Translations proofread by EDPB Members.

This language version has not yet been proofread.

Lignes directrices 05/2022 sur l'utilisation de la technologie de reconnaissance faciale dans le domaine répressif

Version 2.0

Adoptées le 26 avril 2023

Historique des versions

Version 1.0	12 mai 2022	Adoption des lignes directrices pour consultation publique
Version 2.0	26 avril 2023	Adoption des lignes directrices après consultation publique

Table des matières

Synthèse 5

1 Introduction 9

2 Technologie 10

2.1 Une technologie biométrique, deux fonctions distinctes 10

2.2 Une grande variété de finalités et d'applications 12

2.3 Fiabilité, exactitude et risques pour les personnes concernées 14

3 Le cadre juridique applicable 15

3.1 Cadre juridique général – La charte des droits fondamentaux de l'Union européenne et la Convention européenne des droits de l'homme (CEDH) 16

3.1.1 Applicabilité de la charte 16

3.1.2 Atteinte aux droits énoncés dans la charte 16

3.1.3 Justifications de l'ingérence 17

3.2 Cadre juridique spécifique – la directive en matière de protection des données dans le domaine répressif 22

3.2.1 Traitement de catégories particulières de données à des fins répressives 22

3.2.2 Décision individuelle automatisée, y compris le profilage 25

3.2.3 Catégories des personnes concernées 26

3.2.4 Droits de la personne concernée 26

3.2.5 Autres exigences légales et garanties 31

4 Conclusion 34

5 Annexes 35

Annexe I – Modèle de description des scénarios 36

Annexe II – Orientations pratiques pour les autorités répressives sur la gestion des projets de technologie de reconnaissance faciale 38

1. ROLES ET RESPONSABILITES 38

2. DEBUT: AVANT L'ACQUISITION DU SYSTEME DE TECHNOLOGIE DE RECONNAISSANCE FACIALE 40

3. LORS DE LA PASSATION DE MARCHES ET AVANT LE DEPLOIEMENT DE LA TECHNOLOGIE DE RECONNAISSANCE FACIALE 42

4. RECOMMANDATIONS APRES LE DEPLOIEMENT DE LA TECHNOLOGIE DE RECONNAISSANCE FACIALE 44

Annexe III – EXEMPLES CONCRETS 45

1 Scénario 1 45

1.1. Description 45

1.2. Cadre juridique applicable 46

1.3. Nécessité et proportionnalité – Finalité/gravité du crime 47

1.4. Conclusion 47
2 Scénario 2 47
2.1. Description 47
2.2. Cadre juridique applicable 48
2.3. Nécessité et proportionnalité – Finalité/gravité du crime/nombre de personnes non impliquées mais concernées par le traitement 49
2.4. Conclusion 49
3 Scénario 3 50
3.1. Description 50
3.2. Cadre juridique applicable 51
3.3. Nécessité et proportionnalité 51
3.4. Conclusion 52
4 Scénario 4 53
4.1. Description 53
4.2. Cadre juridique applicable 54
4.3. Nécessité et proportionnalité 54
4.4. Conclusion 54
5 Scénario 5 54
5.1. Description 54
5.2. Cadre juridique applicable 56
5.3. Nécessité et proportionnalité 56
5.4. Conclusion 59
6 Scénario 6 59
6.1. Description 59
6.2. Cadre juridique applicable 60
6.3. Nécessité et proportionnalité 60
6.4. Conclusion 60

SYNTHESE

De plus en plus d'autorités répressives font appel à la technologie de reconnaissance faciale, ou envisagent de le faire. Utilisée pour **authentifier** ou pour **identifier** une personne, cette technologie s'emploie également dans le cadre de vidéos (par exemple, CCTV) ou de photographies. Elle peut être utilisée à diverses fins, notamment pour rechercher des personnes figurant sur les listes de surveillance de la police ou pour surveiller les mouvements d'une personne dans l'espace public.

La technologie de reconnaissance faciale repose sur le traitement de **données biométriques** et inclut donc le traitement de catégories particulières de données à caractère personnel. Elle se sert souvent de composantes de l'**intelligence artificielle** (IA) ou de l'apprentissage automatique, ce qui permet un traitement de données à grande échelle, mais entraîne également un risque de discrimination et de faux résultats. Elle peut être utilisée tant dans des situations de contrôle en mode un-à-un que dans des foules immenses et dans des centres de transport importants.

La technologie de reconnaissance faciale est un **outil sensible pour les autorités répressives**. Celles-ci sont des autorités d'exécution et disposent de pouvoirs souverains. Cette technologie est susceptible d'interférer avec les droits fondamentaux, y compris au-delà du droit à la protection des données à caractère personnel, et d'affecter la stabilité sociale et politique de nos démocraties.

En ce qui concerne la protection des données à caractère personnel dans le contexte répressif, il convient de respecter les **exigences de la directive en matière de protection des données dans le domaine répressif**. Celle-ci prévoit un cadre pour l'utilisation de la technologie de reconnaissance faciale, en particulier en son article 3, point 13 (sur la notion de «données biométriques»), son article 4 (sur les principes relatifs au traitement des données à caractère personnel), son article 8 (sur la licéité du traitement), son article 10 (sur le traitement portant sur des catégories particulières de données à caractère personnel) et son article 11 (sur la décision individuelle automatisée).

Plusieurs autres droits fondamentaux peuvent également être affectés par l'application de la technologie de reconnaissance faciale. Par conséquent, la **charte des droits fondamentaux de l'Union européenne** (ci-après la «charte») est essentielle pour l'interprétation de la directive en matière de protection des données dans le domaine répressif, en particulier le droit à la protection des données à caractère personnel visé à l'article 8 de la charte, et le droit au respect de la vie privée prévu à l'article 7 de la charte.

Les **mesures législatives** qui servent de base juridique pour le traitement des données à caractère personnel interfèrent directement avec les droits garantis par les articles 7 et 8 de la charte. Le traitement de données biométriques en toutes circonstances constitue une atteinte grave en soi, et ce, quel que soit le résultat, par exemple une concordance positive. Toute limitation de l'exercice des droits et libertés fondamentaux doit être prévue par la loi et respecter le contenu essentiel de ces droits et libertés.

La base juridique doit être libellée de manière **suffisamment claire** pour permettre à tous les citoyens de savoir précisément à quelles conditions et dans quelles circonstances elle habilite les autorités à recourir à toute mesure de collecte de données et de surveillance secrète. Une simple transposition en droit interne de la clause générale inscrite à l'article 10 de la directive susmentionnée manquerait de précision et de prévisibilité.

Il convient de **consulter** l'autorité de contrôle compétente en matière de protection des données avant que le législateur national ne crée une nouvelle base juridique pour toute forme de traitement de données biométriques utilisant la reconnaissance faciale.

Les mesures législatives doivent être **appropriées** en vue d'atteindre les objectifs légitimes poursuivis par la législation en cause. Un **objectif d'intérêt général**, aussi fondamental soit-il, ne justifie pas, en soi, une limitation à un droit fondamental. Les mesures législatives devraient **différencier** et cibler les personnes qu'elles couvrent à la lumière de l'objectif visé, par exemple la lutte contre des formes graves de criminalité spécifiques. Si la mesure englobe toutes les personnes d'une manière générale sans une telle différenciation, limitation ou exception, elle intensifie l'ingérence. Cette même conséquence se produit également si le traitement des données concerne une partie importante de la population.

Les données doivent être traitées de manière à garantir l'applicabilité et l'efficacité des règles et principes de l'Union en matière de protection des données. L'**évaluation de la nécessité et de la proportionnalité** doit également, selon les situations, permettre d'identifier et d'examiner toutes les implications possibles pour les autres droits fondamentaux. Si les données sont systématiquement traitées à l'insu des personnes concernées, elles sont susceptibles de générer un **sentiment général de surveillance constante**, ce qui peut avoir des effets dissuasifs en ce qui concerne l'ensemble des droits fondamentaux concernés, ou certains d'entre eux, tels que la dignité humaine au titre de l'article 1er, la liberté de pensée, de conscience et de religion au titre de l'article 10, la liberté d'expression au titre de l'article 11 ainsi que la liberté de réunion et d'association au titre de l'article 12 de la charte.

Le traitement de catégories particulières de données, telles que les données biométriques, ne peut être considéré comme «**strictement nécessaire**» (article 10 de la directive en matière de protection des données dans le domaine répressif) que si l'ingérence dans la protection des données à caractère personnel et ses restrictions est limitée à ce qui est absolument nécessaire, c'est-à-dire indispensable, et à l'exclusion de tout traitement de nature générale ou systématique.

Une photographie ayant été **manifestement rendue publique** (article 10 de la directive susmentionnée) par la personne concernée ne signifie pas que les données biométriques correspondantes, qui peuvent être extraites de la photographie par des moyens techniques spécifiques, puissent être considérées comme ayant été manifestement rendues publiques. Les paramètres par défaut d'un service, par exemple la mise à disposition de modèles au public, ou l'absence de choix, par exemple si les modèles sont rendus publics sans que l'utilisateur soit en mesure de modifier ce paramètre, ne devraient en aucun cas être interprétés comme des données manifestement rendues publiques.

L'article 11 de la directive en matière de protection des données dans le domaine répressif établit un cadre pour la **prise de décision individuelle automatisée**. L'utilisation de la technologie de reconnaissance faciale implique l'utilisation de catégories spéciales de données et peut conduire à un profilage, en fonction de la manière dont cette technologie est appliquée et de l'objectif poursuivi. En tout état de cause, conformément au droit de l'Union et à l'article 11, paragraphe 3, de la directive, le profilage entraînant une discrimination à l'égard de personnes physiques sur la base de catégories particulières de données à caractère personnel est interdit.

L'article 6 de la directive concerne la nécessité d'établir une **distinction entre les différentes catégories de personnes concernées**. Il est fort probable qu'aucune ingérence ne soit justifiée quant aux personnes concernées pour lesquelles il n'existe aucune preuve susceptible de présumer que leur comportement pourrait avoir un lien, même indirect ou lointain, avec l'objectif légitime selon la directive.

Le **principe de minimisation des données** (de l'article 4, paragraphe 1, point e), de la directive) exige également que tout matériel vidéo non pertinent pour la finalité du traitement soit toujours supprimé

ou anonymisé (par exemple, par floutage sans possibilité rétroactive de récupérer les données) avant le déploiement.

Le responsable du traitement doit examiner attentivement la manière (ou la possibilité) de satisfaire aux exigences relatives aux **droits de la personne concernée** avant de lancer tout traitement recourant à la technologie de reconnaissance faciale, étant donné que la reconnaissance faciale implique souvent le traitement portant sur des catégories particulières de données à caractère personnel sans aucune interaction apparente avec la personne concernée.

L'exercice effectif des droits de la personne concernée repose sur le respect par le responsable du traitement de ses **obligations d'information** (article 13 de la directive). Lors de l'évaluation de l'existence d'un «cas particulier» conformément à l'article 13, paragraphe 2, de la directive, il convient de tenir compte de plusieurs facteurs, notamment si des données à caractère personnel sont collectées à l'insu de la personne concernée, étant donné qu'il s'agit de la seule manière de permettre aux personnes concernées d'exercer effectivement leurs droits. Si la prise de décision se fonde uniquement sur la technologie de reconnaissance faciale, il faut informer les personnes concernées des caractéristiques de cette décision automatisée.

En ce qui concerne les **demandes d'accès** et conformément au principe de minimisation des données, les données biométriques stockées et liées à une identité, également par des données alphanumériques, devraient permettre à l'autorité compétente de confirmer une demande d'accès. Cette dernière se fonde sur une recherche effectuée par ces données alphanumériques et ne nécessite pas un nouveau traitement des données biométriques d'autres personnes (c'est-à-dire en effectuant une recherche à l'aide de la technologie de reconnaissance faciale dans une base de données).

Les risques pour les personnes concernées sont particulièrement graves si des données inexactes sont stockées dans une base de données de la police et/ou partagées avec d'autres entités. Le responsable du traitement doit **corriger** les données stockées et les systèmes de reconnaissance faciale en conséquence (voir également le considérant 47 de la directive susmentionnée).

Le droit à la **limitation** revêt une grande importance en ce qui concerne la technologie de reconnaissance faciale (fondée sur un ou plusieurs algorithmes et ne donnant donc jamais de résultat définitif) dans les situations présentant de grandes quantités de données collectées et un éventuel écart dans l'exactitude et la qualité de l'identification.

Une **analyse de l'impact relative à la protection des données (AIPD)** avant de recourir à la technologie de reconnaissance faciale constitue une obligation (voir l'article 27 de la directive). Le comité européen de la protection des données recommande de publier les résultats de ces évaluations ou, à tout le moins, les principaux résultats et conclusions de l'AIPD, afin de renforcer la confiance et la transparence.

La plupart des cas de déploiement et d'utilisation de la technologie de reconnaissance faciale comportent un risque intrinsèque élevé pour les droits et libertés des personnes concernées. Par conséquent, l'autorité recourant à cette technologie devrait **consulter** l'autorité de contrôle compétente avant ledit recours au système.

Compte tenu de la nature unique des données biométriques, l'autorité chargée de la mise en œuvre et/ou de l'utilisation de la technologie de reconnaissance faciale devrait accorder une attention particulière à la **sécurité du traitement**, conformément à l'article 29 de la directive en matière de protection des données dans le domaine répressif. L'autorité répressive devrait en particulier veiller à ce que le système soit conforme aux normes pertinentes et mette en œuvre des mesures de protection

des modèles biométriques. Les principes et garanties de protection des données doivent être intégrés dans la technologie avant le début du traitement des données à caractère personnel: par conséquent, même lorsqu'une autorité répressive entend appliquer et recourir à la technologie de reconnaissance faciale provenant de fournisseurs externes, elle doit veiller, par exemple au moyen de la procédure de passation des marchés, à la seule utilisation desdites technologies reposant sur les principes de **protection des données dès la conception et de protection des données par défaut**.

La **journalisation** (voir l'article 25 de la directive en matière de protection des données dans le domaine répressif) constitue une garantie importante pour la vérification de la licéité du traitement, tant en interne (c'est-à-dire l'autocontrôle par le responsable du traitement ou par le sous-traitant concerné) que par les autorités de contrôle externes. Pour les systèmes de reconnaissance faciale, la journalisation est également recommandée pour les modifications de la base de données de référence et pour les tentatives d'identification ou de vérification, y compris pour l'utilisateur, le résultat et le score de confiance. La journalisation n'est toutefois qu'un élément essentiel du **principe général de responsabilité** (voir l'article 4, paragraphe 4, de la directive susmentionnée). Le responsable du traitement doit être en mesure de démontrer que le traitement respecte les principes fondamentaux de protection des données énoncés à l'article 4, paragraphes 1 à 3, de ladite directive.

Le comité européen de la protection des données rappelle sa **demande**, préparée conjointement avec le Contrôleur européen de la protection des données, **de l'interdiction** de certains types de traitement en ce qui concerne 1) l'identification biométrique à distance des personnes dans des espaces accessibles au public, 2) les systèmes de reconnaissance faciale fondés sur l'intelligence artificielle (IA) qui classent les personnes à partir de leurs données biométriques dans des groupes en fonction de l'origine ethnique, du genre, ainsi que des opinions politiques ou de l'orientation sexuelle, ou selon d'autres critères de discrimination, 3) l'utilisation de la technologie de reconnaissance faciale et de technologies similaires pour déduire les émotions d'une personne physique et 4) le traitement de données à caractère personnel dans un contexte répressif qui s'appuierait sur une base de données alimentée par la collecte de données à caractère personnel à grande échelle et de manière indifférenciée, par exemple en «extrayant» des photographies et des images faciales accessibles en ligne.

Une surveillance efficace par les autorités de contrôle compétentes en matière de protection des données constitue une garantie essentielle des droits fondamentaux en jeu. Par conséquent, les États membres doivent veiller à ce que les ressources des autorités de contrôle soient appropriées et suffisantes pour leur permettre d'exécuter leur mission.

Les présentes **lignes directrices s'adressent** aux législateurs au niveau de l'Union et des États membres, ainsi qu'aux autorités répressives et à leurs agents qui mettent en œuvre et utilisent les systèmes de technologie de reconnaissance faciale. Elles s'adressent également aux personnes qui sont intéressées plus généralement ou qui sont des personnes concernées, en particulier s'il agit des droits des personnes concernées.

Les présentes **lignes directrices ont vocation** à apporter des informations sur certaines propriétés de la technologie de reconnaissance faciale et sur le cadre juridique applicable dans le domaine répressif (en particulier la directive en matière de protection des données dans le domaine répressif).

- En outre, elles fournissent un **outil pour aider à la première classification du caractère sensible d'un cas d'utilisation donné** (annexe I).
- Elles comprennent également des **orientations pratiques à l'intention des autorités répressives qui souhaitent acquérir et exploiter un système de reconnaissance faciale** (annexe II).

- Elles décrivent également plusieurs **cas d'utilisation** typiques **et énumèrent de nombreuses considérations pertinentes**, notamment en ce qui concerne le test de nécessité et de proportionnalité (annexe III).

1 INTRODUCTION

1. La technologie de reconnaissance faciale peut être utilisée pour reconnaître automatiquement les personnes d'après leur visage. Elle repose souvent sur l'intelligence artificielle, comme les technologies d'apprentissage automatique. Les applications de cette technologie sont de plus en plus testées et utilisées dans divers domaines, de l'usage individuel à l'usage d'organisations privées et de l'administration publique. Les autorités répressives s'attendent également à ce qu'il y ait des avantages lorsqu'elles ont recours à la technologie de reconnaissance faciale. Elle promet, en effet, des solutions à des défis relativement nouveaux, tels que les enquêtes impliquant une grande quantité de preuves capturées, mais aussi à des problèmes connus, notamment en ce qui concerne le manque de personnel pour les tâches d'observation et de recherche.

2. Une grande partie de l'intérêt accru accordé à cette technologie repose sur son efficacité et son évolutivité. À cela s'ajoutent les inconvénients inhérents à la technologie et à son application, y compris à grande échelle. Bien qu'une simple manipulation puisse entraîner l'analyse de milliers d'ensembles de données à caractère personnel, de légers effets résultant de la discrimination algorithmique ou d'une erreur d'identification peuvent déjà toucher gravement un grand nombre de personnes dans leur comportement et leur vie quotidienne. L'ampleur du traitement des données à caractère personnel, et en particulier des données biométriques, est un autre élément clé de la technologie de reconnaissance faciale. En effet, le traitement des données à caractère personnel constitue une atteinte au droit fondamental à la protection des données à caractère personnel, conformément à l'article 8 de la charte des droits fondamentaux de l'Union européenne (ci-après, la «charte»).

3. Le recours à la technologie de reconnaissance faciale par les autorités répressives aura, et c'est déjà le cas dans une certaine mesure, d'importantes répercussions sur les personnes et les groupes de personnes, y compris les minorités. Ces répercussions auront également des effets considérables sur la manière dont nous cohabitons et sur notre stabilité politique sociale et démocratique, qui accorde une grande importance au pluralisme et à l'opposition politique. Le droit à la protection des données à caractère personnel est souvent une condition préalable essentielle pour garantir d'autres droits fondamentaux. Il est grandement probable que l'utilisation de la technologie de reconnaissance faciale vienne interférer avec les droits fondamentaux au-delà du droit à la protection des données à caractère personnel.

4. Le comité européen de la protection des données juge donc important de contribuer à l'intégration en cours de cette technologie dans le domaine répressif couvert respectivement par la directive en matière de protection des données dans le domaine répressif[1] et par les dispositions nationales qui la transposent, et de fournir les présentes lignes directrices. Les présentes lignes directrices visent à apporter des informations pertinentes aux législateurs à l'échelle de l'Union et des États membres ainsi qu'aux autorités répressives et à leurs agents lorsqu'ils mettent en œuvre des systèmes de

[1] 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

reconnaissance faciale et qu'ils les utilisent. Le champ d'application des lignes directrices se limite à la technologie de reconnaissance faciale. Toutefois, d'autres formes de traitement de données à caractère personnel fondées sur la biométrie auxquelles ont recours les autorités répressives, en particulier lorsqu'elles impliquent un traitement à distance, peuvent entraîner des risques similaires ou supplémentaires pour les personnes, les groupes et la société. En fonction des circonstances, certains aspects des présentes lignes directrices peuvent également se révéler utiles. Enfin, les personnes qui sont intéressés plus généralement ou qui sont des personnes concernées peuvent également y trouver des informations importantes, notamment en ce qui concerne les droits des personnes concernées.

