mesure que l'enfant grandit et que le temps passe, la précision d'une correspondance biométrique diminue. Le risque d'une correspondance erronée augmente lorsque des images faciales enregistrées à un jeune âge sont comparées plus de cinq ans après leur collecte ([139]). Les technologies actuelles de reconnaissance faciale garantissent une correspondance fiable lorsque l'enfant avait au moins six ans au moment de la capture de l'image faciale biométrique et que la correspondance est détectée dans un délai de cinq ans. En général, les recherches indiquent que la précision de la technologie de reconnaissance faciale est nettement inférieure pour les enfants de moins de 13 ans ([140]). Les tests logiciels indiquent clairement que les images des personnes les plus jeunes donnent lieu à un nombre considérablement plus élevé de faux négatifs (échecs) par rapport aux autres groupes d'âge, très probablement en raison de leur croissance rapide et du changement d'apparence de leur visage.

Le vieillissement, c'est-à-dire le temps qui s'écoule entre la prise d'une image et sa comparaison, affecte négativement la précision des technologies de reconnaissance faciale ([141]). La recherche scientifique ne permet pas de tirer des conclusions sur la fiabilité d'une correspondance lorsque plus de cinq ans se sont écoulés. Il en va de même pour les images faciales des personnes âgées si on les compare à des images prises plusieurs années auparavant.

En ce qui concerne la conservation systématique à des fins répressives de données biométriques relatives à des personnes non condamnées, la CouEDH a souligné dans l'affaire *S. et Marper c. Royaume-Uni* qu'elle pouvait être particulièrement préjudiciable dans le cas de mineurs, en raison de leur situation spéciale et de l'importance que revêtent leur développement et leur intégration dans la société ([142]). En outre, lorsque la reconnaissance faciale est utilisée pour prévenir, détecter et enquêter sur des infractions terroristes et d'autres formes graves de criminalité,

([134]) Grother, P., Ngan, M., et Hanaoka, K. (2019), *Ongoing Face Recognition Vendor Test (FRVT). Part 1: Verification*, 12 avril 2019.

([135]) FRA (2018), *Guide pour la prévention du profilage illicite aujourd'hui et demain*, Office des publications, Luxembourg, décembre 2018, p. 39.

([136]) Convention des Nations unies relative aux droits de l'enfant, New York, 20 novembre 1989 (1577 Recueil des traités des Nations unies, p. 3).

([137]) Arrêt de la Cour de justice du 27 juin 2006, *Parlement/Conseil*, C-540/03, ECLI:EU:C:2006:429, points 37 et 57; arrêt de la Cour de justice du 14 février 2008, *Dynamic Medien*, C-244/06, ECLI:EU:C:2008:85, point 39. Pour une vue d'ensemble de la protection des droits de l'enfant en vertu du droit de l'UE, voir FRA et Conseil de l'Europe (2015), *Manuel de droit européen en matière de droits de l'enfant*, Office des publications, Luxembourg, novembre 2015.

([138]) Voir RGPD, considérants 38 et 58.

([139]) FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Office des publications, Luxembourg, mars 2018, p. 109.

([140]) Centre commun de recherche de la Commission européenne, Institut pour la protection et la sécurité des citoyens (2013), *Fingerprint Recognition for Children*, Office des publications, Luxembourg, septembre 2013; Chaudhary, A., Sahni, S., et Saxena, S. (2014), *Survey: Techniques for Aging Problems in face recognition*, *MIT International Journal of Computer Science and Information Technology*, vol. 4(2), août 2014, p. 82-88; Ramanathan, N., Chellappa, R., et Biswas, S. (2009), «Computational methods for modelling facial aging: A survey», *Journal of Visual Languages and Computing* 20, p. 131-144; Galbally, J., Ferrara, P., Haraksim, R., Psyllos, A., et Beslay, L. (2019), *Study on Face Identification Technology for its Implementation in the Schengen Information System*, Office des publications, Luxembourg, juillet 2019, p. 16, 112.

([141]) Grother, P., Ngan, M., et Hanaoka, K. (2019), *Ongoing Face Recognition Vendor Test (FRVT). Part 1: Verification*, 12 avril 2019; Galbally, J., Ferrara, P., Haraksim, R., Psyllos, A., et Beslay, L. (2019), *Study on Face Identification Technology for its Implementation in the Schengen Information System*, Office des publications, Luxembourg, juillet 2019, p. 71.

([142]) CouEDH, *S. et Marper c. Royaume-Uni* (GC), n°s 30562/04 et 30566/04, 4 décembre 2008, paragraphes 124 et 125.

il est difficile de voir comment cela peut justifier le traitement d'images faciales d'enfants n'ayant pas atteint l'âge de la responsabilité pénale ([143]).