5. Les présentes lignes directrices se composent d'un document principal et de trois annexes. Ce document principal a pour objet de présenter la technologie et le cadre juridique applicable. En vue de faciliter de déterminer certains des aspects majeurs permettant de classifier la gravité de l'atteinte aux droits fondamentaux selon un domaine d'application donné, un modèle est proposé à l'annexe I. Les autorités répressives qui souhaitent acquérir et exploiter un système de reconnaissance faciale trouveront des orientations pratiques à l'annexe II. En fonction du champ d'application de la technologie de reconnaissance faciale, différentes considérations pourraient se montrer pertinentes: à cette fin, une série de scénarios hypothétiques et de considérations pertinentes sont proposés à l'annexe III.

2 TECHNOLOGIE

2.1 Une technologie biométrique, deux fonctions distinctes

6. La reconnaissance faciale est une technologie probabiliste qui peut reconnaître automatiquement les personnes grâce à leur visage afin de les authentifier ou de les identifier.

7. Elle relève de la catégorie plus large de la technologie biométrique. La biométrie englobe l'ensemble des processus automatisés utilisés pour reconnaître une personne en quantifiant les caractéristiques physiques, physiologiques ou comportementales (empreintes digitales, structure de l'iris, voix, démarche, schémas des vaisseaux sanguins, etc.). Ces caractéristiques sont définies comme des «données biométriques», en ce sens qu'elles permettent d'identifier la personne ou de confirmer son identification.

8. C'est le cas des visages ou, plus précisément, de leur traitement technique à l'aide de dispositifs de reconnaissance faciale: à partir de l'image d'un visage (une photographie ou une vidéo) appelée «échantillon» biométrique, il est possible d'extraire une représentation numérique de caractéristiques distinctes de ce visage (ce qui correspond à un «modèle»).

9. Un modèle biométrique est une représentation numérique des caractéristiques uniques qui ont été extraites d'un échantillon biométrique et qui peuvent être stockées dans une base de données biométriques[2]. Il est censé être unique et spécifique à chaque personne et il est, en principe, permanent dans le temps[3]. Dans la phase de reconnaissance, l'appareil compare ce modèle à d'autres modèles précédemment produits ou calculés directement à partir d'échantillons biométriques tels que des visages trouvés sur une image, une photographie ou une vidéo. La «reconnaissance faciale» est donc un processus en deux étapes: la collecte de l'image faciale et sa transformation en un modèle,

[2] Lignes directrices sur la reconnaissance faciale, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, (Convention 108), Conseil de l'Europe, juin 2021.

[3] Ces caractéristiques peuvent dépendre du type de biométrie et de l'âge de la personne concernée.

suivie de la reconnaissance du visage en comparant le modèle correspondant à un ou plusieurs autres modèles.

10. Comme tout processus biométrique, la reconnaissance faciale peut remplir deux fonctions distinctes:

    - l'**authentification** d'une personne, destinée à vérifier qu'une personne est qui elle prétend être. Le système comparera alors un modèle ou un échantillon biométrique pré-enregistré (par exemple, stocké sur une carte à puce ou un passeport biométrique) avec un seul visage, tel que celui d'une personne se trouvant à un point de contrôle, afin de vérifier s'il s'agit d'une seule et même personne. Cette fonctionnalité repose donc sur la comparaison de deux modèles. Il s'agit de la **vérification** en mode un -à un;

    - l'**identification** d'une personne, destinée à trouver une personne parmi un groupe de personnes, dans une zone spécifique, une image ou une base de données. Le système doit alors traiter chaque visage capturé pour générer un modèle biométrique et vérifier ensuite s'il correspond à une personne connue du système. Cette fonctionnalité repose donc sur la comparaison d'un modèle avec une base de données de modèles ou d'échantillons (ligne de base). Il s'agit de l'identification en mode un à plusieurs. Par exemple, elle permet de relier les données contenues dans des dossiers passagers (nom de famille, prénom) à un visage, si la comparaison est effectuée au moyen d'une base de données de photographies associées aux noms et aux prénoms. Il peut également s'agir de suivre une personne dans une foule, sans nécessairement faire le lien avec son identité civile.

11. Dans les deux cas, les techniques de reconnaissance faciale utilisées reposent sur une estimation de la concordance entre les modèles, à savoir entre celui qui est comparé et le ou les modèles de référence. De ce point de vue, elles sont probabilistes: la comparaison déduit une probabilité plus ou moins élevée que la personne soit effectivement la personne à authentifier ou à identifier. Si cette probabilité dépasse un certain seuil dans le système, défini par l'utilisateur ou le développeur du système, le système supposera l'existence d'une concordance.

12. Bien que l'authentification et l'identification soient des fonctions distinctes, elles concernent toutes deux le traitement de données biométriques relatives à une personne physique identifiée ou identifiable. Elles constituent de ce fait un traitement de données à caractère personnel, et plus précisément un traitement portant sur des catégories particulières de données à caractère personnel.

13. La reconnaissance faciale fait partie d'un éventail plus large de techniques de traitement des images vidéo. Certaines caméras vidéo peuvent filmer des personnes à l'intérieur d'une zone définie, en particulier leurs visages, mais elles ne peuvent être utilisées en tant que telles pour reconnaître automatiquement des personnes. Il en va de même pour la photographie: un appareil photo n'est pas un système de reconnaissance faciale, étant donné que les photographies de personnes doivent être traitées d'une manière spécifique afin d'en extraire des données biométriques.

14. La simple détection de visages par des caméras dites «intelligentes» ne constitue pas non plus nécessairement un système de reconnaissance faciale. Bien qu'elles soulèvent également des questions importantes en matière d'éthique et d'efficacité, les techniques numériques permettant de détecter des comportements anormaux ou des événements violents, ou celles permettant de reconnaître des émotions faciales ou même des silhouettes, ne peuvent pas être considérées comme des systèmes biométriques traitant des catégories particulières de données à caractère personnel, à condition qu'elles ne visent pas à identifier une personne de manière unique et que le traitement de données à caractère personnel concerné n'englobe pas d'autres catégories particulières de données à caractère personnel. Ces exemples ne sont pas sans lien avec la reconnaissance faciale et sont toujours

soumis aux règles en matière de protection des données à caractère personnel[4]. En outre, ce type de système de détection peut être utilisé en conjonction avec d'autres systèmes visant à identifier une personne et être ainsi considéré comme une technologie de reconnaissance faciale.

15. Contrairement aux systèmes de capture et de traitement vidéo, par exemple, qui nécessitent l'installation de dispositifs physiques, la reconnaissance faciale est une fonctionnalité logicielle qui peut être mise en œuvre dans les systèmes existants (caméras, bases de données d'images, etc.). Cette fonctionnalité peut donc être connectée ou couplée à une multitude de systèmes et combinée avec d'autres fonctionnalités. Il convient d'accorder une attention particulière à l'intégration dans une infrastructure existante en raison des risques inhérents liés au fait que la technologie de reconnaissance faciale pourrait être imperceptible et facilement cachée[5].

2.2 Une grande variété de finalités et d'applications

16. Au-delà du champ d'application des présentes lignes directrices et en dehors du champ d'application de la directive en matière de protection des données dans le domaine répressif, la reconnaissance faciale peut être utilisée pour un large éventail d'objectifs, tant à des fins commerciales que pour répondre à des préoccupations en matière de sécurité publique ou d'application de la loi. Elle peut être utilisée dans de nombreux cadres différents: dans la relation personnelle entre un utilisateur et un service (accès à une application), pour l'accès à un lieu spécifique (filtrage physique), ou sans limitation particulière dans l'espace public (reconnaissance faciale en temps réel). Elle peut être appliquée à tout type de personne concernée: un client d'un service, un employé, un simple observateur, une personne recherchée ou une personne impliquée dans une procédure judiciaire ou administrative, etc. Certaines utilisations sont déjà courantes et répandues, tandis que d'autres sont actuellement au stade expérimental ou spéculatif. Bien que les présentes lignes directrices ne concernent pas toutes ces utilisations et applications, le comité européen de la protection des données rappelle qu'elles ne peuvent être mises en œuvre que si elles sont conformes au cadre juridique applicable, et en particulier au règlement général sur la protection des données (RGPD) et aux dispositions nationales pertinentes[6]. Même dans le cadre de la directive en matière de protection des données dans le domaine répressif, outre les fonctions d'authentification ou d'identification, les données traitées au moyen de la technologie de reconnaissance faciale peuvent également être traitées à d'autres fins, telles que la catégorisation.

17. Plus précisément, une échelle d'utilisations potentielles pourrait être envisagée en fonction du niveau de contrôle des personnes sur leurs données à caractère personnel, des moyens effectifs dont elles disposent pour exercer ce contrôle et de leur droit d'initiative pour activer et utiliser cette technologie, des conséquences pour elles (en cas de reconnaissance ou de non-reconnaissance) et de l'ampleur du traitement effectué. La reconnaissance faciale fondée sur un modèle stocké sur un appareil personnel (carte à puce, smartphone, etc.) qui appartient à une personne, utilisé à des fins d'authentification et d'usage strictement personnel par l'intermédiaire d'une interface spécifique, ne présente pas les mêmes risques que, par exemple, l'utilisation à des fins d'identification, dans un environnement non contrôlé, sans la participation active des personnes concernées. Cette utilisation consiste à comparer

[4] Toutefois, l'article 10 de la directive en matière de protection des données dans le domaine répressif (ou l'article 9 du règlement général sur la protection des données) s'applique aux systèmes utilisés pour classer les personnes, à partir de données biométriques, dans des groupes basés sur l'origine ethnique, les opinions politiques ou l'orientation sexuelle, ou dans d'autres catégories particulières de données à caractère personnel.
[5] Par exemple, dans les caméras piétons qui sont de plus en plus utilisées dans la pratique.
[6] Voir également les lignes directrices 3/2019 du comité européen de la protection des données sur le traitement des données à caractère personnel par des dispositifs vidéo, adoptées le 29 janvier 2020, pour de plus amples orientations.

le modèle de chaque visage entrant dans la zone de surveillance aux modèles d'un large échantillon de la population stocké dans une base de données. Entre ces deux extrêmes se trouve un spectre très varié d'utilisations et de questions connexes liées à la protection des données à caractère personnel.

18. En vue de mieux illustrer le cadre dans lequel les technologies de reconnaissance faciale sont actuellement débattues ou mises en œuvre, que ce soit à des fins d'authentification ou d'identification, le comité européen de la protection des données estime qu'il est pertinent de mentionner une série d'exemples. Les exemples repris ci-dessous sont uniquement descriptifs et ne devraient pas être considérés comme une quelconque évaluation préliminaire de leur conformité avec l'acquis de l'Union dans le domaine de la protection des données.

Exemples d'authentification par reconnaissance faciale

19. Il est possible de concevoir l'authentification de manière à ce que les utilisateurs en aient le contrôle total, par exemple pour permettre l'accès à des services ou à des applications uniquement dans un cadre domestique. Par conséquent, elle est largement utilisée par les propriétaires de smartphones pour déverrouiller leur appareil, au lieu d'utiliser l'authentification par mot de passe.

20. L'authentification par reconnaissance faciale peut également servir à vérifier l'identité d'une personne souhaitant bénéficier de services de tiers publics ou privés. Ces processus offrent ainsi un moyen de créer une identité numérique à l'aide d'une application mobile (smartphone, tablette, etc.), cette identité pouvant ensuite être utilisée pour accéder à des services administratifs en ligne.

21. En outre, l'authentification par reconnaissance faciale peut viser à contrôler l'accès physique à un ou plusieurs lieux prédéterminés, comme les entrées de bâtiments ou des points de passage précis. Cette fonctionnalité est, par exemple, mise en œuvre pour certains traitements aux fins du franchissement des frontières, lorsque le visage de la personne se présentant au poste-frontière est comparé à celui enregistré dans son document d'identité (passeport ou titre de séjour sécurisé).

Exemples d'identification par reconnaissance faciale

22. Il est possible d'utiliser l'identification de manières très diverses. Il s'agit notamment, sans s'y limiter, des utilisations ci-dessous actuellement observées, testées ou envisagées dans l'Union.

- la recherche de l'identité d'une personne non identifiée (victime, suspect, etc.) dans une base de données de photographies;
- la surveillance des mouvements d'une personne dans l'espace public. Son visage est comparé aux modèles biométriques des personnes qui voyagent ou ont voyagé dans la zone surveillée, par exemple lorsqu'un bagage est abandonné ou après qu'une infraction a été commise;
- la reconstitution du parcours d'une personne et de ses interactions ultérieures avec d'autres personnes physiques, par une comparaison différée des mêmes éléments en vue d'identifier ses contacts par exemple;
- l'identification biométrique à distance dans les espaces publics des personnes recherchées. Tous les visages capturés en direct par les caméras de vidéoprotection sont comparés, en temps réel, à une base de données détenue par les forces de sécurité;
- la reconnaissance automatique des personnes sur une image pour identifier, par exemple, les personnes avec lesquelles elles sont en relation sur un réseau social qui permet la reconnaissance automatique. L'image est comparée aux modèles de tous les membres du réseau qui ont consenti

à cette fonctionnalité afin de permettre l'identification nominative des personnes avec lesquelles ils sont en relation;

- l'accès aux services, certains distributeurs de billets reconnaissant leurs clients en comparant un visage capturé par une caméra avec la base de données d'images faciales détenue par la banque;

- le suivi du voyage d'un passager à un certain stade dudit voyage. Le modèle, calculé en temps réel, de toute personne s'enregistrant aux portes d'embarquement situées à certaines étapes du voyage (points de dépôt des bagages, portes d'embarquement, etc.), est comparé aux modèles des personnes précédemment enregistrées dans le système.

23. Outre l'utilisation de la technologie de reconnaissance faciale dans le domaine répressif, le large éventail d'applications observées nécessite certainement un débat global et une approche stratégique afin d'assurer la cohérence et la conformité avec l'acquis de l'Union dans le domaine de la protection des données.

2.3 Fiabilité, exactitude et risques pour les personnes concernées

24. Comme pour toute technologie, la mise en œuvre de la reconnaissance faciale peut également rencontrer des difficultés, notamment en ce qui concerne la fiabilité et l'efficacité d'authentification ou d'identification, la question plus générale de la qualité et de la précision des données «sources» et le résultat du traitement des données au moyen de cette technologie.

25. Ces défis technologiques entraînent des risques particuliers pour les personnes concernées, qui sont d'autant plus importants ou graves dans le domaine répressif, compte tenu des effets possibles pour ces personnes, qu'il s'agisse d'effets juridiques ou d'autres effets les affectant de manière similaire et significative. Il semble donc également utile de souligner que l'utilisation ex post de la technologie de reconnaissance faciale n'est pas en soi plus sûre, étant donné que les personnes peuvent être suivies dans le temps et dans l'espace. Par conséquent, l'utilisation ex post présente, elle aussi, des risques spécifiques qui doivent être évalués au cas par cas[7].

26. Comme l'a souligné l'Agence des droits fondamentaux de l'Union européenne dans son rapport de 2019, «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 %)[8] 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 concordance 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. 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 «mystifcation») sont importantes, en particulier à des fins répressives.»[9]

27. À cet égard, le comité européen de la protection des données estime qu'il est important de rappeler que la technologie de reconnaissance faciale, qu'elle soit utilisée à des fins d'authentification ou d'identification, ne fournit pas de résultat définitif. Elle s'appuie cependant sur des probabilités selon

[7] Voir les exemples présentés à l'annexe III.

[8] Ce taux de précision découle du rapport cité et reflète un taux bien meilleur que les performances actuelles des algorithmes dans les applications de la technologie de reconnaissance faciale.

[9] Agence des droits fondamentaux de l'Union européenne, *Technologie de reconnaissance faciale: considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi*, 21 novembre 2019.

lesquelles deux visages, ou des images de visages, correspondent à la même personne[10]. Ce résultat se détériore encore davantage lorsque la qualité de l'échantillon biométrique utilisée pour la reconnaissance faciale est médiocre. Parmi les facteurs de qualité médiocre figurent le manque de netteté des images d'entrée, la faible résolution de la caméra, le mouvement et la faible lumière. D'autres aspects ayant un effet significatif sur les résultats sont la prévalence et la mystification, par exemple lorsque des criminels tentent d'éviter de passer devant les caméras ou de duper la technologie de reconnaissance faciale. De nombreuses études ont également mis en lumière que ces résultats statistiques résultant du traitement algorithmique peuvent également faire l'objet de biais, notamment en raison de la qualité des données sources ainsi que des bases de données d'entraînement, ou d'autres facteurs, tels que le choix de la localisation du déploiement. En outre, il convient également de souligner l'incidence de la technologie de reconnaissance faciale sur d'autres droits fondamentaux, tels que le respect de la vie privée et familiale, la liberté d'expression et d'information, la liberté de réunion et d'association, etc.

28. Il importe donc de tenir compte des critères que sont la fiabilité et la précision de la technologie de reconnaissance faciale pour évaluer le respect des principes clés de la protection des données, conformément à l'article 4 de la directive en matière de protection des données dans le domaine répressif, et en particulier en ce qui concerne l'équité et la précision.

29. Le comité européen de la protection des données insiste sur la nécessité pour les responsables du traitement, dans le cadre de leur obligation de rendre compte, de procéder à une évaluation régulière et systématique du traitement algorithmique afin de garantir en particulier l'exactitude, l'équité et la fiabilité du résultat du traitement de données à caractère personnel, tout en soulignant que des données de haute qualité sont essentielles pour produire des algorithmes de haute qualité. Les données à caractère personnel utilisées à des fins d'évaluation, d'entraînement et de développement des systèmes de reconnaissance faciale ne peuvent être traitées qu'avec l'appui d'une base juridique suffisante et conformément aux principes communs de protection des données.

3 LE CADRE JURIDIQUE APPLICABLE

30. L'utilisation de la technologie de reconnaissance faciale est intrinsèquement liée au traitement de données à caractère personnel, y compris de catégories particulières de données. Elle a, de ce fait, une incidence directe ou indirecte sur un certain nombre de droits fondamentaux, consacrés par la charte des droits fondamentaux de l'Union européenne. Ce point est particulièrement pertinent dans le domaine de l'application de la loi et de la justice pénale. Par conséquent, il convient d'utiliser la technologie de reconnaissance faciale dans le strict respect du cadre juridique applicable.

31. Les informations suivantes sont destinées à être prises en considération lors de l'évaluation des futures mesures législatives et administratives ainsi que lors de l'application de la législation existante à chaque cas qui implique la technologie de reconnaissance faciale. La pertinence des différentes exigences varie en fonction des circonstances particulières: en raison du caractère imprévisible de circonstances futures, il convient de considérer ces informations comme un outil d'aide à la décision et non comme un référentiel exhaustif.

[10] Cette probabilité est appelée «score de confiance».

3.1 Cadre juridique général – La charte des droits fondamentaux de l'Union européenne et la Convention européenne des droits de l'homme (CEDH)

3.1.1 Applicabilité de la charte

32. La charte des droits fondamentaux de l'Union européenne (ci-après la «charte») s'adresse aux institutions, organes et organismes de l'Union, ainsi qu'aux États membres lorsqu'ils mettent en œuvre le droit de l'Union.

33. La réglementation du traitement des données biométriques à des fins répressives conformément à l'article 1er, paragraphe 1, de la directive en matière de protection des données dans le domaine répressif pose inévitablement la question du respect des droits fondamentaux, en particulier du respect de la vie privée et des communications au titre de l'article 7 de la charte et du droit à la protection des données à caractère personnel prévu à l'article 8 de la charte.

34. La collecte et l'analyse de séquences vidéo de personnes physiques, y compris de leurs visages, entraînent le traitement de données à caractère personnel. En cas de traitement technique de l'image, ce dernier englobe également les données biométriques. Le traitement technique de données relatives au visage d'une personne physique en fonction de la date et du lieu permet de tirer des conclusions concernant sa vie privée. Ces conclusions peuvent faire référence aux origines raciales ou ethniques, à la santé, à la religion, aux habitudes de la vie quotidienne, aux lieux de résidence permanents ou temporaires, aux déplacements quotidiens ou autres, aux activités exercées, aux relations sociales de cette personne et aux environnements sociaux dans lesquels elle évolue. Le large éventail d'informations susceptibles d'être révélées par l'application de la technologie de reconnaissance faciale montre clairement les conséquences possibles sur le droit à la protection des données à caractère personnel prévu à l'article 8 de la charte, mais aussi sur le droit au respect de la vie privée inscrit à l'article 7 de la charte.