En outre, dans certains cas, l'impact de la technologie de reconnaissance faciale sur l'intérêt supérieur de l'enfant peut également être positif. Les systèmes de reconnaissance faciale peuvent contribuer à protéger le droit de l'enfant à préserver son identité ([144]). Conformément à la CNUDE, si un enfant est privé des éléments constitutifs de son identité ou de certains d'entre eux, les États doivent lui accorder une assistance et une protection appropriées, pour que son identité soit rétablie aussi rapidement que possible ([145]). Les systèmes de reconnaissance faciale utilisés par la police et les gardes-frontières peuvent aider à retrouver les enfants disparus ou enlevés, y compris les enfants victimes de la criminalité, et à empêcher l'enlèvement d'enfants. Une enquête à petite échelle de la FRA aux postes frontières montre que des enfants portés disparus sont fréquemment identifiés aux points de passage frontaliers ([146]).

Par conséquent, les technologies de reconnaissance faciale doivent tenir compte de toutes les considérations susmentionnées lors du traitement des images d'enfants. Les enfants — mais aussi les personnes âgées — ne devraient pas être mis dans une situation dans laquelle ils seraient, en raison de leur âge, affectés de manière disproportionnée par les conséquences négatives des technologies de reconnaissance faciale. Le traitement doit respecter pleinement l'article 24 (droits de l'enfant) et l'article 25 (droits des personnes âgées) de la Charte.

7.4. Liberté d'expression et liberté de réunion et d'association

La liberté d'expression et d'information est la pierre angulaire d'une société démocratique ([147]). Ce droit est consacré à l'article 11, paragraphe 1, de la Charte et à l'article 10 de la CEDH. Comme il ressort de l'article 52, paragraphe 3, de la Charte et de la jurisprudence de la CJUE ([148]), le sens et la portée de ce droit sont les mêmes que ceux de la CEDH, tel qu'interprété par la CouEDH. Les limitations qui peuvent lui être imposées ne peuvent donc pas dépasser celles prévues à l'article 10, paragraphe 2, de la CEDH ([149]).

L'article 12, paragraphe 1, de la Charte reconnaît et protège la liberté de réunion et d'association, qui correspond au même droit consacré à l'article 11 de la CEDH. En vertu de l'article 11, paragraphe 2, de la CEDH, les restrictions à ce droit ne sont autorisées que si elles sont prévues par la loi, visent l'un des buts légitimes qui y sont expressément énumérés (par exemple la sécurité nationale, la sécurité publique, la prévention de la criminalité) et constituent des mesures nécessaires dans une société démocratique. Ces limitations s'appliquent également au droit de la Charte garantissant la liberté de réunion et d'association, conformément à l'article 52, paragraphe 3, de la Charte.

L'utilisation de technologies de reconnaissance faciale pour traiter les images faciales capturées par des caméras vidéo dans l'espace public peut porter atteinte à la liberté d'opinion et d'expression d'une personne, notamment parce qu'un aspect nécessaire de l'exercice de cette liberté est l'anonymat de groupe ([150]). À cet égard, un tribunal allemand a déclaré illégale la publication de photos prises lors de manifestations via les réseaux sociaux, en raison de son effet négatif sur la liberté d'association ([151]). Le fait de savoir que des personnes sont surveillées par des technologies de reconnaissance faciale dans les espaces publics crée un effet dissuasif et peut inciter les personnes à modifier leur comportement. Elles peuvent ne pas exprimer leurs pensées de la même manière ([152]). Cela porte atteinte à leur liberté d'expression.

Si l'on décourage des personnes d'assister à des manifestations, cela va non seulement à l'encontre de leur liberté d'expression, mais constitue également une ingérence grave dans leur liberté de réunion. Le droit de réunion pacifique permet aux personnes de contribuer collectivement à modeler la société dans laquelle elles vivent d'une manière puissante mais pacifique. La liberté de réunion protège la capacité de chacun à exercer son autonomie tout en étant solidaire d'autrui ([153]). L'utilisation de technologies de reconnaissance faciale lors de rassemblements pacifiques peut décourager des personnes de manifester. Si elle est appliquée lors de manifestations violentes, la technologie peut tout de même affecter ceux qui protestent pacifiquement aux côtés des émeutiers. Le

([143]) FRA (2018), *The revised Visa Information System and its fundamental rights implications — Opinion of the European Union Agency for Fundamental Rights*, avis 2/2018 de la FRA (VIS), Vienne, 30 août 2018, p. 67 et 69.

([144]) CNUDE, article 8.

([145]) CNUDE, article 8, paragraphe 2.

([146]) FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Office des publications, Luxembourg, mars 2018, p. 114.

([147]) CouEDH, *Mouvement Raelien Suisse c. Suisse*, nº 16354/06, 13 juillet 2012, paragraphe 48.

([148]) Arrêt de la Cour de justice du 17 décembre 2015, *Neptune Distribution*, C-157/14, ECLI:EU:C:2015:823, point 65.

([149]) *Explications relatives à la Charte des droits fondamentaux*, JO 2007 C 303, explication sur l'article 11, p. 21.

([150]) International Justice and Public Safety Network (2011), *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*, 30 juin 2011, p. 18.

([151]) *Verwaltungsgericht Gelsenkirchen (2018), 14 K 3543/18 (ECLI:DE:VGGE:2018:1023.14K3543.18.00).*

([152]) Conseil des droits de l'homme (2019), *Surveillance et droits de l'homme — Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, David Kaye, A/HRC/41/35.

([153]) ONU, Comité des droits de l'homme, *Projet d'observation générale nº 37 sur le droit de réunion pacifique (article 21)*, projet préparé par le rapporteur Christof Heyns, juillet 2019, paragraphe 1.

déploiement de technologies de reconnaissance faciale peut avoir un effet dissuasif au regard duquel des personnes s'abstiennent d'exercer légalement leur liberté de réunion et d'association par crainte des conséquences négatives qui pourraient en découler ([154]). Elles pourraient ainsi être dissuadées de rencontrer des personnes ou des organisations particulières, d'assister à certaines réunions ou de participer à certaines manifestations. La capacité de s'engager dans ces formes d'activité est protégée par la Charte. Cet effet dissuasif a également des implications évidentes sur le fonctionnement efficace de la démocratie participative, et interfère donc directement avec la liberté de réunion et d'association ([155]). Les experts de la société civile indiquent que les technologies de reconnaissance faciale peuvent avoir un impact négatif sur la volonté des manifestants de s'engager dans l'activisme. Par conséquent, le déploiement d'une technologie de reconnaissance faciale lors de manifestations devrait répondre à un seuil de nécessité et de proportionnalité encore plus élevé que dans d'autres espaces publics.

La FRA a souligné que les organisations de la société civile de certains États membres de l'UE sont déjà très préoccupées par le fait que leur travail soit soumis à la surveillance de l'État ([156]). Il est donc essentiel que les autorités soient transparentes quant à l'utilisation des technologies de reconnaissance faciale et qu'une législation solide soit mise en place quant à l'utilisation de cette technologie de surveillance ([157]).

7.5. Droit à une bonne administration

Le droit à une bonne administration est un principe général bien établi du droit de l'UE défini par la CJUE et, en tant que tel, il lie tous les États membres de l'UE ([158]). Il s'agit également d'un droit fondamental consacré à l'article 41 de la Charte, mais il concerne uniquement les actions des institutions, organes et organismes de l'Union ([159]). En tant que principe général du droit de l'UE, il exige des États membres de l'UE qu'ils appliquent les exigences du droit à une bonne administration dans toute action publique. Ce droit comprend, sans s'y limiter, le droit d'accès de toute personne au dossier qui la concerne et l'obligation pour toute autorité publique de motiver ses décisions ([160]). L'accès au dossier facilite la compréhension des éléments de preuve sur lesquels la décision a été prise, et/ou des raisons qui la sous-tendent, plaçant ainsi la personne dans une meilleure position pour présenter des contre-arguments lors de l'exercice de son droit d'être entendue ([161]). L'obligation de motivation rend, du point de vue des personnes affectées, le processus décisionnel plus transparent, de sorte que la personne concernée puisse savoir pourquoi une mesure ou une action a été prise. Selon la CJUE, le contexte dans lequel les décisions individuelles sont prises est important pour déterminer l'étendue de l'obligation de motivation ([162]).

Le droit à une bonne administration s'applique également lorsque les autorités répressives traitent des images faciales en utilisant des technologies de reconnaissance faciale. Bien que le droit à une bonne administration puisse être soumis à certaines limitations, la question est de savoir comment garantir qu'un nombre potentiellement élevé de personnes aient toutes accès à leurs dossiers (données à caractère personnel stockées). Une autre question est de savoir comment faire en sorte que la police et les autres autorités publiques indiquent toujours les raisons pour lesquelles une personne est arrêtée et/ou fouillée sur la base d'une détection par reconnaissance faciale.