35. Dans de telles circonstances, il n'est pas non plus inconcevable que la collecte, l'analyse et le traitement ultérieur des données biométriques (faciales) en question puissent avoir un effet sur la manière dont les personnes se sentent libres d'agir, même si elles agissent en parfaite conformité avec ce qui est admis dans une société libre et ouverte. Ils pourraient également avoir de graves conséquences sur l'exercice de leurs droits fondamentaux, tels que leur droit à la liberté de pensée, de conscience et de religion, à la liberté d'expression, et à la liberté de réunion pacifique et à la liberté d'association en vertu des articles 1er, 10, 11 et 12 de la charte. Ce type de traitement comporte également d'autres risques, notamment le risque d'utilisation abusive des données à caractère personnel recueillies par les autorités compétentes à la suite d'un accès et d'une utilisation illicites de ces données, d'une violation de la sécurité, etc. Les risques dépendent souvent du traitement et de ses circonstances, comme le risque d'accès et d'utilisation illicites par des agents de police ou par d'autres parties non autorisées. Toutefois, certains risques sont simplement inhérents à la nature unique des données biométriques. Contrairement à une adresse ou un numéro de téléphone, il est impossible pour une personne concernée de modifier ses caractéristiques uniques, telles que le visage ou l'iris. En cas d'accès non autorisé ou de publication accidentelle de données biométriques, leur utilisation comme mots de passe ou clés cryptographiques serait compromise, ou elles pourraient être utilisées pour d'autres activités de surveillance non autorisées au détriment de la personne concernée.

3.1.2 Atteinte aux droits énoncés dans la charte

36. Le traitement de données biométriques en toutes circonstances constitue une atteinte grave en soi, et ce, quel que soit le résultat, par exemple une concordance positive. Le traitement constitue une

atteinte même si le modèle biométrique est immédiatement supprimé après que la comparaison avec une base de données de la police a abouti à un résultat négatif.

37. L'atteinte aux droits fondamentaux des personnes concernées peut résulter d'un acte de droit qui a pour finalité ou pour effet de restreindre le droit fondamental en question[11]. Elle peut également résulter d'un acte d'une autorité publique ayant la même finalité ou le même effet, voire d'une entité privée chargée par la loi d'exercer l'autorité publique et les pouvoirs publics.

38. Une mesure législative qui sert de base juridique au traitement des données à caractère personnel interfère directement avec les droits garantis par les articles 7 et 8 de la charte[12].

39. L'utilisation des données biométriques et de la technologie de reconnaissance faciale, dans de nombreux cas, porte également souvent atteinte au droit à la dignité humaine, garanti par l'article 1er de la charte. Le principe de dignité humaine exige que les personnes ne soient pas traitées comme de simples objets. La technologie de reconnaissance faciale calcule des caractéristiques existentielles et hautement personnelles, à savoir les traits du visage, sous une forme lisible par machine dans le but de s'en servir comme une plaque d'immatriculation humaine ou une carte d'identité, objectivant ainsi le visage.

40. Un tel traitement peut également interférer avec d'autres droits fondamentaux, tels que les droits prévus aux articles 10, 11 et 12 de la charte, dans la mesure où les effets dissuasifs sont soit prévus par la vidéosurveillance pertinente des autorités répressives, soit découlent de celle-ci.

41. En outre, il convient également d'examiner attentivement les risques susceptibles de naître de l'utilisation des technologies de reconnaissance faciale par les autorités répressives en ce qui concerne le droit d'accéder à un tribunal impartial et la présomption d'innocence visés aux articles 47 et 48 de la charte. Le résultat de l'application de cette technologie, par exemple une concordance, peut non seulement conduire à ce qu'une personne soit soumise à d'autres mesures de police, mais aussi constituer une preuve décisive dans une procédure judiciaire. Les lacunes de la technologie de reconnaissance faciale, notamment la possibilité de partialité, de discrimination ou d'identification erronée («résultat faussement positif»), peuvent donc avoir de graves conséquences, y compris sur les procédures pénales. En outre, lors de l'évaluation des éléments de preuve, le résultat de l'application de la technologie peut être privilégié, même en présence d'éléments de preuve contradictoires («biais d'automatisation»).

3.1.3 Justifications de l'ingérence

42. L'article 52, paragraphe 1, de la charte dispose que toute limitation de l'exercice des droits et libertés doit être prévue par la loi et respecter le contenu essentiel de ces droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

3.1.3.1 Prévue par la loi

43. L'article 52, paragraphe 1, de la charte fixe l'exigence d'une base juridique spécifique. Elle doit être libellée de manière suffisamment claire pour permettre aux citoyens de savoir précisément à quelles conditions et dans quelles circonstances les autorités sont habilitées à recourir à toute mesure de collecte de données et de surveillance secrète[13]. Elle doit indiquer, avec une clarté raisonnable, la

[11] CJUE, C-219/91 – Ter Voort, RoC 1992 I-05485, point 36 et suivants; CJUE, C-200/96 – Metronome, RoC 1998 I-1953, point 28.
[12] CJUE, C-594/12, point 36; CJUE, C-291/12, point 23 et suivants.
[13] Cour européenne des droits de l'homme, Shimovolos c. Russie; Vukota-Bojić c. Suisse, point 68.

portée et les modalités d'exercice du pouvoir discrétionnaire pertinent conféré aux autorités publiques afin d'assurer aux personnes le niveau minimal de protection garanti par l'état de droit dans une société démocratique[14]. En outre, la licéité exige des garanties suffisantes pour garantir, en particulier, le respect du droit d'une personne au titre de l'article 8 de la charte. Ces principes s'appliquent également au traitement de données à caractère personnel effectué à des fins d'évaluation, d'entraînement et de développement des systèmes de technologie de reconnaissance faciale.

44. Étant donné que les données biométriques, lorsqu'elles sont traitées dans le but d'identifier une personne physique de manière unique, constituent des catégories particulières de données énumérées à l'article 10 de la directive en matière de protection des données dans le domaine répressif, les différentes applications de la technologie de reconnaissance faciale nécessiteraient, dans la plupart des cas, une loi spécifique décrivant précisément l'application et les conditions de son utilisation. Cette description englobe notamment les types d'infractions et, le cas échéant, le seuil de gravité approprié de ces infractions, afin, entre autres, d'exclure effectivement les infractions mineures.[15]

3.1.3.2 Le contenu essentiel des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel inscrits aux articles 7 et 8 de la charte

45. Les limitations des droits fondamentaux propres à chaque situation doivent toujours garantir le respect du contenu essentiel du droit particulier. Le contenu essentiel se réfère au noyau même du droit fondamental concerné[16]. Il convient également de respecter la dignité humaine, même lorsqu'un droit est limité[17].

46. Les indices d'une éventuelle violation du noyau intangibles sont les suivants:

- une disposition qui impose des limitations indépendamment du comportement individuel d'une personne ou de circonstances exceptionnelles[18];
- le recours devant les tribunaux est impossible ou entravé[19];
- Avant d'imposer une limitation stricte, les circonstances de la personne concernée ne sont pas prises en considération[20];
- en ce qui concerne les droits prévus aux articles 7 et 8 de la charte: outre une large collecte de métadonnées de communication, l'acquisition de la connaissance du contenu de la communication électronique pourrait porter atteinte à l'essence de ces droits[21];
- En ce qui concerne les droits prévus aux articles 7, 8 et 11 de la charte: la législation qui exige que les fournisseurs d'accès aux services de communication publique en ligne et les fournisseurs de services d'hébergement conservent, de manière générale et sans distinction, entre autres, les données à caractère personnel relatives à ces services[22];
- En ce qui concerne les droits visés à l'article 8 de la charte: l'absence de principes de base en matière de protection et de sécurité des données pourrait également porter atteinte à l'essence même du droit[23].

---

[14] Cour européenne des droits de l'homme, Piechowicz c. Pologne, point 212.
[15] Voir par exemple les arrêts de la CJUE dans les affaires C-817/19 Ligue des droits humains, point 151 f, C-207/16 Ministerio Fiscal, point 56.
[16] CJUE, affaire C-279/09, RoC 2010 I-13849, point 60.
[17] Explications relatives à la charte des droits fondamentaux, titre I, Explication de l'article 1er, JO C 303 du 14.12.2007, p. 17 à 35.
[18] CJUE C-601/15, point 52.
[19] CJUE, affaire C-400/10, RoC 2010 I-08965, point 55.
[20] CJUE, affaire C-408/03, RoC 2006 I-02647, point 68.
[21] CJUE, 203/15 - Tele2 Sverige, point 101 en référence à l'affaire C-293/12 et C-594/12, point 39 de la CJUE.
[22] CJUE C, 512/18, La Quadrature du Net, points 209 et suivants.
[23] CJUE, affaire C-594/12, point 40.

3.1.3.3 L'objectif légitime

47. Comme expliqué au point 3.1.3, les limitations aux droits fondamentaux doivent répondre effectivement à des objectifs d'intérêt général reconnus par l'Union européenne ou répondre au besoin de protection des droits et libertés d'autrui.

48. L'Union reconnaît à la fois les objectifs mentionnés à l'article 3 du traité sur l'Union européenne et d'autres intérêts protégés par des dispositions spécifiques des traités[24], à savoir notamment un espace de liberté, de sécurité et de justice, la prévention de la criminalité et la lutte contre ce phénomène. Dans ses relations avec le reste du monde, l'Union devrait contribuer à la paix et à la sécurité et à la protection des droits de l'homme.

49. La besoin de protection des droits et libertés d'autrui fait référence aux droits des personnes qui sont protégés par le droit de l'Union européenne ou de ses États membres. L'évaluation doit être effectuée dans le but de concilier les exigences de la protection des différents droits et de trouver un juste équilibre entre ceux-ci[25].

3.1.3.4 Test de nécessité et proportionnalité

50. Lorsqu'il s'agit des atteintes aux droits fondamentaux, l'étendue du pouvoir discrétionnaire du législateur national et de l'Union peut se révéler limitée. Tout dépend d'un certain nombre de facteurs, notamment du domaine concerné, de la nature du droit en question garanti par la charte, de la nature et de la gravité de l'atteinte et de l'objectif poursuivi par l'atteinte[26]. Les mesures législatives doivent être appropriées en vue d'atteindre les objectifs légitimes poursuivis par la législation en question. En outre, la mesure ne doit pas dépasser les limites de ce qui est approprié et nécessaire pour atteindre ces objectifs[27]. Un objectif d'intérêt général, aussi fondamental soit-il, ne justifie pas en soi de limiter un droit fondamental[28].

51. Selon la jurisprudence constante de la Cour de justice de l'Union européenne, les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire[29]. Il en découle également qu'il n'existe pas de moyens moins intrusifs pour atteindre l'objectif visé. En fonction de celui-ci, il convient de déterminer et d'évaluer minutieusement d'autres solutions possibles, notamment du personnel supplémentaire, des contrôles plus fréquents ou un éclairage public supplémentaire. Les mesures législatives devraient différencier et cibler les personnes couvertes par ces mesures à la lumière de l'objectif poursuivi, par exemple la lutte contre les formes graves de criminalité. Si elles couvrent toutes les personnes d'une manière générale sans

[24] Explications relatives à la charte des droits fondamentaux de l'Union européenne, titre I, Explication de l'article 52, JO C 303 du 14.12.2007, p. 17 à 35.
[25] Jarass GrCh, 3. Auflage, 2016, Charta der Grundrechte der Europäischen Union, Art. 52, points 31 et 32.
[26] CJUE, affaire C-594/12, point 47 avec les sources suivantes: voir, par analogie, l'article 8 de la CEDH, Cour européenne des droits de l'homme, S. et Marper c. Royaume-Uni [GC], n^{os} 30562/04 et 30566/04, point 102, CEDH, 2008-V.
[27] CJUE, affaire C-594/12, point 46 avec les sources suivantes: affaire C-343/09, Afton Chemical, EU:C:2010:419, point 45; Volker und Markus Schecke et Eifert, EU:C:2010:662, point 74; affaires C-581/10 et C-629/10, Nelson e.a, EU:C:2012:657, point 71; et C-629/10, EU:C:2012:657, point 71; affaire C-283/11 Sky Österreich EU:C:2013:28, point 50; et affaire C-101/12, Schaible, EU:C:2013:661, point 29.
[28] CJUE, affaire C-594/12, point 51.
[29] CJUE, affaire C-594/12, point 52, avec les sources suivantes: affaire C-473/12, IPI, EU:C:2013:715, point 39 et la jurisprudence citée.

une telle différenciation, limitation ou exception, elles accentuent l'atteinte[30]. Il en va de même si le traitement des données porte sur une partie importante de la population[31].

52. La protection des données à caractère personnel résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la charte est particulièrement importante pour le droit au respect de la vie privée consacré à l'article 7 de la charte[32]. La réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences de sorte que les personnes dont les données ont été traitées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données[33]. Le besoin de telles garanties est d'autant plus grand lorsque des données à caractère personnel font l'objet d'un traitement automatique et lorsqu'il existe un risque important d'accès illicite aux données[34]. En outre, l'autorisation interne ou externe, par exemple judiciaire, du déploiement de la technologie de reconnaissance faciale peut également servir de garanties et peut s'avérer nécessaire dans certains cas d'atteinte grave.[35]

53. Il convient d'adapter les règles prévues à la situation spécifique, par exemple en ce qui concerne la quantité de données traitées, la nature des données[36] et le risque d'accès illicite aux données. Il s'agirait alors de mettre en œuvre des règles qui serviraient, en particulier, à régir la protection et la sécurité des données en question de manière claire et stricte en vue de garantir leur intégrité et leur confidentialité totales[37].

54. En ce qui concerne la relation entre le responsable du traitement et le sous-traitant, il ne devrait pas être permis à ce dernier de ne tenir compte que de considérations économiques au moment de déterminer le niveau de sécurité à appliquer aux données à caractère personnel, sous peine de compromettre un niveau de protection suffisamment élevé[38].

55. Un acte de droit doit fixer des conditions de fond et de procédure ainsi que des critères objectifs permettant de déterminer les limites de l'accès accordé aux autorités compétentes aux données et de leur utilisation ultérieure. Aux fins de la prévention, de la détection ou des poursuites pénales, les infractions concernées devraient être considérées comme suffisamment graves pour justifier l'étendue et la gravité de ces atteintes aux droits fondamentaux consacrés, par exemple, par les articles 7 et 8 de la charte[39].

56. Les données doivent être traitées en garantissant l'applicabilité et l'effet des règles de l'Union en matière de protection des données, en particulier celles prévues à l'article 8 de la charte, qui dispose

[30] CJUE, affaire C-594/12, point 57.
[31] CJUE, affaire C-594/12, point 56.
[32] CJUE, affaire C-594/12, point 53.
[33] CJUE, affaire C-594/12, point 54, avec les sources suivantes: voir, par analogie, l'article 8 de la CEDH, Cour européenne des droits de l'homme, Liberty et autres c. Royaume-Uni, nº 58243/00, points 62 et 63, du 1er juillet 2008; Rotaru c. Roumanie, points 57 à 59, ainsi que S et Marper c. Royaume-Uni, point 99).
[34] CJUE, affaire C-594/12, point 55, avec les sources suivantes: voir, par analogie, en ce qui concerne l'article 8 de la CEDH, S. et Marper c. Royaume-Uni, point 103, et M. K. c. France, 18 avril 2013, nº 19522/09, point 35.
[35] Cour européenne des droits de l'homme, Szabó et Vissy c. Hongrie, points 73 à 77.
[36] Voir également les exigences renforcées en matière de mesures techniques et organisationnelles lors du traitement de catégories particulières de données, article 29, paragraphe 1, de la directive en matière de protection des données dans le domaine répressif.
[37] CJUE, affaire C-594/12, point 66.
[38] CJUE, affaire C-594/12, point 67.
[39] CJUE, affaire C-594/12, points 60 et 61.

que le respect des exigences en matière de protection et de sécurité est soumis au contrôle d'une autorité indépendante. Le lieu géographique du traitement peut, dans ce cas, être pertinent[40].

57. Eu égard aux différentes étapes du traitement des données à caractère personnel, il convient d'établir une distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées[41]. La détermination des conditions du traitement, par exemple la détermination de la durée de conservation, doit être fondée sur des critères objectifs en vue de garantir que l'atteinte est limitée à ce qui est strictement nécessaire[42].

58. L'évaluation de la nécessité et de la proportionnalité doit, en fonction de chaque situation, identifier et examiner toutes les incidences qui relèvent du champ d'application d'autres droits fondamentaux, tels que la dignité humaine au sens de l'article 1er de la charte, la liberté de pensée, de conscience et de religion au sens de l'article 10 de la charte, la liberté d'expression au sens de l'article 11 de la charte ainsi que la liberté de réunion et d'association au sens de l'article 12 de la charte.

59. En outre, il convient d'envisager avec gravité que si les données sont systématiquement traitées à l'insu des personnes concernées, l'idée générale d'une surveillance constante pourrait apparaître[43]. Il peut en résulter des effets dissuasifs sur certains droits fondamentaux concernés, ou sur l'ensemble d'entre eux.

60. Afin de faciliter et de rendre opérationnelle l'évaluation de la nécessité et de la proportionnalité des mesures législatives liées à la reconnaissance faciale dans le domaine répressif, les législateurs des États membres et de l'Union pourraient tirer parti des outils pratiques disponibles spécialement conçus pour cette mission. En particulier, la boîte à outils sur la nécessité et la proportionnalité[44] fournie par le Contrôleur européen de la protection des données pourrait être utilisée.

3.1.3.5 Article 52, paragraphe 3, et article 53 de la charte (niveau de protection, y compris par rapport à celui de la CEDH)

61. Selon l'article 52, paragraphe 3, et l'article 53 de la charte, le sens et la portée des droits de ladite charte qui correspondent aux droits garantis par la CEDH doivent être identiques à ceux fixés par la CEDH. Si, pour l'article 7 de la charte, principalement, un équivalent peut être trouvé dans la CEDH, ce n'est pas le cas pour l'article 8 de la charte[45]. L'article 52, paragraphe 3, de la charte n'empêche pas le droit de l'Union de prévoir une protection plus étendue. Étant donné que la CEDH ne constitue pas un instrument juridique formellement intégré au droit de l'Union, la législation de l'Union doit être adoptée à la lumière des droits fondamentaux consacrés par la charte[46].

62. D'après l'article 8 de la CEDH, il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit au respect de la vie privée et familiale que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la

[40] CJUE, affaire C-594/12, point 68.
[41] CJUE, affaire C-594/12, point 63.
[42] CJUE, affaire C-594/12, point 64.
[43] CJUE, affaire C-594/12, point 37.
[44] Contrôleur européen de la protection des données: Évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel: boîte à outils (11.04.2017), Contrôleur européen de la protection des données: Lignes directrices du Contrôleur européen de la protection des données portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel (19.12.2019).
[45] CJUE, affaire C-203/15, Tele2 Sverige, point 129.
[46] CJUE, affaire C-311/18, point 99.

prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

63. La CEDH fixe également des normes relatives à la détermination des limitations. L'une des exigences fondamentales, outre l'état de droit, est la prévisibilité. En vue de satisfaire à l'exigence de prévisibilité, le droit doit être libellé de manière suffisamment claire pour permettre à toutes les personnes de savoir précisément dans quelles circonstances et à quelles conditions la puissance publique est habilitée à prendre de pareilles mesures[47]. Cette exigence est reconnue par la CJUE et la législation de l'Union en matière de protection des données (voir section 3.2.1.1).

64. En complément des droits de l'article 8 de la CEDH, il convient de pleinement respecter les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[48]. Néanmoins, il sied de considérer que ces dispositions ne représentent qu'une norme minimale au regard du droit de l'Union en vigueur.

3.2 Cadre juridique spécifique – la directive en matière de protection des données dans le domaine répressif

65. Un certain cadre concernant l'utilisation de la technologie de reconnaissance faciale est prévu dans la directive en matière de protection des données dans le domaine répressif. Tout d'abord, l'article 3, point 13, de ladite directive définit la notion de «données biométriques»[49]. Pour plus de détails, voir la section 2.1 ci-dessus. Deuxièmement, l'article 8, paragraphe 2, précise que, pour être licite, tout traitement doit être régi par le droit national qui précise au moins les objectifs du traitement, les données à caractère personnel à traiter et la finalité du traitement. Le traitement doit également être nécessaire aux fins énoncées à l'article 1er, paragraphe 1, de la directive. Les articles 10 et 11 de cette même directive constituent d'autres dispositions particulièrement pertinentes en ce qui concerne les données biométriques. L'article 10 doit être lu conjointement avec l'article 8 de la directive[50]. Il y a lieu de toujours respecter les principes de traitement des données à caractère personnel énoncés à l'article 4 de la directive et toute évaluation d'un éventuel traitement biométrique recourant à la technologie de reconnaissance faciale devrait être guidée par ces principes.

3.2.1 Traitement de catégories particulières de données à des fins répressives

66. Conformément à l'article 10 de la directive en matière de protection des données dans le domaine répressif, le traitement de catégories particulières de données, telles que les données biométriques, n'est autorisé que lorsque cela est strictement nécessaire et sous réserve de garanties appropriées pour les droits et les libertés de la personne concernée. En outre, lorsque le droit de l'Union ou de l'État membre l'autorise, il n'est permis que pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique, ou lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée. Cette clause générale souligne le caractère sensible du traitement de catégories particulières de données.

[47] Cour européenne des droits de l'homme, arrêt, AFFAIRE COPLAND c. ROYAUME-UNI, 03/04/2007, requête nº 62617/00, point 46.
[48] STCE nº 108.
[49] Article 3, point 13 de la directive en matière de protection des données dans le domaine répressif: «Données biométriques»: 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.
[50] WP258, Avis sur certaines questions clés de la directive (UE) 2016/680 (directive «police»), p. 8.

3.2.1.1 Autorisé par le droit de l'Union ou de l'État membre

67. Sur la question du type de mesure législative nécessaire, le considérant 33 de la directive en matière de protection des données dans le domaine répressif stipule que «[l]orsque la présente directive fait référence au droit d'un État membre, à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné»[51].

68. L'article 52, paragraphe 1, de la charte dispose que toute limitation de l'exercice des droits et libertés reconnus par la charte doit être «prévue par la loi». Cette disposition rappelle l'expression «prévue par la loi» utilisée à l'article 8, paragraphe 2 de la Convention européenne des droits de l'homme, qui renvoie non seulement au respect du droit applicable, mais aussi à la qualité de celui-ci sans préjudice de la nature de l'acte, qui doit être compatible avec l'état de droit.

69. Le considérant 33 de la directive susmentionnée précise en outre que «[c]ependant, ce droit d'un État membre, cette base juridique ou cette mesure législative devrait être clair et précis et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice et de la Cour européenne des droits de l'homme. Le droit des États membres qui réglemente le traitement des données à caractère personnel relevant du champ d'application de la présente directive devrait préciser au minimum les objectifs, les données à caractère personnel qui feront l'objet d'un traitement, les finalités du traitement et les procédures pour garantir l'intégrité et la confidentialité des données à caractère personnel et les procédures prévues pour la destruction de celles-ci».

70. Le droit national doit être libellé de manière suffisamment claire pour permettre à toutes les personnes concernées de savoir précisément dans quelles circonstances et à quelles conditions les responsables du traitement sont habilités à recourir à de pareilles mesures. Il s'agit notamment d'éventuelles conditions préalables au traitement, telles que des types spécifiques d'éléments de preuve, ainsi que la nécessité d'une autorisation judiciaire ou interne. Le droit concerné peut être neutre sur le plan technologique dans la mesure où les risques et les caractéristiques spécifiques du traitement des données à caractère personnel par les systèmes de reconnaissance faciale sont suffisamment pris en compte. Conformément à la directive en matière de protection des données dans le domaine répressif et à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme, il est en effet essentiel que les mesures législatives, qui visent à fournir une base juridique à une mesure de reconnaissance faciale, soient prévisibles pour les personnes concernées.

71. Une mesure législative ne peut être invoquée en tant que loi autorisant le traitement de données biométriques au moyen de la technologie de reconnaissance faciale à des fins répressives si elle constitue une simple transposition de la clause générale de l'article 10 de la directive susmentionnée.

72. Outre les données biométriques, ledit article 10 réglemente le traitement d'autres catégories particulières de données telles que l'orientation sexuelle, les opinions politiques et les croyances religieuses, couvrant ainsi un large éventail de traitements. En outre, cette disposition ne contiendrait pas d'exigences spécifiques indiquant dans quelles circonstances et à quelles conditions les autorités répressives seraient habilitées à recourir à la technologie de reconnaissance faciale. En raison de la mention d'autres types de données et de la nécessité explicite de garanties spéciales sans autre précision, la disposition transposant l'article 10 de la directive dans le droit national, dont le libellé est tout aussi général et abstrait, ne peut être invoquée en tant que base juridique pour le traitement de données biométriques recourant à la reconnaissance faciale, étant donné qu'elle manquerait de

[51] Le type de mesures législatives envisagées doit être conforme au droit de l'Union ou de l'État membre. En fonction du niveau d'interférence de la limitation, une mesure législative particulière, qui tient compte du niveau de norme, pourrait être requise au niveau national.

précision et de prévisibilité. Il conviendrait de consulter l'autorité nationale de contrôle compétente en matière de protection des données avant que le législateur ne crée une nouvelle base juridique pour toute forme de traitement de données biométriques utilisant la reconnaissance faciale, conformément à l'article 28, paragraphe 2, ou à l'article 46, paragraphe 1, point c), de la directive.

3.2.1.2 Strictement nécessaire

73. Le traitement ne peut être considéré comme «strictement nécessaire» que si l'ingérence dans la protection des données à caractère personnel et ses restrictions sont limitées à ce qui est absolument nécessaire[52]. L'ajout du terme «strictement» traduit l'intention du législateur de ne traiter des catégories particulières de données que dans des conditions encore plus strictes que les conditions de nécessité (voir ci-dessus, point 3.1.3.4). Il convient d'interpréter cette exigence comme étant indispensable. Elle limite la marge d'appréciation laissée à l'autorité répressive lors du test de nécessité à un minimum absolu. Conformément à la jurisprudence constante de la Cour de justice de l'Union européenne, la condition de la «stricte nécessité» est également étroitement liée à l'exigence de critères objectifs afin de définir les circonstances et les conditions dans lesquelles le traitement peut être effectué, excluant ainsi tout traitement de nature générale ou systématique[53].

3.2.1.3 Manifestement rendues publique

74. Lorsqu'il s'agit de déterminer si le traitement concerne des données qui sont manifestement rendues publiques par une personne concernée, il convient de rappeler qu'une photographie en tant que telle n'est pas systématiquement considérée comme une donnée biométrique[54]. Par conséquent, le fait qu'une photographie ait été manifestement rendue publique par la personne concernée ne signifie pas que les données biométriques connexes, qui peuvent être extraites de la photographie par des moyens techniques spécifiques, sont considérées comme ayant été manifestement rendues publiques.

75. Quant aux données à caractère personnel en général, la personne concernée doit avoir délibérément rendu le modèle biométrique (et pas simplement une image faciale) librement accessible et public par l'intermédiaire d'une source ouverte pour que ses données biométriques soient considérées comme manifestement rendues publiques. Si un tiers divulgue les données biométriques, l'on ne peut considérer que les données ont été manifestement rendues publiques par la personne concernée.

76. En outre, il ne suffit pas d'interpréter le comportement d'une personne concernée pour considérer que des données biométriques ont été manifestement rendues publiques. Par exemple, dans le cas des réseaux sociaux ou des plateformes en ligne, le comité européen de la protection des données estime que l'absence d'activation ou de paramétrage de fonctions de confidentialité spécifiques par la personne concernée ne suffit pas pour pouvoir considérer que cette personne a manifestement rendu publiques ses données à caractère personnel et que ces données (par exemple des photographies) peuvent être traitées sous forme de modèles biométriques et utilisées à des fins d'identification sans le consentement de la personne concernée. Plus généralement, il convient de ne pas interpréter comme des données manifestement rendues publiques les paramètres par défaut d'un service,

[52] Jurisprudence cohérente sur le droit fondamental au respect de la vie privée, voir CJUE, affaire C-73/07 point 56 (Satakunnan Markkinapörssi et Satamedia); CJUE, affaires C-92/09 et C-93/09 point 77 (Schecke et Eifert); CJUE, C-594/12, point 52 (droits numériques); CJUE, affaire C-362/14, point 92 (Schrems).

[53] CJUE, affaire C-623/17, point 78.

[54] Voir le considérant 51 du RGPD: «[l]e traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique. »

comme la mise à la disposition du public de modèles ou l'absence de choix, par exemple le fait que les modèles sont rendus publics sans que l'utilisateur puisse modifier ce cadre.

3.2.2 Décision individuelle automatisée, y compris le profilage

77. L'article 11, paragraphe 1, de la directive en matière de protection des données dans le domaine répressif prévoit l'obligation pour les États membres d'interdire, de manière générale, les décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, qui produisent des effets juridiques défavorables pour la personne concernée ou qui l'affectent de manière significative. Par dérogation à cette interdiction générale, un tel traitement ne peut être possible que s'il est autorisé par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis et qui prévoit des garanties appropriées pour les droits et libertés de la personne concernée, à tout le moins le droit d'obtenir une intervention humaine de la part du responsable du traitement. Elle ne peut être utilisée que de manière restrictive. Ce seuil s'applique aux catégories ordinaires (c'est-à-dire non particulières) de données à caractère personnel. Un seuil encore plus élevé et un usage plus restrictif s'appliquent à la dérogation prévue à l'article 11, paragraphe 2, de la directive susmentionnée. Ce dernier souligne une nouvelle fois que les décisions prises en vertu du paragraphe 1 ne sont pas fondées sur des catégories particulières de données, à savoir, en particulier, des données biométriques aux fins d'identifier une personne physique de manière unique. Une dérogation ne peut être prévue que si des mesures appropriées pour la sauvegarde des droits et libertés de la personne concernée et des intérêts légitimes de la personne physique concernée sont en place. Elle doit être lue en complément et à la lumière des prémisses de l'article 10 de la directive.

78. En fonction du système de reconnaissance faciale, même une intervention humaine évaluant ses résultats ne constitue pas nécessairement une garantie suffisante permettant de respecter les droits des personnes et en particulier le droit à la protection des données à caractère personnel, compte tenu de la partialité et de l'erreur qui peuvent résulter du traitement lui-même. En outre, l'intervention humaine ne peut être considérée comme une garantie que si la personne qui intervient peut remettre en question de manière critique les résultats de la technologie de reconnaissance faciale au moment de l'intervention humaine. Il est primordial de permettre à la personne de comprendre le système de reconnaissance faciale et ses limites, ainsi que d'interpréter correctement ses résultats. Il est également nécessaire de mettre en place un lieu de travail et une organisation qui contrebalancent les effets du biais d'automatisation et qui évitent de favoriser l'acceptation non critique des résultats, par exemple en raison du manque de temps, de la lourdeur des procédures, des effets néfastes potentiels sur la carrière, etc.

79. En vertu de l'article 11, paragraphe 3, de la directive, tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel, telles que les données biométriques, est interdit, conformément au droit de l'Union. D'après l'article 3, point 4, de la directive, «profilage» renvoie à toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne. Lorsque l'on examine si des mesures appropriées sont prévues pour sauvegarder les droits et libertés de la personne concernée et les intérêts légitimes de la personne physique, il faut garder à l'esprit que l'utilisation de la technologie de reconnaissance faciale peut conduire à un profilage, en fonction de son application et de la finalité pour laquelle elle est utilisée. En tout état de cause, conformément au droit de l'Union et à l'article 11, paragraphe 3, de la directive, le profilage entraînant

une discrimination à l'égard de personnes physiques sur la base de catégories particulières de données à caractère personnel est interdit.

3.2.3 Catégories des personnes concernées

80. L'article 6 de la directive en matière de protection des données dans le domaine répressif concerne la nécessité d'établir une distinction entre les différentes catégories de personnes concernées, et ce, le cas échéant et dans la mesure du possible. Elle doit se manifester dans la manière de traiter les données. Les exemples donnés audit article permettent de déduire qu'en règle générale, le traitement des données à caractère personnel doit répondre aux critères de nécessité et de proportionnalité, y compris en ce qui concerne la catégorie de personnes concernées[55]. Il est également possible de déduire qu'en ce qui concerne les personnes concernées pour lesquelles il n'existe aucun élément de preuve susceptible de suggérer que leur comportement pourrait avoir un lien, même indirect ou lointain, avec l'objectif légitime prévu par la directive, il n'y a très probablement aucune justification d'une ingérence[56]. Si aucune distinction au sens de l'article 6 de ladite directive n'est applicable ou possible, il convient de tenir rigoureusement compte de la dérogation à la règle dudit article dans l'évaluation de la nécessité et de la proportionnalité de l'ingérence. La distinction entre les différentes catégories de personnes concernées apparaît comme une exigence essentielle lorsqu'il s'agit de traitement de données à caractère personnel impliquant la reconnaissance faciale, compte tenu également de la possibilité de résultats faussement positifs ou faussement négatifs, qui peuvent avoir des conséquences importantes pour les personnes concernées ainsi que dans le cadre d'une enquête.

81. Comme indiqué précédemment, lors de la mise en œuvre du droit de l'Union, les dispositions de la charte des droits fondamentaux de l'Union européenne doivent être respectées (voir article 52 de la charte). Le cadre et les critères prévus par la directive en matière de protection des données dans le domaine répressif doivent donc être lus à la lumière de la charte. Les actes juridiques de l'Union et de ses États membres ne doivent pas être en deçà de cette mesure et doivent garantir le plein effet de la charte.

3.2.4 Droits de la personne concernée

82. Le comité européen de la protection des données a déjà fourni des orientations sur les droits des personnes concernées dans le cadre du RGPD sous différents aspects[57]. La directive en matière de protection des données dans le domaine répressif prévoit des droits similaires pour les personnes concernées et un avis du groupe de travail «article 29» comprend des orientations générales à ce sujet, cet avis ayant été approuvé par le comité européen de la protection des données[58]. Dans certaines circonstances, la directive susmentionnée prévoit des limitations de ces droits, les paramètres de celles-ci étant développés plus en détail à la section 3.2.4.6. intitulée «Limites légitimes des droits de la personne concernée».

83. Bien que l'ensemble des droits des personnes concernées énumérés au chapitre III de la directive en matière de protection des données dans le domaine répressif s'appliquent naturellement au traitement des données à caractère personnel au moyen de la technologie de reconnaissance faciale, le chapitre suivant se concentre sur certains des droits et aspects sur lesquels il pourrait être particulièrement intéressant de recevoir des orientations. En outre, ce chapitre et son analyse

[55] Voir également CJUE, affaire C-594/12, points 56 à 59.
[56] Voir également CJUE, affaire C-594/12, point 58.
[57] Voir, par exemple, les lignes directrices 1/2022 du comité européen de la protection des données sur les droits des personnes concernées — Droit d'accès et les lignes directrices 3/2019 du comité européen de la protection des données sur le traitement des données à caractère personnel par dispositifs vidéo.
[58] WP258, Avis sur certaines questions clés de la directive en matière de protection des données dans le domaine répressif (UE 2016/680).

reposent sur le fait que le traitement réalisé avec la technologie de reconnaissance faciale en question a été soumis aux exigences légales décrites dans le chapitre précédent.

84. Compte tenu de la nature du traitement des données à caractère personnel effectué avec la technologie de reconnaissance faciale (traitement portant sur des catégories particulières de données à caractère personnel qui s'effectue souvent sans interaction apparente avec la personne concernée), le responsable du traitement doit examiner attentivement la manière (ou la possibilité) de satisfaire aux exigences de la directive susmentionnée avant de lancer tout traitement recourant à la technologie de reconnaissance faciale. En particulier, en analysant attentivement:

- qui sont les personnes concernées (souvent plus que la ou les personnes qui constituent la principale cible aux fins du traitement),
- la manière dont les personnes concernées sont informées du traitement recourant à la technologie de reconnaissance faciale (voir section 3.2.4.1),
- la manière dont les personnes concernées peuvent exercer leurs droits (à cet égard, les droits d'information et d'accès ainsi que les droits de rectification ou de limitation peuvent être particulièrement difficiles à faire respecter si la technologie de reconnaissance faciale est utilisée pour toutes les vérifications autres que la vérification en mode un à un en contact direct avec la personne concernée).

3.2.4.1 Faire connaître les droits et les informations aux personnes concernées sous une forme concise, intelligible et facilement accessible

85. La technologie de reconnaissance faciale pose des problèmes lorsqu'il s'agit de s'assurer que les personnes concernées sont informées du traitement de leurs données biométriques. La situation est particulièrement difficile lorsqu'une autorité répressive analyse, à l'aide de cette technologie, du matériel vidéo provenant d'un tiers ou fourni par celui-ci, étant donné qu'elle n'a guère la possibilité, et la plupart du temps aucune, d'informer la personne concernée au moment de la collecte (par exemple au moyen d'un panneau sur place). Tout matériel vidéo non pertinent pour l'enquête (ou pour la finalité du traitement) devrait toujours être supprimé ou anonymisé (par exemple par floutage sans possibilité de récupération rétroactive des données) avant tout traitement de données biométriques, afin d'éviter le risque de non-respect du principe de minimisation énoncé à l'article 4, paragraphe 1, point e), de la directive en matière de protection des données dans le domaine répressif et les obligations d'information énoncées à l'article 13, paragraphe 2, de ladite directive. Il incombe au responsable du traitement d'évaluer quelles informations seraient importantes pour la personne concernée dans l'exercice de ses droits et de veiller à la fourniture des informations nécessaires. L'exercice effectif des droits de la personne concernée dépend du respect par le responsable du traitement de ses obligations d'information.

86. L'article 13, paragraphe 1, de la directive susmentionnée précise quelles informations minimales doivent être fournies à la personne concernée en général. Ces informations peuvent être fournies sur le site internet du responsable du traitement, sous forme imprimée (par exemple, un dépliant disponible sur demande) ou par d'autres sources faciles d'accès pour la personne concernée. En tout état de cause, le responsable du traitement doit veiller à ce que les informations soient effectivement fournies en ce qui concerne au moins les éléments suivants:

- l'identité et les coordonnées du responsable du traitement, y compris du délégué à la protection des données;

- la finalité du traitement et le fait qu'il s'agit d'un traitement recourant à la technologie de reconnaissance faciale;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle et les coordonnées de cette dernière;
- le droit de demander l'accès aux données à caractère personnel, leur rectification ou leur effacement, ainsi que la limitation du traitement des données à caractère personnel.

87. En outre, dans des cas spécifiques définis par le droit national, qui devraient être en conformité avec l'article 13, paragraphe 2, de la directive précédemment mentionnée[59], par exemple le traitement recourant à la technologie de reconnaissance faciale, les informations suivantes doivent être fournies directement à la personne concernée:

- la base juridique du traitement;
- des informations sur le lieu de collecte des données à caractère personnel effectuée à l'insu de la personne concernée;
- la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;
- le cas échéant, les catégories de destinataires des données à caractère personnel (y compris les pays tiers et les organisations internationales).