L'exercice du droit d'accès d'une personne au dossier qui la concerne, y compris aux données à caractère personnel stockées dans les systèmes d'information, suppose qu'elle soit informée que ses données à caractère personnel y figurent. Souvent, les personnes ne sont pas informées du fait que leur visage est enregistré et traité dans une base de données à des fins de comparaison. Si elles ne sont pas informées du traitement, elles ne sont pas non plus en mesure de demander l'accès à leurs données.

Les éléments clés du droit à une bonne administration, tels que le droit d'accès de toute personne au dossier qui la concerne et l'obligation pour l'administration de motiver ses décisions, ont également été traduits en dispositions plus spécifiques dans la législation de l'UE sur la protection des données. L'article 8, paragraphe 2, de la Charte et l'acquis de l'UE en matière de protection des données prévoient un droit d'accès, de rectification et d'effacement de ses propres données à caractère personnel stockées. La possibilité d'exercer le droit d'accès relève du droit à un recours effectif. Si la finalité du

([154]) Fussey, P., et Murray, D. (2019), *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, université d'Essex, Human Rights Centre, juillet 2019, p. 36, et note de bas de page 87.

([155]) Ibid., p. 38, et Laperruque, J. (2019), *Facing the Future of Surveillance — Task Force on Facial Recognition Surveillance*, POGO, Washington, 4 mars 2019.

([156]) FRA (2018), *Difficultés rencontrées par les organisations de la société civile actives dans le domaine des droits de l'homme dans l'UE*, Office des publications, Luxembourg, janvier 2018.

([157]) Voir également Privacy International (2019), *Privacy International's contribution to the half-day general discussion on Article 21 of ICCPR*, février 2019, p. 7.

([158]) Dans une jurisprudence récente, voir l'arrêt de la Cour de justice du 8 mai 2014, *N.*, C-604/12, ECLI:EU:C:2014:302, point 49.

([159]) Également confirmé par l'arrêt de la Cour de justice du 17 juillet 2014, *YS e.a.*, C 141/12 et C 372/12, ECLI:EU:C:2014:2081, points 66 à 70.

([160]) Ces éléments, initialement développés par la jurisprudence de la CJUE, ont été inscrits à l'article 41, paragraphe 2, de la Charte. Pour en savoir plus sur ce droit dans les publications d'éminents universitaires, voir Craig, P. (2014), «Article 41 — Right to Good Administration», dans Hervey, T., Kenner, J., Peers, S., et Ward, A. (eds.), *The EU Charter of Fundamental Rights. A Commentary*, Hart Publishing, Oxford et Portland Oregon, p. 1069-1098.

([161]) Ibid., p. 1082.

([162]) Ibid., p. 1086 et 1087.

traitement des données concerne: 1) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière, 2) l'exécution de sanctions pénales, ou 3) la sauvegarde de la sécurité publique, le droit d'accès aux données à caractère personnel et le droit de demander leur rectification ou leur effacement peuvent être limités dans les cas suivants, conformément à la directive en matière de protection des données dans le domaine répressif ([163]):

- pour éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires;
- pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;
- pour protéger la sécurité publique;
- pour protéger la sûreté de l'État;
- pour protéger les droits et libertés d'autrui ([164]).

Ces exemptions découlent de l'obligation pour les autorités répressives de travailler en respectant un certain degré de confidentialité et de secret afin d'assurer l'efficacité de leur travail. Dans ce contexte, et comme l'a souligné la FRA dans de précédents rapports ([165]), des mécanismes de responsabilisation indépendants sont essentiels pour garantir l'accès effectif à des voies de recours. Une combinaison d'organes de contrôle interne et externe, actifs à différents stades du processus (avant, pendant et après l'utilisation des technologies de reconnaissance faciale) garantirait que les droits des personnes soient protégés de manière adéquate et efficace.

Selon les recherches de la FRA, il subsiste encore un manque de sensibilisation et de compréhension de la manière d'exercer le droit d'accès, de rectification ou d'effacement des données à caractère personnel inexactes qui sont stockées dans des systèmes d'information à grande échelle ([166]). Il en va de même pour les bases de données de reconnaissance faciale utilisées à des fins répressives. Cette situation est exacerbée par le fait que très peu de juristes sont spécialisés dans l'application du droit d'accès, de rectification et d'effacement des données à caractère personnel dans les systèmes d'information, y compris les images faciales utilisées pour la reconnaissance faciale.