88. Alors que l'article 13, paragraphe 1, de la directive concerne les informations générales mises à la disposition du public, l'article 13, paragraphe 2, concerne quant à lui les informations supplémentaires à fournir à une personne concernée dans des cas spécifiques, par exemple lorsque des données sont collectées directement auprès de la personne concernée ou indirectement à son insu[60]. Il n'existe pas de définition claire de ce que l'on entend par «cas spécifiques» à l'article 13, paragraphe 2, de la directive. Toutefois, ils font référence à des situations dans lesquelles les personnes concernées doivent être informées du traitement qui les concerne spécifiquement et recevoir des informations appropriées afin d'exercer effectivement leurs droits. Lors de la détermination d'un «cas spécifique», le comité européen de la protection des données estime qu'il convient de tenir compte de plusieurs facteurs, y compris si des données à caractère personnel sont collectées à l'insu de la personne concernée, étant donné qu'il s'agirait de la seule manière de permettre aux personnes concernées d'exercer effectivement leurs droits. D'autres exemples de «cas spécifiques» pourraient être les cas dans lesquels des données à caractère personnel sont traitées ultérieurement dans le cadre d'une procédure de coopération pénale internationale ou dans le cas d'un traitement de données à caractère personnel dans le cadre d'opérations sous couverture, comme le prévoit le droit national. En outre, il découle du considérant 38 de la directive que si la décision est prise uniquement sur la base de la technologie de reconnaissance faciale, les personnes concernées doivent être informées des caractéristiques de la prise de décision automatisée. Cet aspect permettrait également d'indiquer qu'il

[59] Par exemple, l'article 56, paragraphe 1, de la loi fédérale allemande sur la protection des données, qui précise, entre autres, quelles informations doivent être fournies aux personnes concernées dans le cadre des opérations sous couverture.

[60] WP258, Avis sur certaines questions clés de la directive en matière de protection des données dans le domaine répressif (UE 2016/680), p. 17-18

s'agit d'un cas spécifique dans lequel des informations supplémentaires devraient être fournies à la personne concernée conformément à l'article 13, paragraphe 2, de la directive[61].

89. Enfin, il faut préciser qu'en vertu de l'article 13, paragraphe 3, de la directive, les États membres peuvent adopter des mesures législatives qui limitent l'obligation de fournir des informations dans des cas spécifiques pour certains objectifs. Cette disposition s'applique dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne concernée.

3.2.4.2 Droit d'accès

90. De manière générale, la personne concernée a le droit de recevoir une confirmation positive ou négative de tout traitement de ses données à caractère personnel et, en cas de réponse positive, l'accès aux données à caractère personnel en tant que telles, ainsi que des informations supplémentaires, comme celles énumérées à l'article 14 de la directive en matière de protection des données dans le domaine répressif. En ce qui concerne la technologie de reconnaissance faciale, lorsque les données biométriques sont stockées et liées à une identité également par des données alphanumériques, l'autorité compétente devrait pouvoir confirmer une demande d'accès sur la base d'une recherche à partir de ces données alphanumériques et sans devoir lancer d'autre traitement des données biométriques d'autres personnes (c'est-à-dire en effectuant une recherche à l'aide de la technologie de reconnaissance faciale dans une base de données). Il convient de respecter le principe de minimisation des données et de ne pas stocker plus de données que ce qui est nécessaire au regard de la finalité du traitement.

3.2.4.3 Le droit à la rectification des données à caractère personnel

91. Étant donné que la technologie de reconnaissance faciale ne prévoit pas une exactitude absolue, il est particulièrement important que les responsables du traitement soient attentifs aux demandes de rectification des données à caractère personnel. Il peut également arriver qu'une personne concernée ait été placée dans une catégorie inexacte à cause de la technologie de reconnaissance faciale, par exemple en étant classée à tort dans la catégorie des suspects sur la base d'une supposition initiale de la façon d'agir dans une séquence vidéo. Les risques pour les personnes concernées sont particulièrement graves si ces données inexactes sont stockées dans une base de données de la police et/ou partagées avec d'autres entités. Le responsable du traitement doit corriger les données stockées et les systèmes de reconnaissance faciale en conséquence (voir le considérant 47 de la directive en matière de protection des données dans le domaine répressif).

3.2.4.4 Droit à l'effacement

92. Dans la plupart des cas, si elle n'est pas utilisée pour la vérification ou l'authentification en mode un à un, la technologie de reconnaissance faciale équivaudra au traitement d'un grand nombre de données biométriques des personnes concernées. Il est donc important que le responsable du traitement examine au préalable les limites à sa finalité et à sa nécessité, de sorte qu'une demande d'effacement conformément à l'article 16 de la directive en matière de protection des données dans le domaine répressif puisse être traitée sans retard injustifié (étant donné que le responsable du traitement doit,

[61] Il convient de noter la différence entre «met à la disposition de la personne concernée» à l'article 13, paragraphe 1, de la directive en matière de protection des données dans le domaine répressif et «fournit à la personne concernée» à l'article 13, paragraphe 2, de ladite directive. Dans ce paragraphe, le responsable du traitement doit veiller à ce que les informations parviennent à la personne concernée, lorsque les informations publiées sur un site internet ne sont pas suffisantes.

entre autres, effacer les données à caractère personnel qui sont traitées au-delà de ce que permet la législation applicable en vertu des articles 4, 8 et 10 de ladite directive).

3.2.4.5 Droit à la limitation

93. Si l'exactitude des données est contestée par la personne concernée et qu'elle ne peut être vérifiée (ou si les données à caractère personnel doivent être conservées à des fins de preuve ultérieure), le responsable du traitement a l'obligation de limiter les données à caractère personnel de cette personne conformément à l'article 16 de la directive sur la protection des données dans le domaine répressif. Cette obligation est d'autant plus importante lorsqu'il s'agit de la technologie de reconnaissance faciale (fondée sur un ou plusieurs algorithmes et ne présentant donc jamais de résultat définitif) dans des situations présentant de grandes quantités de données collectées et un éventuel écart dans l'exactitude et la qualité de l'identification. Un matériel vidéo de mauvaise qualité (provenant d'une scène de crime, par exemple) entraîne une augmentation du risque de faux positifs. En outre, un manque de mises à jour régulières des images faciales figurant sur une liste de surveillance augmentera également le risque de résultats faussement positifs ou faussement négatifs. Dans des cas spécifiques, lorsque des données ne peuvent pas être effacées parce qu'il existe des motifs raisonnables de croire que l'effacement pourrait porter atteinte aux intérêts légitimes de la personne concernée, il conviendrait plutôt de limiter les données et de les traiter uniquement aux fins qui ont empêché leur effacement (voir le considérant 47 de la directive susmentionnée).

3.2.4.6 Limitations légitimes des droits de la personne concernée

94. En ce qui concerne les obligations d'information du responsable du traitement et le droit d'accès des personnes concernées, les limitations ne sont autorisées que dans la mesure où elles sont prévues par la loi. Cette dernière doit elle-même constituer une mesure nécessaire et proportionnée dans une société démocratique, dans le respect des droits fondamentaux et des intérêts légitimes de la personne physique concernée (voir l'article 13, paragraphes 3 et 4, l'article 15 et l'article 16, paragraphe 4, de la directive en matière de protection des données dans le domaine répressif). Lorsque la technologie de reconnaissance faciale est utilisée à des fins répressives, l'on peut s'attendre à ce qu'elle soit utilisée dans des circonstances dans lesquelles informer la personne concernée ou autoriser l'accès aux données serait préjudiciable pour l'objectif poursuivi. Tel est le cas, par exemple, dans le cadre d'une enquête policière sur un crime ou pour protéger la sécurité nationale ou la sécurité publique.

95. Le droit d'accès ne donne pas automatiquement l'accès à toutes les informations, par exemple dans une affaire pénale où les données personnelles d'une personne sont en jeu. Un exemple plausible de cas dans lequel des limitations du droit peuvent être autorisées pourrait être dans le cadre d'une enquête pénale.

3.2.4.7 Exercice des droits par l'intermédiaire de l'autorité de contrôle

96. Dans les cas de limitations légitimes à l'exercice des droits en vertu du chapitre III de la directive en matière de protection des données dans le domaine répressif, la personne concernée peut demander à l'autorité de protection des données d'exercer ses droits en son nom en vérifiant la licéité du traitement du responsable du traitement. Il incombe au responsable du traitement d'informer la personne concernée de la possibilité d'exercer ses droits de cette manière (voir article 17 et article 46, paragraphe 1, point g), de la directive). Pour la technologie de reconnaissance faciale, le responsable du traitement doit alors veiller à la mise en place de mesures appropriées pour que cette demande puisse être traitée, par exemple en permettant la recherche de documents enregistrés, à condition que la personne concernée fournisse des informations suffisantes pour localiser les données à caractère personnel la concernant.

3.2.5 Autres exigences légales et garanties

3.2.5.1 Article 27 sur l'analyse d'impact relative à la protection des données

97. Une analyse d'impact relative à la protection des données (AIPD) avant de recourir à la technologie de reconnaissance faciale constitue une obligation, étant donné que le type de traitement, en particulier avec les nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, compte tenu de la nature, de la portée, du contexte et des finalités du traitement. L'utilisation de la technologie de reconnaissance faciale impliquant un traitement automatique systématique des catégories particulières de données, l'on pourrait supposer que, dans de tels cas, le responsable du traitement serait, en principe, tenu de procéder à une AIPD. Ladite analyse devrait contenir au minimum une description générale des opérations de traitement envisagées, une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, les mesures de sécurité et les mécanismes visant à assurer la protection des données à caractère personnel et à démontrer la conformité. Le comité européen de la protection des données recommande de publier les résultats de ces évaluations ou, à tout le moins, les principaux résultats et conclusions de l'AIPD, afin de renforcer la confiance et la transparence[62].

3.2.5.2 Article 28 sur la consultation préalable de l'autorité de contrôle

98. Conformément à l'article 28 de la directive en matière de protection des données dans le domaine répressif, le responsable du traitement ou le sous-traitant doit consulter l'autorité de contrôle avant le traitement: a) lorsqu'une analyse d'impact relative à la protection des données indique que le traitement entraînerait un risque élevé en l'absence de mesures prises par le responsable du traitement pour atténuer le risque; ou b) lorsque le type de traitement, en particulier avec les nouvelles technologies, de nouveaux mécanismes ou de nouvelles procédures, comporte un risque élevé pour les droits et libertés des personnes concernées. Comme expliqué à la section 2.3 des présentes lignes directrices, le comité européen de la protection des données estime que la plupart des cas de déploiement et d'utilisation de la technologie de reconnaissance faciale comportent un risque intrinsèque élevé pour les droits et les libertés des personnes concernées. Par conséquent, en plus de l'analyse d'impact relative à la protection des données, l'autorité qui déploie la technologie de reconnaissance faciale devrait consulter l'autorité de contrôle compétente avant son déploiement.

3.2.5.3 Article 29 sur la sécurité du traitement

99. En raison de la nature unique des données biométriques, il est impossible pour une personne concernée de les modifier en cas de compromission, par exemple à la suite d'une violation de données. Par conséquent, l'autorité compétente qui met en œuvre et/ou utilise la technologie de reconnaissance faciale devrait accorder une attention particulière à la sécurité du traitement, conformément à l'article 29 de la directive en matière de protection des données dans le domaine répressif. En particulier, l'autorité répressive devrait veiller à la conformité du système avec les normes pertinentes et mettre en œuvre des mesures de protection des modèles biométriques[63]. Cette obligation est d'autant plus pertinente si l'autorité répressive fait appel à un prestataire de services tiers (sous-traitant de données).

[62] Pour plus d'informations, voir WP248 rév. 01, 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».

[63] Voir, par exemple: ISO/IEC 24745 Sécurité de l'information, cybersécurité et protection de la vie privée — Protection des informations biométriques.

3.2.5.4 Article 20 sur la protection des données dès la conception et la protection des données par défaut

100. La protection des données dès la conception et la protection des données par défaut, conformément à l'article 20 de la directive en matière de protection des données dans le domaine répressif, vise à garantir que les principes et garanties de protection des données, comme la minimisation des données et la limitation du stockage, sont intégrés dans la technologie grâce à des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, avant même le début du traitement des données à caractère personnel et seront appliquées tout au long de leur cycle de vie. Compte tenu du risque élevé inhérent aux droits et libertés des personnes physiques, le choix de ces mesures ne devrait pas dépendre uniquement de considérations économiques[64]. Il devrait plutôt viser à mettre en œuvre l'état de l'art en matière de technologies de protection des données. Dans le même ordre d'idées, si une autorité répressive a l'intention d'appliquer et d'utiliser la technologie de reconnaissance faciale provenant de fournisseurs externes, elle doit veiller, par exemple par le biais d'une procédure de passation de marchés, au déploiement de technologies de reconnaissance faciale fondées sur les principes de la protection des données dès la conception et de la protection des données par défaut uniquement[65]. La transparence sur le fonctionnement de la technologie de reconnaissance faciale n'est donc pas limitée par des revendications de secrets commerciaux ou de droits de propriété intellectuelle.

3.2.5.5 Article 25 sur la journalisation

101. La directive en matière de protection des données dans le domaine répressif prévoit différentes méthodes permettant au responsable du traitement ou au sous-traitant de démontrer la licéité du traitement et de garantir l'intégrité et la sécurité des données. À cet égard, les journaux du système constituent un outil très utile et une garantie importante pour la vérification de la licéité du traitement, tant en interne (c'est-à-dire l'autocontrôle) que par les autorités de contrôle externes, telles que les autorités de protection des données. En vertu de l'article 25 de la directive, il convient d'établir des journaux au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé: la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement. En outre, les journaux des opérations de consultation et de communication devraient permettre d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué des données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel. Dans le contexte des systèmes de reconnaissance faciale, il est également recommandé de consigner les opérations de traitement supplémentaires suivantes (en partie au-delà de l'article 25 de la directive):

- les modifications de la base de données de référence (ajout, suppression ou mise à jour). Le journal devrait conserver une copie de l'image pertinente (ajoutée, supprimée ou mise à jour) lorsqu'il n'est pas possible de vérifier autrement la licéité ou le résultat des opérations de traitement;

- les tentatives d'identification ou de vérification, y compris le résultat et le score de confiance. Le principe de minimisation stricte devrait s'appliquer, de sorte que seul l'identifiant de l'image de la base de données de référence soit conservé dans les journaux, au lieu de stocker l'image de

[64] Voir considérant 53 de la directive en matière de protection des données dans le domaine répressif.

[65] Pour de plus amples informations, voir les lignes directrices du comité européen de la protection des données sur la protection des données dès la conception et la protection des données par défaut, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

référence. Il convient d'éviter de consigner les données biométriques d'entrée, sauf si cela est nécessaire (par exemple, uniquement dans les cas de concordance);

- l'identifiant de l'utilisateur qui a demandé la tentative d'identification ou de vérification;

- les données à caractère personnel stockées dans les journaux des systèmes sont soumises à des limitations strictes (par exemple, des audits) et ne devraient pas être utilisées à d'autres fins (par exemple, pour être en mesure de continuer à procéder à la reconnaissance/vérification, y compris une image qui a été supprimée des bases de données de référence). Il conviendrait de mettre en œuvre des mesures de sécurité en vue de garantir l'intégrité des journaux, et des systèmes de surveillance automatique visant à détecter les abus de journaux sont fortement recommandés. Pour les journaux de la base de données de référence, les mesures de sécurité devraient être équivalentes à celles de la base de données de référence, en cas de stockage d'images faciales. En outre, il faudrait mettre en place des processus automatiques visant à garantir le respect de la durée de conservation des données pour les journaux.

3.2.5.6 Article 4, paragraphe 4, sur la responsabilité

102. Le responsable du traitement doit être en mesure de démontrer la conformité du traitement avec les principes énoncés à l'article 4, paragraphes 1 à 3, conformément à l'article 4, paragraphe 4, de la directive en matière de protection des données dans le domaine répressif. Une documentation systématique et actualisée du système (y compris les mises à jour, les mises à niveau et la formation algorithmique), des mesures techniques et organisationnelles (y compris le contrôle des performances du système et l'intervention humaine potentielle) et du traitement des données à caractère personnel est primordiale à cet égard. La journalisation est particulièrement importante pour démontrer la licéité du traitement, conformément à l'article 25 de la directive (voir section 3.2.5.5). Le principe de responsabilité concerne le système et le traitement, ainsi que la documentation des garanties procédurales telles que les évaluations de la nécessité et de la proportionnalité, les AIPD et les consultations internes (par exemple, l'approbation par la direction du projet ou les décisions internes sur les valeurs de score de confiance) et les consultations externes (par exemple, l'autorité de protection des données). L'annexe II contient un certain nombre d'éléments à cet égard.

3.2.5.7 Article 47 sur le contrôle effectif

103. Le contrôle effectif par les autorités compétentes de protection des données constitue l'une des garanties les plus importantes pour les libertés et droits fondamentaux des personnes concernées par le recours à la technologie de reconnaissance faciale. Fournir à chaque autorité de protection des données les ressources humaines, techniques et financières, des locaux et des infrastructures nécessaires est une condition préalable à l'accomplissement efficace de leurs tâches et à l'exercice de leurs pouvoirs[66]. Plus cruciales encore que le nombre de personnes disponibles sont les compétences des experts, qui devraient couvrir un très large éventail de questions, allant des enquêtes pénales et de la coopération policière à l'analyse des mégadonnées et à l'intelligence artificielle. Par conséquent, les États membres devraient veiller à ce que les ressources des autorités de contrôle soient appropriées et suffisantes pour leur permettre de remplir leur mandat de protection des droits des personnes concernées et suivre de près toute évolution à cet égard[67].

[66] Voir la communication de la Commission intitulée «Premier rapport sur l'application et le fonctionnement de la directive (UE) 2016/680 en matière de protection des données dans le domaine répressif, COM(2022) 364 final, point 3.4.1.

[67] Voir la contribution du comité européen de la protection des données à l'évaluation, par la Commission européenne, de la directive en matière de protection des données dans le domaine répressif au titre de

4 CONCLUSION

104. L'utilisation des technologies de reconnaissance faciale est intrinsèquement liée au traitement de quantités importantes de données à caractère personnel, y compris de catégories particulières de données. Le visage et, plus généralement, les données biométriques sont liés de manière permanente et irrévocable à l'identité d'une personne. Par conséquent, l'utilisation de la reconnaissance faciale a une incidence directe ou indirecte sur un certain nombre de libertés et droits fondamentaux inscrits dans la charte des droits fondamentaux de l'Union européenne, qui peuvent aller au-delà du respect de la vie privée et de la protection des données, comme la dignité humaine, la liberté de circulation, la liberté de réunion, etc. Ce point est particulièrement pertinent dans le domaine de l'application de la loi et de la justice pénale.

105. Le comité européen de la protection des données comprend qu'il est essentiel que les autorités répressives aient à leur disposition les meilleurs outils possible pour identifier rapidement les auteurs d'actes terroristes ou d'autres infractions pénales graves. Toutefois, ces outils devraient être utilisés dans le strict respect du cadre juridique applicable et uniquement dans les cas où ils satisfont aux exigences de nécessité et de proportionnalité, comme le prévoit l'article 52, paragraphe 1, de la charte. En outre, si les technologies modernes peuvent faire partie de la solution, elles ne constituent en aucun cas une «solution miracle».

106. Certains cas d'utilisation de la technologie de reconnaissance faciale présentent des risques inacceptables pour les personnes et la société («lignes rouges»). C'est pourquoi le comité européen de la protection des données et le contrôleur européen de la protection des données ont demandé leur interdiction générale[68].

107. Ainsi, l'identification biométrique des personnes effectuée à distance dans des espaces accessibles au public présente un risque élevé d'intrusion dans la vie privée des personnes et n'a pas sa place dans une société démocratique, étant donné que, par nature, elle se traduit par une surveillance de masse. Dans le même ordre d'idées, le comité européen de la protection des données estime que les systèmes de reconnaissance faciale fondés sur l'IA qui classent les personnes à partir de leurs données biométriques dans des groupes en fonction de l'origine ethnique, du genre, ainsi que des opinions politiques ou de l'orientation sexuelle, ne sont pas compatibles avec la charte. En outre, le comité européen de la protection des données est convaincu que l'utilisation de la reconnaissance faciale ou de technologies similaires pour déduire les émotions d'une personne physique est hautement indésirable et devrait être interdite, éventuellement avec peu d'exceptions dûment justifiées. Le comité européen de la protection des données estime également que le traitement de données à caractère personnel dans un contexte répressif qui s'appuierait sur une base de données alimentée par la collecte de données à caractère personnel à grande échelle et de manière indifférenciée, par exemple en «extrayant» des photographies et des images faciales accessibles en ligne, en particulier celles mises à disposition par l'intermédiaire des réseaux sociaux, ne satisferait pas, en tant que telle, à l'exigence de stricte nécessité prévue par le droit de l'Union.

---

l'article 62, paragraphe 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.