7.6. Droit à un recours effectif

L'article 47 de la Charte garantit un droit à un recours effectif devant un tribunal, et à accéder à un tribunal impartial. Ce droit fondamental à effet horizontal permet aux personnes de contester une mesure portant atteinte à tout droit qui leur est conféré par la législation de l'UE, et pas seulement en ce qui concerne les droits fondamentaux garantis par la Charte ([167]). Le droit à un recours effectif couvre également les décisions prises à l'aide de technologies de reconnaissance faciale, comme une mesure (telle qu'une arrestation par la police) fondée exclusivement ou de manière significative sur la reconnaissance faciale ([168]). La CJUE a souligné que l'article 47 constitue une réaffirmation du principe de protection juridictionnelle effective et que les caractéristiques d'un recours doivent être déterminées en conformité avec ce principe ([169]).

Une condition préalable à l'exercice du droit à un recours effectif est qu'une personne doit être informée que son image faciale est traitée. Comme l'a noté la CJUE, dans le cadre de mesures de sécurité portant atteinte au droit à la vie privée et au droit à la protection des données à caractère personnel, les autorités répressives nationales doivent notifier les personnes concernées, selon les procédures nationales applicables, dès que cette notification n'est plus susceptible de compromettre les enquêtes menées par ces autorités ([170]). Une telle situation se produit, par exemple, lorsque les autorités répressives alimentent une «liste de surveillance» utilisée pour la reconnaissance faciale avec un grand nombre d'images faciales. La CJUE a constaté que la notification est, en fait, nécessaire pour permettre aux personnes concernées par ces mesures

([163]) Articles 15 et 16.

([164]) Voir également FRA (2018), *Guide pour la prévention du profilage illicite aujourd'hui et demain*, Office des publications, Luxembourg, décembre 2018, p. 105.

([165]) Voir FRA (2015), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU — Volume I: Members States' legal framework*, Office des publications, Luxembourg, novembre 2015; et FRA (2017), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU — Volume II: field perspectives and legal update*, Office des publications, Luxembourg, octobre 2017.

([166]) FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Office des publications, Luxembourg, mars 2018, p. 17, 100 et 101.

([167]) Réseau d'experts indépendants en matière de droits fondamentaux, *Commentary on the Charter on Fundamental Rights of the European Union*, juin 2006, p. 360. Voir aussi: FRA et Conseil de l'Europe (2016), *Manuel de droit européen en matière d'accès à la justice*, Office des publications, Luxembourg, juin 2016, p. 92.

([168]) Commissaire aux droits de l'homme du Conseil de l'Europe (2019), *Décoder l'intelligence artificielle: 10 mesures pour protéger les droits de l'homme — Recommandation*, Conseil de l'Europe, Strasbourg, mai 2019, p. 13.

([169]) Arrêt de la Cour de justice du 13 mars 2007, *Unibet*, C-432/05, ECLI:EU:C:2007:163, point 37; arrêt de la Cour de justice du 27 juin 2013, *Agrokonsulting-04*, C-93/12, ECLI:EU:C:2013:432, point 59; arrêt de la Cour de justice du 18 décembre 2014, *Abdida*, C-562/13, ECLI:EU:C:2014:2453, point 45.

([170]) Arrêt de la Cour de justice du 21 décembre 2016, *Tele2 Sverige*, C-203/15 et C-698/15, ECLI:EU:C:2016:970, point 12. Voir également, mutatis mutandis, l'arrêt de la Cour de justice du 19 janvier 2010, *Kücükdeveci*, C-555/07, ECLI:EU:C:2010:21, point 52; l'arrêt de la Cour de justice du 6 octobre 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, point 95.

d'exercer, entre autres, leur droit à un recours juridictionnel effectif garanti par l'article 47 de la Charte ([171]).

La législation de l'UE sur la protection des données confirme à nouveau que le droit à un recours juridictionnel effectif doit être prévu en ce qui concerne les décisions du responsable du traitement ou du sous-traitant ([172]) ainsi que de l'autorité de contrôle ([173]). Les données traitées par les technologies de reconnaissance faciale ne font pas exception. Les personnes pourraient vouloir contester les raisons pour lesquelles leur image faciale a été incluse dans la «liste de surveillance», pourquoi cela a été fait de manière non transparente et sans leur consentement, ou demander réparation pour une fausse correspondance positive qui a eu des conséquences négatives pour elles (par exemple un contrôle, une fouille ou une arrestation illégale), y compris demander réparation pour le préjudice subi ([174]) (par exemple, la personne a manqué son vol de correspondance ou a été empêchée à tort d'entrer dans un pays de l'UE et a manqué une réunion de travail).

Il est crucial de noter que la possibilité d'introduire une réclamation administrative auprès d'une autorité de contrôle, comme le prévoient le RGPD et la directive en matière de protection des données dans le domaine répressif ([175]) n'est pas considérée comme un recours juridictionnel effectif au sens de l'article 47 de la Charte, puisqu'aucun tribunal n'est impliqué dans un tel contrôle. Un contrôle judiciaire devrait toujours rester possible et accessible si les mécanismes internes de règlement des litiges et autres systèmes alternatifs s'avèrent insuffisants ou lorsque la personne concernée opte pour un contrôle judiciaire ([176]).

([171]) Arrêt de la Cour de justice du 21 décembre 2016, *Tele2 Sverige*, C-203/15 et C-698/15, ECLI:EU:C:2016:970, point 12.

([172]) Directive en matière de protection des données dans le domaine répressif, article 54; RGPD, article 79.

([173]) Directive en matière de protection des données dans le domaine répressif, article 53; RGPD, article 78.

([174]) Directive en matière de protection des données dans le domaine répressif, considérant 88 et article 56; RGPD, considérant 146 et article 82.

([175]) Directive en matière de protection des données dans le domaine répressif, article 52; RGPD, article 77.

([176]) Conseil de l'Europe (2019), *Projet de recommandation du Comité des ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme*, Comité d'experts sur la dimension droits de l'homme des traitements automatisées de données et différentes formes d'intelligence artificielle (MSI-AUT), MSI-AUT(2018)06rev1, 26 juin 2019, paragraphe 4.5.

Conclusions

L'utilisation de la technologie de reconnaissance faciale — une technologie qui s'est développée rapidement ces dernières années et qui est de plus en plus utilisée par de multiples acteurs — affecte de nombreux droits fondamentaux. Cependant, il existe peu d'informations sur la manière et l'étendue de l'utilisation de cette technologie par les autorités répressives, ainsi que sur l'impact de son utilisation sur les droits fondamentaux. Travailler avec de nouvelles technologies utilisant l'IA, qui ne sont pas encore totalement comprises et pour lesquelles on ne dispose pas de beaucoup d'expérience, nécessite l'implication de tous les acteurs pertinents et experts de différentes disciplines.

Le droit de l'UE reconnaît que les images faciales constituent des données biométriques, compte tenu du fait qu'elles peuvent être utilisées pour identifier des personnes. La technologie de reconnaissance faciale peut être utilisées de multiples façons: il peut s'agir de vérifier l'identité d'une personne, de déterminer si un individu figure sur une liste de personnes, voire de répertorier des personnes selon différentes caractéristiques. La technologie de reconnaissance faciale en temps réel détecte tous les visages sur des séquences vidéo et les compare ensuite avec les visages figurant sur des listes de surveillance — elle pourrait être utilisée dans les espaces publics.

Bien que l'on dispose de peu d'informations sur l'utilisation réelle de la technologie de reconnaissance faciale dans l'UE, plusieurs États membres envisagent, testent ou planifient l'utilisation de cette technologie à des fins répressives. Plus activement, la police du Royaume-Uni a effectué plusieurs tests, dans des situations de la vie réelle telles que des événements sportifs, en utilisant de véritables listes de surveillance. D'autres services répressifs, comme la police de Berlin, en Allemagne, ou de Nice, en France, ont testé la précision de la technologie dans des tests de plus grande envergure menés auprès de volontaires. L'absence d'informations plus complètes sur l'utilisation réelle de la technologie limite les possibilités d'analyser ses implications en matière de droits fondamentaux. En particulier, il n'existe aucune loi ou autre orientation ou information sur les personnes qui seront incluses dans les listes de surveillance potentielles.

Les implications en matière de droits fondamentaux de l'utilisation de la technologie de reconnaissance faciale varient considérablement en fonction de la finalité, du contexte et de la portée de l'utilisation. Certaines des implications en matière de droits fondamentaux résultent du manque de précision de la technologie. La précision a fortement augmenté, mais la technologie s'accompagne toujours d'un certain taux d'erreur, qui peut avoir un impact négatif sur les droits fondamentaux. En outre, et c'est important, plusieurs préoccupations concernant les droits fondamentaux subsisteraient même en cas d'absence totale d'erreurs.