[68] Voir l'avis conjoint 5/2021 du comité européen de la protection des données et du contrôleur européen de la protection des données sur la «Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées en matière d'intelligence artificielle (Législation sur l'intelligence artificielle)https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

5 ANNEXES

Annexe I: Modèle d’assistance

Annexe II: Orientations pratiques pour les autorités répressives sur la gestion des projets de technologie de reconnaissance faciale

Annexe III: Exemples concrets

ANNEXE I – MODELE DE DESCRIPTION DES SCENARIOS

(Avec des boîtes d'information pour les aspects traités dans le scénario)

Description du traitement:

- Description du traitement, contexte (lien avec le crime), finalité

Source d'informations:

- Types de personnes concernées: ☐ tous les citoyens ☐ les condamnés ☐ les suspects
  ☐ les enfants ☐ les autres personnes vulnérables
- Source de l'image: ☐ espaces accessibles au public ☐ internet
  ☐ entité privée ☐ autres personnes physiques ☐ autres .....
- Lien avec le crime: ☐ Lien temporel direct ☐ Lien temporel non direct
  ☐ Lien géographique direct ☐ Lien géographique non direct
  ☐ Pas nécessaire
- Mode de saisie de l'information: ☐ à distance ☐ dans une cabine ou un environnement contrôlé
- Contexte – incidence sur d'autres droits fondamentaux:
  ☐ Non
  Oui, à savoir ☐ Liberté de réunion
  ☐ Liberté d'expression
  ☐ Divers:.....
- Possibilités en matière de sources d'information supplémentaires sur la personne concernée:
  ☐ Document d'identité ☐ Utilisation d'un téléphone public ☐ Plaque d'immatriculation du véhicule
  ☐ Autre .....

Base de données de référence (à laquelle les informations saisies sont comparées):

- Spécificité: ☐ bases de données à finalité générale ☐ bases de données spécifiques liées au domaine de la criminalité
- Description de l'alimentation de ces bases de données de référence (et leur base juridique)
- Changement de finalité de la base de données (par exemple, la sécurité des biens privés était l'objectif principal): ☐ OUI ☐ NON

Algorithme:

- Type de traitement: ☐ vérification en mode un à un» (authentification) ☐ identification en mode un à plusieurs
- Considérations liées à la précision

- Garanties techniques

Résultat:

- Incidence: ☐ directe (par exemple, la personne concernée peut être arrêtée, interrogée, ou comportement discriminatoire)

  ☐ non directe (utilisé pour les modèles statistiques, aucune action en justice grave à l'encontre des personnes concernées)

- Décision automatisée: ☐ OUI ☐ NON
- Durée de conservation

Analyse juridique:

- Analyse de la nécessité et de la proportionnalité — Finalité/gravité du crime/nombre de personnes non impliquées mais concernées par le traitement
- Type d'information préalable à la personne concernée: ☐ Lors de l'entrée dans la zone spécifique

  ☐ De manière générale sur le site internet de l'autorité répressive

  ☐ Sur le site internet de l'autorité répressive pour le traitement spécifique

  ☐ Autre .....
- Cadre juridique applicable:

  ☐ Directive en matière de protection des données dans le domaine répressif principalement transposée dans le droit national

  ☐ Droit national générique pour l'utilisation des données biométriques par les autorités répressives

  ☐ Droit national spécifique pour ce traitement (reconnaissance faciale) pour cette autorité compétente

  ☐ Droit national spécifique pour ce traitement (décision automatisée)

Conclusion:

Considérations générales sur la question de savoir si le traitement décrit est susceptible d'être compatible avec le droit de l'Union (et certaines indications relatives aux conditions juridiques préalables)

ANNEXE II – ORIENTATIONS PRATIQUES POUR LES AUTORITES REPRESSIVES SUR LA GESTION DES PROJETS DE TECHNOLOGIE DE RECONNAISSANCE FACIALE

La présente annexe fournit des orientations pratiques supplémentaires à l'intention des autorités répressives qui prévoient de lancer un projet utilisant la technologie de reconnaissance faciale. Elle donne davantage d'informations sur les mesures organisationnelles et techniques à envisager lors du déploiement du projet et ne doit pas être considérée comme une liste exhaustive des étapes à suivre ou des mesures à prendre. Elle devrait également être lue parallèlement aux lignes directrices 3/2019 du comité européen de la protection des données sur le traitement des données à caractère personnel par des dispositifs vidéo[69], à toute réglementation de l'Union et de l'Espace économique européen, et aux lignes directrices dudit comité relatives à l'utilisation de l'intelligence artificielle.

La présente annexe fournit des lignes directrices fondées sur l'hypothèse que les autorités répressives se muniront de la technologie de reconnaissance faciale (en tant que produits commerciaux). Si l'autorité répressive prévoit de développer la technologie de reconnaissance faciale (ou l'entraîner davantage), des exigences supplémentaires s'appliquent pour sélectionner les ensembles de données d'entraînement, de validation et d'essai nécessaires à utiliser pendant ledit développement, ainsi que les rôles ou les mesures pour l'environnement de développement. De même, un produit commercial peut nécessiter d'autres ajustements pour l'utilisation prévue, auquel cas les exigences susmentionnées pour la sélection des ensembles de données d'essai, de validation et d'entraînement devraient être respectées.

Le fait d'appartenir à la même autorité répressive ne donne pas en soi un accès complet aux données biométriques. Comme pour toute autre catégorie de données à caractère personnel, les données biométriques collectées pour une certaine finalité répressive au titre d'une base juridique spécifique ne peuvent être utilisées sans une base juridique appropriée pour une finalité répressive différente (article 4, paragraphe 2, de la directive (UE) 2016/680 en matière de protection des données dans le domaine répressif). Le développement ou l'entraînement d'un outil de reconnaissance faciale est également considéré comme une finalité différente. Il convient alors d'évaluer le caractère nécessaire et proportionnel du traitement des données biométriques aux fins de mesure des performances ou d'entraînement de la technologie dans l'objectif d'éviter les répercussions des faibles performances sur les personnes concernées, compte tenu de la finalité initiale du traitement.

1. ROLES ET RESPONSABILITES

Lorsqu'une autorité répressive utilise la technologie de reconnaissance faciale pour l'exécution de ses tâches relevant du champ d'application de la directive en matière de protection des données dans le domaine répressif (prévention et détection des infractions pénales, enquêtes et poursuites en la matière, etc., conformément à l'article 3 de ladite directive), elle peut être considérée comme le responsable du traitement pour la technologie de reconnaissance faciale. Toutefois, les autorités répressives sont composées de plusieurs unités ou départements susceptibles d'intervenir dans ce traitement, soit en définissant le processus d'application de la technologie de reconnaissance faciale, soit en l'appliquant dans la pratique. En raison des spécificités de cette technologie, il peut s'avérer

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

nécessaire d'associer différentes unités, soit pour aider à mesurer ses performances, soit pour l'entraîner davantage.

Dans un projet recourant à cette technologie, plusieurs parties prenantes[70] au sein des autorités répressives peuvent devoir participer:

- Équipe de direction – pour approuver le projet après avoir évalué les risques et les avantages potentiels.
- Délégué à la protection des données et/ou service juridique de l'autorité répressive – pour aider à évaluer la licéité de la mise en œuvre d'un certain projet de technologie de reconnaissance faciale; pour aider à réaliser l'AIPD; pour garantir le respect et l'exercice des droits des personnes concernées.
- Propriétaire de processus – pour agir en tant qu'unité spécifique au sein de l'autorité répressive compétente en vue de développer le projet, en décidant des détails du projet de technologie de reconnaissance faciale, y compris les exigences de performance du système; pour décider de la mesure d'équité appropriée; pour fixer le score de confiance[71]; pour déterminer les seuils acceptables de partialité; pour reconnaître les risques potentiels que le projet de technologie de reconnaissance faciale pose pour les droits et libertés des personnes (en consultant également le délégué à la protection des données et le service informatique chargé de l'IA et/ou le service de la science des données (voir ci-dessous) et les présenter à l'équipe de direction. Le propriétaire du processus consultera également le gestionnaire de la base de données de référence, avant de décider des détails du projet de technologie de reconnaissance faciale, afin de comprendre à la fois l'objectif d'utilisation de la base de données de référence, mais aussi ses détails techniques. En cas de réentraînement d'une technologie de reconnaissance acheté, le propriétaire du processus sera également chargé de la sélection de l'ensemble de données d'entraînement. Étant donné qu'il s'agit de l'unité responsable de l'élaboration et des décisions des détails du projet, le propriétaire du processus est chargé de mener l'AIPD.
- Service informatique chargé de l'IA et/ou service de la science des données – pour aider à la réalisation d'une DPIA; pour expliquer les paramètres disponibles permettant de mesurer la performance du système, l'équité[72] et les biais potentiels; pour mettre en œuvre la technologie et les garanties techniques afin d'empêcher l'accès non autorisé aux données collectées, les cyberattaques, etc. En cas de réentraînement d'une technologie de reconnaissance faciale achetée, le service informatique chargé de l'IA ou le service de la science des données entraînera le système, sur la base de l'ensemble de données d'entraînement fourni par le propriétaire du processus. Ce service sera également chargé de mettre en place les mesures visant à atténuer les risques identifiés conjointement par les propriétaires des processus (par exemple, les risques spécifiques à l'IA tels que les attaques par inférence de modèles).

[70] Les rôles suivants sont indicatifs des différentes parties prenantes et de leurs responsabilités dans un projet recourant à la technologie de reconnaissance faciale. Bien que le langage utilisé dans la présente annexe pour décrire les rôles ne soit pas péremptoire, chaque autorité répressive doit définir et attribuer des rôles similaires en fonction de son organisation. Il peut arriver qu'une unité cumule plusieurs rôles, par exemple le propriétaire du processus et le gestionnaire de la base de données de référence, ou le propriétaire du processus et le service informatique chargé de l'IA et/ou le service de la science des données (lorsque l'unité du propriétaire du processus dispose de toutes les connaissances techniques nécessaires).

[71] Le score de confiance est le niveau de confiance de la prédiction (concordance), sous la forme d'une probabilité. Par exemple, si l'on compare deux modèles, il y a 90 % de certitude que ceux-ci appartiennent à la même personne. Le score de confiance est différent de la performance de la technologie de reconnaissance faciale, mais il a une incidence sur la performance. Plus le seuil de confiance est élevé, moins les résultats de la technologie de reconnaissance faciale seront faussement positifs et plus ils seront faussement négatifs.

[72] L'équité peut être définie comme l'absence de discrimination injuste et illégale, telle que les préjugés liés au genre ou à la race.

- Utilisateurs finaux (tels que les agents de police sur le terrain ou les laboratoires de médecine légale) – pour procéder à une comparaison avec la base de données; pour examiner de manière critique les résultats en tenant compte des preuves antérieures et pour fournir un retour d'information au propriétaire du processus en cas de résultats faussement positifs et d'indications d'une éventuelle discrimination.
- Gestionnaire de la base de données de référence – l'unité spécifique au sein de l'autorité répressive compétente chargée de l'accumulation et de la gestion de la base de données de référence, c'est-à-dire la base de données par rapport à laquelle les images seront comparées, y compris la suppression des images faciales après la période de conservation définie. Cette base de données peut être créée spécifiquement pour le projet de technologie de reconnaissance faciale envisagé ou peut préexister, à des fins compatibles. Le gestionnaire de la base de données de référence est chargé de définir le moment et les circonstances de la conservation des images faciales. Il définit également leurs exigences en matière de conservation des données (en fonction du temps ou d'autres critères).

Étant donné que la plupart des cas de déploiement et d'utilisation de la technologie de reconnaissance faciale présentent un risque intrinsèque élevé pour les droits et libertés des personnes concernées, l'autorité de contrôle compétente de protection des données devrait également participer dans le cadre de la consultation préalable requise par l'article 28 de la directive en matière de protection des données dans le domaine répressif.

2. DEBUT: AVANT L'ACQUISITION DU SYSTEME DE TECHNOLOGIE DE RECONNAISSANCE FACIALE

Le propriétaire du processus d'une autorité répressive devrait d'abord avoir une compréhension claire du ou des processus faisant appel à la technologie de reconnaissance faciale (le ou les cas d'utilisation) et s'assurer qu'il existe une base juridique pour fonder le cas d'utilisation prévu. Dans cette optique, il doit:

- décrire formellement le cas d'utilisation. Il convient de décrire le problème à résoudre et la manière dont la technologie de reconnaissance faciale fournira une solution ainsi que la vue d'ensemble du processus (tâche) dans lequel elle sera appliquée. À cet égard, les autorités répressives devraient documenter au moins[73]:
  - les catégories de données à caractère personnel enregistrées dans le processus;
  - les objectifs et les buts concrets pour lesquels cette technologie sera utilisée, y compris les conséquences potentielles pour la personne concernée après une concordance;
  - la manière dont les images faciales seront collectées (y compris des informations sur le contexte de cette collecte, par exemple à la porte de l'aéroport, des vidéos provenant de caméras de sécurité situées en dehors d'un magasin où un crime a été commis, etc., et les catégories de personnes concernées dont les données biométriques seront traitées);
  - la base de données par rapport à laquelle les images seront comparées (base de données de référence), ainsi que des informations sur la manière dont elle a été créée, sa taille et la qualité des données biométriques qu'elle contient;
  - les acteurs des autorités répressives qui seront autorisés à utiliser le système de reconnaissance faciale et à agir sur celui-ci dans le contexte répressif (leurs profils et leurs droits d'accès doivent être définis par le propriétaire du processus);

[73] L'annexe I fournit une liste d'éléments aidant le responsable du traitement à décrire un cas d'utilisation de la technologie de reconnaissance faciale.

- la période de conservation envisagée pour les données d'entrée, ou le moment qui déterminera la fin de cette période (comme la clôture ou la fin de la procédure pénale conformément au droit procédural national pour laquelle elles ont été initialement collectées), ainsi que toute action ultérieure (suppression des données, anonymisation et utilisation à des fins statistiques ou de recherche, etc.);
- la mise en œuvre de la journalisation et l'accessibilité des journaux et des dossiers conservés;
- les mesures de performance (par exemple, l'exactitude, la précision, le rappel, le score F1) et leurs seuils minimaux acceptables[74].
- l'estimation du nombre de personnes qui seront soumises à la technologie de reconnaissance faciale et la période ou l'occasion à laquelle elles le seront.

- réaliser une évaluation de la nécessité et de la proportionnalité[75]. L'existence de cette technologie ne justifie pas forcément son utilisation. Le propriétaire du processus doit d'abord déterminer s'il existe une base juridique appropriée pour le traitement envisagé. Il est nécessaire de consulter à cette fin le délégué à la protection des données et le service juridique. La raison derrière l'utilisation de la technologie de reconnaissance faciale devrait être son caractère nécessaire et proportionné en vue de résoudre un problème spécifiquement défini par les autorités répressives. Elle doit être évaluée en fonction de l'objectif, de la gravité du crime et du nombre de personnes non impliquées mais affectées par le système de la reconnaissance faciale. Aux fins de l'évaluation de la licéité, il convient de tenir compte, à tout le moins: de la directive en matière de protection des données dans le domaine répressif[76], du RGPD[7778], de tout cadre juridique existant en matière d'IA[79] et des lignes directrices connexes fournies par les autorités de contrôle compétentes en matière de protection des données (telles que les lignes directrices 3/2019 du comité européen de la protection des données sur le traitement des données à caractère personnel par des

[74] Il existe différentes mesures pour évaluer la performance d'un système de reconnaissance faciale. Chaque mesure donne une vision différente des résultats du système et sa capacité à fournir une image adéquate de la performance du système de reconnaissance faciale dépend de son cas d'utilisation. Si l'accent est mis sur l'obtention de pourcentages élevés de concordance correcte d'un visage, des mesures telles que la précision et le rappel pourraient être utilisés. Toutefois, elles ne permettent pas d'évaluer la qualité du traitement des exemples négatifs par la technologie de reconnaissance faciale (nombre d'entre eux ayant été erronément mis en correspondance avec le système). Le propriétaire du processus, avec l'aide du service informatique chargé de l'IA et du service de la science des données, devrait être en mesure de définir les exigences de performance et de les exprimer dans la mesure la plus appropriée en fonction du cas d'utilisation de cette technologie.

[75] D'autres mesures permettant de tenir compte de la nécessité peuvent être envisagées en ce qui concerne l'adaptation et l'utilisation du système, de sorte que la description du cas d'utilisation peut également être légèrement modifiée au cours de l'évaluation de la nécessité et de la proportionnalité.

[76] 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.

[77] 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.

[78] Dans les cas où un projet scientifique visant à effectuer des recherches sur l'utilisation de la technologie de reconnaissance faciale devrait traiter des données à caractère personnel, mais que ce traitement ne relèverait pas de l'article 4, paragraphe 3, de la directive en matière de protection des données dans le domaine répressif, le RGPD serait généralement applicable (article 9, paragraphe 2, de ladite directive). Dans le cas de projets pilotes qui seraient suivis d'opérations répressives, la directive resterait applicable.

[79] Par exemple, il existe une proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL ÉTABLISSANT DES RÈGLES HARMONISÉES CONCERNANT L'INTELLIGENCE ARTIFICIELLE (LÉGISLATION SUR L'INTELLIGENCE ARTIFICIELLE) ET MODIFIANT CERTAINS ACTES LÉGISLATIFS DE L'UNION, mais celle-ci n'a pas encore été établie en tant que règlement.

dispositifs vidéo[80]). Ces actes législatifs de l'Union devraient toujours être corroborés par les exigences nationales applicables, en particulier dans le domaine du droit de la procédure pénale. L'évaluation de la proportionnalité devrait déterminer les droits fondamentaux des personnes concernées susceptibles d'être affectées (au-delà du respect de la vie privée et de la protection des données). Elle doit également décrire toute limite (ou l'absence de limites) imposée au système de reconnaissance faciale dans le cas d'utilisation et en tenir compte. Par exemple, si le système fonctionnera en continu ou de manière temporaire et s'il sera limité à une zone géographique.

- réaliser une analyse d'impact relative à la protection des données (AIPD) [81]. Il conviendrait de procéder à une AIPD, étant donné que le déploiement de la technologie de reconnaissance faciale dans le domaine répressif est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes[82]. L'AIPD devrait contenir en particulier: une description générale des opérations de traitement envisagées[83], une évaluation des risques pour les droits et libertés des personnes concernées[84], les mesures envisagées pour faire face à ces risques, les garanties, les mesures de sécurité et les mécanismes permettant d'assurer la protection des données à caractère personnel et de démontrer la conformité avec la législation. L'AIPD est un processus continu, de sorte que tout nouvel élément du traitement devrait être ajouté. De plus, l'évaluation des risques devrait être mise à jour à chaque étape du projet.
- obtenir l'approbation de l'équipe de direction en expliquant les risques pour les droits et libertés des personnes concernées (posés par le cas d'utilisation et la technologie utilisée) et les différents plans de traitement des risques.

3. LORS DE LA PASSATION DE MARCHES ET AVANT LE DEPLOIEMENT DE LA TECHNOLOGIE DE RECONNAISSANCE FACIALE

- Décider des critères de sélection de la technologie de reconnaissance faciale (algorithme). Le propriétaire du processus devrait décider des critères de sélection d'un algorithme avec l'aide du service informatique chargé de l'IA et/ou du service de la science des données. Dans la pratique, ces critères incluraient l'équité et les mesures de performance arrêtées dans la description du cas

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[81] Des orientations supplémentaires sur les AIPD sont disponibles: dans les lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et à la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement 2016/679, WP248 rév. 01, disponible à l'adresse suivante: https://ec.europa.eu/newsroom/article29/items/611236 et la boîte à outils «Responsabilisation sur le terrain» du contrôleur européen de la protection des données, partie II, disponible à l'adresse suivante: https://edps.europa.eu/node/4582_en.

[82] En fonction du cas d'utilisation, la technologie de reconnaissance faciale peut répondre aux critères suivants, entraînant un traitement à haut risque (tirés des lignes directrices concernant l'AIPD, WP248 rév. 01): surveillance systématique, traitement des données à grande échelle, recherche de concordance ou interconnexion d'ensembles de données, utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles.

[83] La description du traitement ainsi que l'évaluation de la nécessité et de la proportionnalité, telles qu'elles ont déjà été décrites dans les étapes précédentes, font également partie de l'AIPD, en plus de l'évaluation des risques. Le cas échéant, une description plus détaillée des flux de données à caractère personnel sera fournie dans ladite analyse.