Nonobstant les différences de contexte, de finalité et de portée de l'utilisation de la technologie de reconnaissance faciale, plusieurs considérations relatives aux droits fondamentaux s'appliquent. La manière dont les images faciales sont obtenues et utilisées — potentiellement sans consentement ni possibilité de se soustraire — peut avoir un impact négatif sur la dignité des personnes. Dans le même ordre d'idées, les droits au respect de la vie privée et à la protection des données à caractère personnel sont au cœur des préoccupations en matière de droits fondamentaux lorsqu'une technologie de reconnaissance faciale est utilisée. En outre, toute utilisation de la technologie doit faire l'objet d'une évaluation approfondie quant à son impact potentiel sur la non-discrimination et les droits des groupes spéciaux, tels que les enfants, les personnes âgées et les personnes handicapées, en raison de la précision variable (parfois inconnue) de la technologie pour ces groupes et en fonction d'autres caractéristiques protégées. Il convient en outre de veiller à ce que le recours à cette technologie ne nuise pas à la liberté d'expression, d'association et de réunion.

Enfin, le présent document souligne qu'il est essentiel de prendre en compte les droits procéduraux lorsque la technologie de reconnaissance faciale est utilisée par les administrations publiques, notamment le droit à une bonne administration et le droit à un recours effectif et à accéder à un tribunal impartial.

Étant donné la nouveauté de la technologie ainsi que le manque d'expérience et d'études détaillées sur l'impact des technologies de reconnaissance faciale, il est important de prendre en compte de nombreux aspects avant de déployer un tel système dans des applications réelles:

- À l'instar des systèmes d'information à grande échelle de l'UE, un cadre juridique clair et suffisamment précis doit réglementer la mise en place et l'utilisation des technologies de reconnaissance faciale. La détermination du caractère nécessaire et proportionné du traitement des images faciales dépendra de la finalité de l'utilisation de la technologie et des garanties mises en place pour protéger les personnes dont les images faciales font l'objet d'un traitement automatisé contre d'éventuelles conséquences négatives. Les formes de reconnaissance faciale qui impliquent un très fort degré d'intrusion dans les droits fondamentaux, compromettant le caractère essentiel et inviolable d'un ou plusieurs droits fondamentaux, sont illégales.

- Il convient d'établir une distinction entre le traitement des images faciales à des fins de vérification, lorsque deux images faciales sont comparées pour vérifier si elles appartiennent à la même personne, et celui destiné à des fins d'identification, lorsqu'une image faciale est comparée à une base de données ou à une liste de surveillance d'images faciales. Le risque d'ingérences

dans les droits fondamentaux est plus élevé dans le deuxième cas, et le test de la nécessité et de la proportionnalité doit donc être plus strict.

- Les technologies dites de «reconnaissance faciale en temps réel», qui consistent à extraire des images faciales à partir de caméras vidéo déployées dans des espaces publics, sont particulièrement difficiles à mettre en œuvre. Une telle utilisation déclenche des ressentis différents au sein de la population et fait craindre un fort déséquilibre de pouvoir entre l'État et l'individu. Ces craintes doivent être prises au sérieux. Étant donné que les personnes peuvent ne pas être informées que leur image faciale est comparée à une liste de surveillance et compte tenu du taux d'erreur plus élevé par rapport aux images faciales prises dans un environnement contrôlé (tel qu'un aéroport ou un poste de police), leur utilisation devrait rester exceptionnelle. Elle devrait être strictement limitée à la lutte contre le terrorisme et d'autres formes graves de criminalité, ou à la recherche de personnes disparues et de victimes de la criminalité.

- Lorsque des images faciales sont extraites à partir de caméras vidéo déployées dans des espaces publics, l'évaluation de la nécessité et de la proportionnalité de la reconnaissance faciale doit également tenir compte de l'emplacement des caméras. Il y a une différence entre un événement sportif ou culturel et des événements où les personnes exercent un de leurs droits fondamentaux. Le déploiement de technologies de reconnaissance faciale lors de manifestations peut avoir un effet dissuasif au regard duquel des personnes s'abstiennent d'exercer légalement leur liberté de réunion et d'association par crainte des conséquences négatives qui pourraient en découler. Il est difficile d'imaginer des situations où le déploiement de technologies de reconnaissance faciale sur des personnes participant à une manifestation pourrait être nécessaire et proportionné.

- Les algorithmes de reconnaissance faciale ne donnent jamais un résultat définitif, mais uniquement des probabilités que deux visages appartiennent à la même personne. Dans le contexte de l'application de la loi, il existe donc une certaine marge d'erreur qui fait que des personnes sont signalées à tort. Lors du déploiement de la technologie, les risques de signaler à tort des personnes doivent être réduits au minimum. Toute personne interpellée à la suite de l'utilisation de la technologie doit être traitée avec dignité.

- Les autorités publiques s'appuient généralement sur des entreprises privées pour l'acquisition et le déploiement de la technologie. L'industrie et la communauté de la recherche scientifique peuvent jouer un rôle important dans l'élaboration de solutions techniques favorisant le respect des droits fondamentaux, y compris la protection des données à caractère personnel. Pour cela, cependant, les considérations relatives aux droits fondamentaux doivent être intégrées dans les spécifications techniques et les contrats. La directive de l'UE sur la passation des marchés publics (2014/24/UE) a renforcé l'engagement des États membres de l'UE en faveur de marchés publics socialement responsables lors de l'achat d'un produit ou d'un service. Dans l'esprit de la directive de 2014, l'UE et ses États membres pourraient appliquer une approche similaire lors de l'acquisition de technologies de reconnaissance faciale ou de la mise en service de recherches innovantes. Le fait de placer les droits fondamentaux et, en particulier, les exigences en matière de protection des données et de non-discrimination au centre de toutes les spécifications techniques, permettrait de s'assurer que l'industrie y accorde l'attention nécessaire. Les mesures possibles pourraient inclure une obligation contraignante de mobiliser des experts en protection des données à caractère personnel et des spécialistes des droits de l'homme dans les équipes qui travaillent sur le développement de la technologie, pour garantir le respect des droits fondamentaux dès la conception. En outre, les spécifications techniques pourraient faire référence à des normes de qualité élevées afin de minimiser les taux de fausses identifications et les impacts négatifs sur le sexe, l'origine ethnique et l'âge.

- Une analyse d'impact sur les droits fondamentaux est un outil essentiel pour garantir une application des technologies de reconnaissance faciale conforme aux droits fondamentaux, quel que soit le contexte dans lequel elles sont employées. Une telle analyse doit évaluer tous les droits affectés, y compris ceux énumérés dans le présent document, de manière exhaustive. Pour leur permettre de procéder à cette évaluation, les autorités publiques doivent obtenir de l'industrie toutes les informations nécessaires à l'évaluation de l'impact de la technologie sur les droits fondamentaux. Les secrets d'affaire ou les informations confidentielles ne doivent pas entraver cet effort ([177]).

- Compte tenu de l'évolution constante de la technologie, les ingérences dans les droits fondamentaux ne sont pas faciles à prévoir. Il est donc essentiel que les développements en matière de reconnaissance faciale fassent l'objet d'un suivi attentif de la part d'organes de surveillance indépendants. L'article 8, paragraphe 3, de la Charte sur la protection des données à caractère personnel exige le contrôle du traitement des données par une autorité indépendante. Pour prévenir les violations des droits fondamentaux et soutenir efficacement les personnes dont les droits fondamentaux sont affectés par la technologie de reconnaissance faciale, les autorités de contrôle doivent disposer d'une expertise, de ressources et de pouvoirs suffisants.

([177]) Voir également Commissaire aux droits de l'homme du Conseil de l'Europe (2019), *Décoder l'intelligence artificielle: 10 mesures pour protéger les droits de l'homme — Recommandation*, Conseil de l'Europe, Strasbourg, mai 2019.

Informations supplémentaires

Les publications suivantes de la FRA fournissent davantage d'informations en rapport avec le sujet de ce document.

- *Data quality and artificial intelligence — mitigating bias and error to protect fundamental rights* (Qualité des données et intelligence artificielle — Atténuer les distorsions et les erreurs pour protéger les droits fondamentaux) (2019), https://fra.europa.eu/en/publication/2019/artificial-intelligence-data-quality
- *#BigData: Discrimination in data-supported decision making* (#Mégadonnées: discrimination dans la prise de décision fondée sur des données) (2018), http://fra.europa.eu/en/publication/2018/big-data-discrimination
- *Under watchful eyes: biometrics, EU IT systems and fundamental rights* (Sous un regard attentif: éléments biométriques, systèmes d'information à grande échelle de l'UE et droits fondamentaux) (2018), http://fra.europa.eu/en/publication/2018/biometrics-rights-protection
- *Fundamental rights and the interoperability of EU information systems: borders and security* (Droits fondamentaux et interopérabilité des systèmes d'information de l'UE: frontières et sécurité) (2017), http://fra.europa.eu/en/publication/2017/fundamental-rights-interoperability
- *The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)* [Impact sur les droits fondamentaux de la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)] (2017), http://fra.europa.eu/en/opinion/2017/etias-impact

FRA – AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE

Schwarzenbergplatz 11 – 1040 Vienne – Autriche
Tél. +43 158030-0 – Fax +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Office des publications
de l'Union européenne

Print: ISBN 978-92-9461-522-0, doi:10.2811/332091
PDF: ISBN 978-92-9461-521-3, doi:10.2811/519455
Manuscrit achevé en janvier 2020

TK-03-20-019-FR-C (print); TK-03-20-019-FR-N (PDF)