[84] L'analyse des risques pour les personnes concernées devrait inclure les risques liés à l'emplacement des images de visage à comparer (local/à distance), les risques liés aux processeurs/sous-processeurs, ainsi que les risques spécifiques à l'apprentissage automatique lorsqu'il est appliqué (par exemple, empoisonnement des données, exemples contradictoires).

d'utilisation. Ils devraient également comprendre des informations relatives aux données avec lesquelles l'algorithme a été entraîné. Les ensembles d'entraînement, d'essai et de validation doivent suffisamment contenir des échantillons de toutes les caractéristiques des personnes concernées par la technologie de reconnaissance faciale (par exemple, l'âge, le genre et la race) en vue de réduire les biais. Le fournisseur de la technologie de reconnaissance faciale devrait fournir des informations et des mesures sur les ensembles de données d'entraînement, d'essai et de validation de ladite technologie, et décrire les mesures prises pour évaluer et atténuer les discriminations et les possibles biais illicites. Dans la mesure du possible, le propriétaire de processus doit vérifier s'il existait une base juridique permettant au fournisseur d'utiliser cet ensemble de données aux fins de l'entraînement des algorithmes (sur la base des informations que le fournisseur mettra à disposition). En outre, le propriétaire de processus devrait veiller à ce que le fournisseur de la technologie de reconnaissance faciale applique des normes de sécurité relatives aux données biométriques, telles que la norme ISO/IEC 24745, qui fournit des orientations pour la protection des informations biométriques dans le cadre de diverses exigences en matière de confidentialité, d'intégrité et de possibilité de renouvellement/révocation pendant le stockage et la transmission, ainsi que d'exigences et de lignes directrices pour la gestion et le traitement sécurisés et conformes au respect de la vie privée des informations biométriques.

- Réentraîner l'algorithme (si nécessaire). Le propriétaire du processus devrait veiller à ce que la mise au point du système de reconnaissance faciale pour obtenir une plus grande précision avant son utilisation fasse également partie des services fournis. Si un entraînement supplémentaire au système de reconnaissance faciale acquis est nécessaire pour respecter les mesures de précision, le propriétaire du processus, en plus de prendre la décision d'un nouvel entraînement, doit décider de l'ensemble de données approprié et représentatif à utiliser et vérifier la licéité de cette utilisation pour les données avec l'aide du service informatique chargé de l'IA et/ou du service de la science des données.
- Mettre en place les garanties appropriées pour traiter les risques liés à la sécurité, à la partialité et aux faibles performances. Il s'agit notamment de mettre en œuvre un processus de surveillance de la technologie de reconnaissance faciale une fois qu'elle est utilisée (journalisation et retour d'information pour garantir l'exactitude et l'équité des résultats). Il convient en outre de veiller à ce que les risques spécifiques à certains systèmes d'apprentissage automatique et de systèmes de reconnaissance faciale (par exemple, l'empoisonnement des données, les exemples contradictoires, inversion de modèles, inférence en boîte blanche) soient identifiés, mesurés et atténués. Le propriétaire du processus devrait également mettre en place des garanties appropriées pour garantir le respect des exigences en matière de conservation des données biométriques incluses dans l'ensemble de données de réentraînement.
- Documenter le système de reconnaissance faciale. Cette démarche devrait inclure une description générale du système de reconnaissance faciale, une description détaillée des éléments dudit système et du processus de sa mise en place, des informations détaillées sur le suivi, le fonctionnement et le contrôle du système, ainsi qu'une description détaillée de ses risques et des mesures d'atténuation. Les éléments inclus dans cette documentation comprendront les principaux éléments de la description du système de reconnaissance faciale des étapes précédentes (voir ci-dessus). Ils seront cependant complétés par des informations relatives au suivi des performances et à l'application des changements au système, y compris les mises à jour des versions et/ou l'entraînement.
- Élaborer des manuels d'utilisation expliquant la technologie et les cas d'utilisation. Ils doivent expliquer clairement tous les scénarios et toutes les conditions préalables dans le cadre desquels la technologie de reconnaissance faciale sera utilisée.
- Former les utilisateurs finaux à l'utilisation de la technologie. Ces formations doivent donner des explications sur les capacités et les limites de la technologie afin que les utilisateurs puissent

comprendre les circonstances dans lesquelles il est nécessaire de l'appliquer et les cas dans lesquels elle peut être inexacte. Elles contribueront également à atténuer les risques liés au non-contrôle ou à la critique du résultat de l'algorithme.

- Consulter l'autorité de contrôle compétente en matière de protection des données, conformément à l'article 28, paragraphe 1, point b), de la directive en matière de protection des données dans le domaine répressif. Fournir des informations conformément à l'article 13 de ladite directive afin d'informer les personnes concernées du traitement et de leurs droits. Ces avis doivent s'adresser aux personnes concernées dans un langage approprié afin qu'elles puissent comprendre le traitement. Ils donnent également des explications sur les éléments de base de la technologie, y compris les taux de précision, les ensembles de données d'entraînement et les mesures prises pour éviter la discrimination et la faible précision de l'algorithme.

4. RECOMMANDATIONS APRES LE DEPLOIEMENT DE LA TECHNOLOGIE DE RECONNAISSANCE FACIALE

- Garantir une intervention humaine et le suivi des résultats. Il convient de ne jamais prendre de mesure à l'égard d'une personne sur la seule foi du résultat d'un traitement effectué au moyen d'une technologie de reconnaissance faciale (ce qui impliquerait une violation de l'article 11 de la directive en matière de protection des données dans le domaine répressif; la décision individuelle automatisée ayant des effets juridiques ou d'autres effets similaires sur la personne concernée). Il convient de garantir l'examen des résultats de la technologie de reconnaissance faciale par un agent de l'autorité répressive. Il s'agit également de veiller à ce que les utilisateurs de l'autorité répressive évitent les biais d'automatisation, en examinant les informations contradictoires et en remettant en question de manière critique les résultats de la technologie. À cet effet, la formation continue et la sensibilisation des utilisateurs finaux revêtent une grande importance, mais l'équipe de direction devrait s'assurer que les ressources humaines sont suffisantes pour exercer une surveillance efficace. Cette recommandation implique de laisser suffisamment de temps à chaque agent pour remettre en question de manière critique les résultats de la technologie. Il convient d'enregistrer, de mesurer et d'évaluer dans quelle mesure le contrôle humain modifie la décision initiale de la technologie de reconnaissance faciale.
- Surveiller et traiter la dérive du modèle de la technologie de reconnaissance faciale (dégradation de la performance) une fois que le modèle est en production.
- Établir un processus pour réévaluer les risques et les mesures de sécurité régulièrement et chaque fois que la technologie ou le cas d'utilisation subit des changements.
- Documenter toute modification apportée au système tout au long de son cycle de vie (par exemple, mises à jour, réentraînement).
- Mettre en place un processus ainsi que les capacités techniques connexes pour traiter les demandes d'accès des personnes concernées. La capacité technique d'extraction des données, au cas où il serait nécessaire de les fournir aux personnes concernées, doit être mise en place avant toute demande.
- Veiller à ce que des procédures soient mises en place en cas de violation des données. En cas de violation de données à caractère personnel impliquant des données biométriques, les risques sont susceptibles d'être élevés. Dans ce cas, tous les utilisateurs concernés devraient avoir connaissance des procédures à suivre. Le délégué à la protection des données devrait être immédiatement informé et il en va de même pour les personnes concernées.

ANNEXE III – EXEMPLES CONCRETS

Il existe de nombreux contextes pratiques et finalités différents de l'utilisation de la reconnaissance faciale, par exemple dans des environnements contrôlés tels que le franchissement des frontières, le recoupement des données provenant de bases de données de la police ou à partir de données à caractère personnel manifestement rendues publiques par la personne concernée, des flux de caméras en direct (reconnaissance faciale en direct), etc. Par conséquent, les risques pour la protection des données à caractère personnel et d'autres libertés et droits fondamentaux varient considérablement dans les différents cas d'utilisation. Afin de faciliter l'évaluation de la nécessité et de la proportionnalité, qui devrait précéder la décision sur le possible déploiement de la reconnaissance faciale, les présentes lignes directrices fournissent une liste non exhaustive des applications possibles de la technologie de reconnaissance faciale dans le domaine répressif.

Les scénarios présentés et évalués sont fondés sur des situations **hypothétiques** et visent à illustrer certaines utilisations concrètes de la technologie de reconnaissance faciale et à fournir une assistance pour des considérations au cas par cas, ainsi qu'à établir un cadre global. Ils n'aspirent pas à être exhaustifs et sont sans préjudice de toute procédure en cours ou à venir engagée par une autorité de contrôle nationale en ce qui concerne la conception, l'expérimentation ou la mise en œuvre des technologies de reconnaissance faciale. La présentation de ces scénarios ne devrait servir qu'à illustrer les orientations déjà fournies dans le présent document aux décideurs politiques, aux législateurs et aux autorités répressives lorsqu'ils conçoivent et envisagent la mise en œuvre de technologies de reconnaissance faciale afin de garantir une conformité totale avec l'acquis de l'Union dans le domaine de la protection des données à caractère personnel. Dans ce contexte, il convient de garder à l'esprit que même dans des situations similaires de recours à la technologie de reconnaissance faciale, la présence ou l'absence de certains éléments peut conduire à un résultat différent de l'évaluation de la nécessité et de la proportionnalité.

1 SCENARIO 1

1.1. Description

Un système de contrôle automatisé aux frontières qui permet un passage automatisé aux frontières en authentifiant l'image biométrique stockée dans le document électronique de voyage des citoyens de l'Union européenne et des autres voyageurs passant la frontière et en vérifiant que le passager est le titulaire légitime du document.

Cette vérification ou authentification n'implique qu'une reconnaissance faciale en mode un à un effectuée dans un environnement contrôlé (par exemple, aux postes électroniques de l'aéroport). Les données biométriques du voyageur franchissant le passage frontalier sont saisies lorsqu'il est explicitement invité à regarder la caméra de la porte électronique. Elles sont ensuite comparées à celles du document présenté (passeport, carte d'identité, etc.) qui est délivré conformément à des exigences techniques spécifiques.

Par ailleurs, bien que le traitement dans de tels cas ne relève pas, en principe, du champ d'application de la directive en matière de protection des données dans le domaine répressif, le résultat de la vérification peut également être utilisé pour la recherche de concordance des données (alphanumériques) de la personne avec les bases de données des autorités répressives dans le cadre du contrôle aux frontières. Il peut donc entraîner des actions ayant un effet juridique significatif pour la personne concernée, par exemple l'arrestation à la suite d'une alerte dans le système d'information

Schengen. Dans des circonstances spécifiques, les données biométriques peuvent également être utilisées pour rechercher des concordances dans les bases de données des autorités répressives (dans ce cas, une identification en mode un à plusieurs sera effectuée à cette étape).

Le résultat du traitement de l'image biométrique a une incidence directe sur la personne concernée: ce n'est qu'en cas de vérification réussie qu'il permet de franchir la frontière. En cas d'identification infructueuse, les gardes-frontières doivent procéder à une deuxième vérification pour s'assurer que la personne concernée est différente de celle représentée dans le document d'identification.

Si une alerte du système d'information Schengen ou de l'État membre est donnée, les gardes-frontières doivent procéder à une seconde vérification et aux autres contrôles nécessaires, puis prendre les mesures qui s'imposent, par exemple arrêter la personne ou informer les autorités concernées.

Source d'informations:

- Types de personnes concernées: ☒ toutes les personnes franchissant les frontières
- Source de l'image: ☒ autre (document d'identité)
- Lien avec le crime: ☒ pas nécessaire
- Mode de saisie des informations: ☒ dans une cabine ou un environnement contrôlé
- Contexte – incidence sur d'autres droits fondamentaux: oui, à savoir: ☒ Droit à la libre circulation ☒ Droit d'asile

Base de données de référence (à laquelle les informations enregistrées sont comparées):

- Spécificité: ☒ bases de données spécifiques relatives au contrôle des frontières

Algorithme:

- Type de vérification: ☒ vérification en mode un à un (authentification)

Résultat:

- Incidence: ☒ directe (la personne concernée est autorisée ou refusée à l'entrée)
- Décision automatisée: ☒ oui

1.2. Cadre juridique applicable

Conformément au règlement (CE) nº 2252/2004 du Conseil[85], les passeports et autres documents de voyage délivrés par les États membres doivent contenir depuis 2004 une image biométrique faciale stockée dans une puce électronique intégrée dans le document.

Le code frontières Schengen[86] définit les exigences en matière de vérification des personnes aux frontières extérieures. Pour les citoyens de l'Union et les autres personnes jouissant du droit à la libre circulation en vertu du droit de l'Union, les contrôles minimaux devraient consister en une vérification de leurs documents de voyage, le cas échéant au moyen de dispositifs techniques. Le code frontières Schengen a ensuite été modifié par le règlement (UE) 2017/2225[87], qui a introduit, entre autres, des définitions pour les «portes électroniques», le «système de contrôle automatisé aux frontières» et le

[85] Règlement (CE) nº 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.

[86] RÈGLEMENT (UE) 2016/399 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen).

[87] Règlement (UE) 2017/2225 du Parlement européen et du Conseil du 30 novembre 2017 modifiant le règlement (UE) 2016/399 en ce qui concerne l'utilisation du système d'entrée/de sortie.

«système en libre-service», ainsi que la possibilité de traiter des données biométriques pour effectuer des vérifications aux frontières.

Par conséquent, l'on pourrait supposer qu'il existe une base juridique claire et prévisible autorisant cette forme de traitement de données à caractère personnel. En outre, le cadre juridique est adopté au niveau de l'Union et est directement applicable aux États membres.

1.3. Nécessité et proportionnalité – Finalité/gravité du crime

La vérification de l'identité des citoyens de l'Union dans le cadre d'un contrôle automatisé aux frontières, à l'aide de leur image biométrique, est un élément des vérifications aux frontières extérieures de l'Union. Par conséquent, elle est directement liée à la sécurité des frontières et sert un objectif d'intérêt général reconnu par l'Union. En outre, les barrières de contrôle automatisé aux frontières contribuent à accélérer le traitement des passagers et à réduire le risque d'erreurs humaines. La portée, l'étendue et l'intensité de l'ingérence dans ce scénario sont donc beaucoup plus limitées par rapport à d'autres formes de reconnaissance faciale. Néanmoins, le traitement des données biométriques crée des risques supplémentaires pour les personnes concernées, qui doivent être correctement pris en compte et atténués par l'autorité compétente qui déploie et exploite la technologie de reconnaissance faciale.

1.4. Conclusion

La vérification de l'identité des citoyens de l'Union dans le cadre d'un contrôle automatisé aux frontières est une mesure nécessaire et proportionnée, pour autant que les garanties appropriées soient en place, en particulier l'application des principes de limitation des finalités, de qualité des données, de transparence et de niveau élevé de sécurité.

2 SCENARIO 2

2.1. Description

Un système d'identification des victimes d'enlèvement de mineurs est mis en place par les autorités répressives. Un agent de police autorisé peut procéder à une comparaison des données biométriques d'un enfant soupçonné d'être enlevé avec une base de données de victimes d'enlèvement de mineurs dans des conditions strictes. Cette comparaison est établie dans l'unique but d'identifier les mineurs qui peuvent correspondre à la description de l'enfant disparu pour lequel une enquête a été ouverte et l'alerte a été lancée.

Le traitement en question consisterait à comparer le visage ou l'image d'une personne qui peut correspondre à la description d'un enfant disparu avec les images stockées dans la base de données. Un tel traitement serait effectué dans des cas spécifiques et non de manière systématique.

La base de données concernée par la comparaison est alimentée par des photos d'enfants disparus pour lesquels un soupçon d'enlèvement de mineur ou une menace pour la vie ou l'intégrité physique de l'enfant a été signalé et une enquête pénale a été ouverte sous le contrôle d'une autorité judiciaire, et pour lesquels une alerte d'enlèvement de mineur a été lancée. Les données sont collectées dans le cadre des procédures établies par l'autorité répressive compétente, à savoir les agents de police autorisés à effectuer des missions de police judiciaire. Les catégories de données personnelles enregistrées sont les suivantes:

- l'identité, le surnom, le nom d'emprunt, la filiation, la nationalité, les adresses, les adresses électroniques, les numéros de téléphone;

- la date et le lieu de naissance;
- les informations relatives à la filiation;
- une photographie avec des caractéristiques techniques permettant l'utilisation d'un dispositif de reconnaissance faciale, et d'autres photographies.

Un agent autorisé doit également examiner et vérifier les résultats de la comparaison afin de corroborer les éléments de preuve antérieurs avec lesdits résultats et d'exclure tout résultat faussement positif éventuel.

Les images d'enfants et les données à caractère personnel ne peuvent être conservées que pendant la durée de l'alerte. Elles doivent en outre être effacées immédiatement après la clôture ou l'arrêt de la procédure pénale conformément aux procédures nationales pour lesquelles elles ont été ajoutées dans la base de données.

Si la durée de conservation des données biométriques dans la base de données peut être envisagée pour une durée relativement longue et définie conformément à la législation nationale, l'exercice des droits des personnes concernées, et en particulier le droit de rectification et d'effacement, prévoit une garantie supplémentaire en vue de limiter l'atteinte au droit à la protection des données à caractère personnel des personnes concernées.

Source d'informations:

- Types de personnes concernées: ☒ les enfants
- Source de l'image: ☒ autre: non prédéfinie, victime présumée d'un enlèvement de mineur
- Lien avec le crime: ☒ lien temporel non direct ☒ lien géographique non direct
- Mode de saisie des informations: ☒ dans une cabine ou un environnement contrôlé
- Contexte – incidence sur d'autres droits fondamentaux: ☒ oui, à savoir: ☒ divers

Base de données de référence (à laquelle les informations saisies sont comparées):

- Spécificité: ☒ base de données spécifique

Algorithme:

- Type de vérification: ☒ identification en mode un à plusieurs

Résultat:

- Incidence: ☒ directe
- Décision automatisée: ☒ NON, examen obligatoire par un agent autorisé

Analyse juridique:

- Cadre juridique applicable: ☒ droit national spécifique pour ce traitement (reconnaissance faciale)

2.2. Cadre juridique applicable

Le droit national prévoit un cadre juridique spécifique qui établit la base de données et qui détermine les finalités du traitement ainsi que les critères d'alimentation, d'accès et d'utilisation de la base de données. Les mesures législatives nécessaires à sa mise en œuvre définissent également une période de conservation et font référence aux principes d'intégrité et de confidentialité applicables. Les mesures législatives précisent également les modalités de la fourniture d'informations à la personne concernée et, dans ce cas, à tout titulaire de la responsabilité parentale, ainsi que l'exercice des droits de la personne concernée et, le cas échéant, la limitation éventuelle de celui-ci. Il convient de consulter

l'autorité de contrôle nationale lors de l'élaboration de la proposition de mesure législative correspondante.

2.3. Nécessité et proportionnalité – Finalité/gravité du crime/nombre de personnes non impliquées mais concernées par le traitement

Conditions et garanties applicables au traitement

La comparaison de la reconnaissance faciale ne peut être effectuée que par un agent autorisé en dernier ressort, sauf s'il n'existe pas d'autres moyens moins intrusifs disponibles et lorsque cela est strictement nécessaire, par exemple en cas de doute quant à l'authenticité d'un document d'identité d'un mineur en voyage et/ou après avoir examiné des éléments de preuve antérieurs et des documents rassemblés indiquant une possible correspondance avec la description d'un enfant disparu pour lequel une enquête pénale est menée.

Une garantie supplémentaire est également prévue en ce qui concerne l'examen et la vérification obligatoires de la comparaison de la reconnaissance faciale par un agent autorisé afin de corroborer des éléments de preuve antérieurs avec le résultat de la comparaison et d'exclure tout possible résultat faussement positif.

Objectif poursuivi

La création de la base de données sert des objectifs importants d'intérêt public général, notamment la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, ainsi que la protection des droits et libertés d'autrui. Cette base de données créée et le traitement prévu semblent contribuer à l'identification des enfants victimes d'enlèvement et peuvent donc être considérés comme une mesure propre à soutenir l'objectif légitime d'enquête et de poursuite en la matière.

Finalité et alimentation de la base de données

Les finalités du traitement sont clairement définies par la loi et la base de données n'est utilisée qu'aux fins d'identification des enfants disparus pour lesquels un soupçon d'enlèvement de mineur a été signalé et une enquête pénale a été ouverte sous le contrôle d'une autorité judiciaire et pour lesquels une alerte pour l'enlèvement de mineur a été lancée. Les conditions fixées par la loi pour l'alimentation de la base de données visent à limiter strictement le nombre de personnes concernées et de données à caractère personnel à inclure dans la base de données. Le titulaire de la responsabilité parentale à l'égard de l'enfant doit être informé du traitement effectué et des conditions d'exercice des droits de l'enfant en ce qui concerne le traitement biométrique envisagé à des fins d'identification ou les données à caractère personnel relatives à l'enfant stockées dans la base de données.

2.4. Conclusion

Au vu de la nécessité et de la proportionnalité du traitement envisagé, de l'intérêt supérieur de l'enfant dans la réalisation de ce traitement de données à caractère personnel, et à condition que des garanties suffisantes soient en place pour assurer notamment l'exercice des droits de la personne concernée, notamment en raison du traitement de données concernant des enfants, cette utilisation de traitement par reconnaissance faciale peut être considérée comme probablement compatible avec le droit de l'Union européenne.

En outre, compte tenu du type de traitement et de la technologie utilisée, qui comporte un risque élevé pour les droits et libertés de la personne concernée, le comité européen de la protection des

données estime que l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement envisagé, doit inclure une consultation préalable de l'autorité de contrôle afin de garantir la cohérence et le respect du cadre juridique applicable (voir article 28, paragraphe 2, de la directive en matière de protection des données dans le domaine répressif).

3 SCENARIO 3

3.1. Description

Au cours des interventions policières lors des émeutes et des enquêtes qui s'ensuivent, un certain nombre de personnes ont été identifiées comme suspectes, par exemple à la suite d'enquêtes antérieures utilisant des images de CCTV ou par des témoins. Les photos de ces suspects sont comparées à celles de personnes enregistrées par les systèmes de CCTV ou les appareils mobiles de personnes présentes sur les lieux d'un crime ou dans les environs.

Afin d'obtenir des éléments de preuve plus détaillés sur les personnes soupçonnées d'avoir participé à des émeutes liées à une manifestation, la police crée une base de données constituée d'images présentant un lien local et temporel peu étroit avec les émeutes. La base de données comprend des enregistrements privés téléchargés par des citoyens vers la police, du matériel provenant des caméras CCTV des transports publics, du matériel de vidéosurveillance appartenant à la police et du matériel publié par les médias, sans aucune limitation ou garantie spécifique. L'affichage de comportements criminels graves n'est pas une condition préalable à la collecte des fichiers dans la base de données. Par conséquent, les personnes non impliquées dans les émeutes sont stockées dans la base de données. Ces personnes représentent un pourcentage important de la population locale qui passait par hasard au moment de la manifestation, ou qui a participé à cette dernière mais pas aux émeutes. Il s'agit de milliers de fichiers vidéo et d'images.

À l'aide d'un logiciel de reconnaissance faciale, tous les visages apparaissant dans ces fichiers sont dotés d'identifiants uniques. Les visages de suspects sont ensuite automatiquement comparés à ces identifiants. La base de données constituée de tous les modèles biométriques des milliers de fichiers vidéo et d'images est conservée jusqu'à ce que toutes les enquêtes possibles soient clôturées. Les concordances positives sont traitées par les agents responsables, qui décident ensuite des mesures à prendre. Il peut s'agir notamment d'attribuer le fichier trouvé dans la base de données au dossier pénal de la personne concernée ainsi que d'autres mesures, comme l'interrogatoire ou l'arrestation de cette personne.

Le droit national prévoit une disposition générique selon laquelle le traitement de données biométriques aux fins d'identifier une personne physique de manière unique est admissible si cela est strictement nécessaire et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée.

Source d'informations:

- Types de personnes concernées: ☒ toutes les personnes
- Source d'image: ☒ Espaces accessibles au public ☒ Entité privée ☒ Autres personnes physiques ☒ Autres: médias
- Lien avec le crime: ☒ lien géographique ou temporel pas nécessairement direct
- Mode de saisie de l'information: ☒ à distance
- Contexte – incidence sur d'autres droits fondamentaux: oui, à savoir ☒ la liberté de réunion
- Sources d'information supplémentaires disponibles sur la personne concernée:

☒ autres: non exclu (comme l'utilisation de distributeurs automatiques de billets ou l'entrée dans des magasins), étant donné qu'aucun contrôle ne peut être exercé sur les motifs des images

Base de données de référence (à laquelle les informations saisies sont comparées):

- Spécificité: ☒ bases de données spécifiques liées au domaine de la criminalité

Algorithme:

- Type de traitement: ☒ identification en mode un à plusieurs

Résultat:

- Incidence: ☒ directe (par exemple, la personne concernée peut être arrêtée, interrogée)
- Décision automatisée: ☒ NON
- Durée de conservation: jusqu'à la clôture de toutes les enquêtes possibles

Analyse juridique:

- Type d'informations préalables fournies à la personne concernée: ☒ de manière générale sur le site internet de l'autorité répressive
- Cadre juridique applicable: ☒ Directive en matière de protection des données dans le domaine répressif principalement transposée dans le droit national ☒ Droit national générique pour l'utilisation des données biométriques par les autorités répressives

3.2. Cadre juridique applicable

Comme expliqué ci-dessus, les bases juridiques qui se contentent de reprendre la clause générale de l'article 10 de la directive en matière de protection des données dans le domaine répressif ne sont pas libellées de manière suffisamment claire pour permettre à toutes les personnes physiques de savoir précisément dans quelles circonstances et à quelles conditions les autorités répressives sont habilitées à utiliser les enregistrements de CCTV des espaces publics pour créer un modèle biométrique de leur visage et le comparer, entre autres, aux bases de données de la police, à d'autres enregistrements de CCTV ou enregistrements privés disponibles. Le cadre juridique établi dans ce scénario ne répond donc pas aux exigences minimales requises pour servir de base juridique.

3.3. Nécessité et proportionnalité

Dans cet exemple, le traitement soulève diverses préoccupations au regard des principes de nécessité et de proportionnalité pour plusieurs raisons, citées ci-après.

Les personnes ne sont pas soupçonnées d'un crime grave. L'affichage de comportements criminels graves n'est pas une condition préalable à l'utilisation des fichiers de la base de données contenant le matériel d'image. En outre, un lien temporel et géographique direct avec le crime n'est pas une condition préalable à l'utilisation des fichiers dans la base de données. Il en résulte qu'un pourcentage significatif de la population locale est stocké dans une base de données biométrique pour une durée potentiellement de plusieurs années, jusqu'à ce que toutes les enquêtes soient clôturées.

La base de données sur les scènes de crime ne se limite pas aux images répondant aux exigences de proportionnalité, ce qui conduit à une quantité illimitée d'images à comparer. Le principe de minimisation des données s'en trouve contredit. Une quantité plus réduite d'images permettrait

également d'envisager des moyens non algorithmiques et moins intrusifs, par exemple des agents «super-reconnaisseurs»[88].

L'exemple étant tiré des environs d'une manifestation, il est également probable que les images révèlent les opinions politiques des participants à ladite manifestation, qui constituent la deuxième catégorie spéciale de données susceptibles d'être affectées dans ce scénario. Il est également difficile de savoir comment empêcher la collecte de ces données et avec quelles garanties. En outre, lorsque les personnes concernées apprennent que leur participation à une manifestation a donné lieu à leur inscription dans une base de données biométriques de la police, cela peut avoir des répercussions désastreuses sur l'exercice futur de leur droit de réunion.

Les modèles biométriques figurant dans la base de données peuvent également être comparés les uns avec les autres, ce qui permet à la police de rechercher une personne spécifique dans tous son matériel et de recréer le comportement d'une personne sur une période de plusieurs jours. Elle peut également rassembler des informations supplémentaires sur les personnes, telles que les contacts sociaux et la participation politique.

L'ingérence est encore renforcée par le fait que les données sont traitées à l'insu des personnes concernées.

Sachant que les personnes enregistrent en permanence des photographies et des vidéos et que même la couverture omniprésente de la CCTV peut être analysée de manière biométrique, de graves effets dissuasifs peuvent apparaître.

L'usage intensif de photographies et de vidéos privées, y compris les abus potentiels tels que la dénonciation, est un autre sujet de préoccupation. Étant donné que l'utilisation abusive, y compris la dénonciation, est également un risque inhérent à la procédure pénale en général, le risque est considérablement plus élevé en ce qui concerne l'évolutivité des données traitées et le nombre de personnes impliquées, étant donné que des personnes pourraient également télécharger des éléments relatifs à une personne ou à un groupe de personnes qui leur déplaisent. Les demandes de la police au public de télécharger des photographies et des vidéos pourraient conduire à des seuils très bas en ce qui concerne la fourniture de matériel, d'autant plus qu'il pourrait être possible de le faire de manière anonyme ou, à tout le moins, sans qu'il soit nécessaire de se présenter et de s'identifier dans un poste de police.

3.4. Conclusion

Dans l'exemple, il n'existe aucune disposition spécifique qui pourrait servir de base juridique. Toutefois, même s'il existait une base juridique suffisante, les exigences de nécessité et de proportionnalité ne seraient pas respectées, ce qui entraînerait une atteinte disproportionnée aux droits de la personne concernée en matière de respect de la vie privée et de protection des données à caractère personnel en vertu de la charte.

[88] C'est-à-dire les personnes dotées d'une capacité extraordinaire de reconnaissance faciale. Voir également: «Face Recognition by Metropolitan Police Super-Recognisers» (Les agents super-reconnaisseurs de la police de Londres et leurs capacités de reconnaissance faciale), 26 février 2016, DOI: 10.1371/Journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/ (en anglais).

4 SCENARIO 4

4.1. Description

La police met en œuvre un moyen d'identifier les suspects qui commettent une infraction grave capturée par les caméras CCTV grâce à la technologie de reconnaissance faciale rétrospective. Un agent sélectionne manuellement une ou plusieurs images de suspects dans le matériel vidéo qui a été collecté sur le lieu du crime ou ailleurs dans le cadre d'une enquête préliminaire et envoie ensuite l'image ou les images au service de police technique et scientifique. Celui-ci utilise la technologie de reconnaissance faciale pour faire correspondre ces images à des images de personnes qui ont été précédemment rassemblées dans une base de données par la police (une «base de données de description» composée de suspects et d'anciens condamnés). La base de données de description est pour cette procédure, temporairement et dans un environnement isolé, analysée avec la technologie de reconnaissance faciale afin de pouvoir effectuer le processus de concordance. Pour réduire au minimum l'atteinte aux droits et aux intérêts des personnes appariées, un nombre très limité d'employés du service de police technique et scientifique sont autorisés à mener la procédure de correspondance proprement dite. L'accès aux données est limité aux agents chargés du dossier spécifique et un contrôle manuel des résultats est effectué avant de transmettre tout résultat à l'agent chargé de l'enquête. Les données biométriques ne sont pas transmises en dehors de l'environnement contrôlé et isolé. Seuls le résultat et l'image (et non le modèle biométrique) sont utilisés par la suite dans le cadre de l'enquête. Les employés reçoivent une formation spécifique sur les règles et procédures applicables à ce traitement. De même, tout traitement de données à caractère personnel et biométriques est suffisamment précisé dans le droit national.

Source d'informations:

- Types de personnes concernées: ☒ les suspects identifiés à partir des enregistrements de CCTV
- Source de l'image: ☒ Espaces accessibles au public ☒ Internet
- Lien avec le crime: ☒ Lien temporel direct
  ☒ Lien géographique direct
- Mode de saisie de l'information: ☒ à distance
- Contexte – incidence sur d'autres droits fondamentaux: oui, à savoir: ☒ Liberté de réunion ☒ Liberté d'expression ☒ Divers: __

Base de données de référence (à laquelle les informations saisies sont comparées):

- Spécificité: ☒ bases de données spécifiques liées au domaine de la criminalité

Algorithme:

- Type de traitement: ☒ identification en mode un à plusieurs

Résultat:

- Incidence: ☒ directe (par exemple, la personne concernée est arrêtée, interrogée)
- Décision automatisée: ☒ NON

Analyse juridique:

- Cadre juridique applicable: ☒ Droit national spécifique pour ce traitement (reconnaissance faciale) pour cette autorité compétente

4.2. Cadre juridique applicable

Dans ce scénario, il est précisé dans le droit national que les données biométriques peuvent être utilisées pour effectuer des analyses médico-légales lorsque cela est strictement nécessaire pour atteindre l'objectif d'identification des suspects qui commettent une infraction grave grâce à la recherche de concordance des images figurant dans la base de données de description. Le droit national précise quelles données peuvent être traitées, ainsi que les procédures visant à préserver l'intégrité et la confidentialité des données à caractère personnel et les procédures de leur destruction, offrant ainsi des garanties suffisantes contre les risques d'abus et d'arbitraire.

4.3. Nécessité et proportionnalité

Pour la police technique et scientifique, l'utilisation de la reconnaissance faciale est clairement plus efficace en termes de temps que la recherche de concordance manuelle. La sélection manuelle des images au préalable limite les ingérences par rapport à la comparaison de l'ensemble du matériel vidéo avec une base de données, ce qui permet de différencier et de cibler uniquement les personnes concernées par l'objectif, à savoir la lutte contre les infractions graves. Il reste toutefois important d'examiner si la recherche de concordance peut être effectuée manuellement dans un délai raisonnable, en fonction du cas d'espèce. La limitation des personnes ayant accès à la technologie et aux données à caractère personnel réduit l'incidence sur les droits au respect de la vie privée et à la protection des données, ainsi que sur les modèles biométriques qui ne sont pas stockés ou utilisés ultérieurement dans le cadre de l'enquête. Le contrôle manuel du résultat se traduit également par une réduction du risque de résultats faussement positifs.

4.4. Conclusion

Il est important que la législation nationale fournisse une base juridique adéquate pour le traitement des données biométriques ainsi que pour la base de données nationale avec laquelle la recherche de concordance est effectuée. Dans ce scénario, plusieurs mesures ont été mises en place afin de limiter l'atteinte aux droits relatifs à la protection des données, telles que les conditions d'utilisation de la technologie de reconnaissance faciale spécifiées dans la base juridique, le nombre de personnes ayant accès à la technologie et aux données biométriques, les contrôles manuels, etc. Cette technologie améliore considérablement l'efficacité des travaux d'enquête de la police technique et scientifique. Elle est en outre fondée sur la loi, ce qui permet à la police de traiter les données biométriques lorsque cela est absolument nécessaire et, par conséquent,dans ces limites, elle peut être considérée comme une ingérence licite dans les droits de la personne.

5 SCENARIO 5

5.1. Description

Une identification biométrique à distance consiste à établir l'identité des personnes à l'aide des éléments d'identification biométriques (image faciale, démarche, iris, etc.) à distance, dans un espace public et de manière continue en les comparant aux données (biométriques) stockées dans une base de données[89]. L'identification biométrique à distance est effectuée en temps réel, si la capture du matériel d'image, la comparaison et l'identification se déroulent sans délai significatif.

Avant chaque déploiement de l'identification biométrique à distance en temps réel, la police établit une liste de surveillance des sujets d'intérêt dans le cadre d'une enquête. Cette liste est alimentée par des images faciales des personnes concernées. Sur la base de renseignements suggérant que les

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

personnes se trouveront dans une zone spécifique, telle qu'un centre commercial ou une place publique, la police décide du moment, du lieu et de la durée du déploiement de l'identification biométrique à distance.

Le jour de l'action, elle se rend sur le terrain pour placer un fourgon de police qui sert de centre de contrôle, avec un officier supérieur de la police à bord. Le fourgon contient des moniteurs affichant des images provenant de caméras CCTV situées à proximité, soit installées de manière ponctuelle, soit connectées aux flux de données vidéo de caméras déjà installées. Lorsque les piétons passent devant les caméras, la technologie isole les images de visage, les convertit en un modèle biométrique et les compare aux modèles biométriques des personnes figurant sur la liste de surveillance.

Si une concordance potentielle entre la liste de surveillance et les personnes passant devant les caméras est détectée, une alerte est envoyée aux agents dans le fourgon. Ces derniers informent ensuite les agents sur le terrain si l'alerte est positive, par exemple à l'aide d'un dispositif radio. L'agent sur le terrain décidera alors s'il y a lieu d'intervenir, d'approcher ou, en fin de compte, d'appréhender la personne. Les mesures prises par l'agent sur le terrain sont enregistrées. Dans le cas d'un contrôle discret, les informations recueillies (telles que l'identité de la personne, ses vêtements et l'endroit où elle se dirige) sont stockées.

Le droit national auquel il est fait référence prévoit une disposition générique selon laquelle le traitement des données biométriques aux fins d'identifier une personne physique de manière unique est admissible si cela est strictement nécessaire et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée.

Source d'informations:

- Types de personnes concernées: ☒ toutes les personnes
- Source de l'image: ☒ espaces accessibles au public
- Lien avec le crime: ☒ lien géographique ou temporel pas nécessairement direct
- Mode de saisie de l'information: ☒ à distance
- Contexte – incidence sur d'autres droits fondamentaux: oui, à savoir: ☒ Liberté de réunion ☒ Liberté d'expression ☒ Divers
- Sources d'information supplémentaires disponibles sur la personne concernée: ☒ autres: non exclu (comme l'utilisation de distributeurs automatiques de billets ou l'entrée dans des magasins)

Base de données de référence (à laquelle les informations saisies sont comparées):

- Spécificité: ☒ bases de données spécifiques liées au domaine de la criminalité

Algorithme:

- Type de traitement: ☒ identification en mode un à plusieurs

Résultat:

- Incidence: ☒ directe (par exemple, la personne concernée est arrêtée, interrogée)
- Décision automatisée: ☒ NON
- Durée de conservation: jusqu'à la clôture de toutes les enquêtes possibles

Analyse juridique:

- Type d'informations préalables fournies à la personne concernée: ☒ de manière générale sur le site internet de l'autorité répressive

- Cadre juridique applicable: ☒ Directive en matière de protection des données dans le domaine répressif principalement transposée dans le droit national ☒ Droit national générique pour l'utilisation des données biométriques par les autorités répressives

5.2. Cadre juridique applicable

Les bases juridiques qui reprennent simplement la clause générale de l'article 10 de la directive en matière de protection des données dans le domaine répressif ne sont pas libellées de manière suffisamment claire pour permettre à toutes les personnes physiques de savoir précisément dans quelles circonstances et à quelles conditions les autorités répressives sont habilitées à utiliser les enregistrements de CCTV des espaces publics pour créer un modèle biométrique de leur visage et le comparer aux bases de données de la police. Le cadre juridique établi dans ce scénario ne répond donc pas aux exigences minimales requises pour servir de base juridique[90].

5.3. Nécessité et proportionnalité

La condition de nécessité et de proportionnalité est d'autant plus importante que l'ingérence est profonde. L'identification biométrique à distance dans les espaces publics a plusieurs conséquences sur les droits fondamentaux:

Les scénarios entraînent la surveillance de tous les passants dans l'espace public concerné. Par conséquent, elle affecte gravement l'attente raisonnable des populations d'être anonymes dans les espaces publics[91]. Il s'agit d'une condition préalable à de nombreuses facettes du processus démocratique, telles que la décision de rejoindre une association civique, de participer à des rassemblements et de rencontrer des personnes de toutes origines sociales et culturelles, de participer à une manifestation politique et de visiter des lieux de toute nature. La notion d'anonymat dans les espaces publics est essentielle pour rassembler et échanger librement des informations et des idées. Elle permet de préserver la pluralité des opinions, la liberté de réunion pacifique et la liberté d'association ainsi que la protection des minorités et de soutenir les principes de la division des pouvoirs et de l'équilibre des pouvoirs. Remettre en cause la notion d'anonymat dans les espaces publics peut avoir un effet dissuasif important sur les citoyens. Ils pourraient s'abstenir de certains comportements qui sont tout à fait dans les attributions d'une société libre et ouverte, ce qui porterait atteinte à l'intérêt public, étant donné qu'une société démocratique requiert l'autodétermination et la participation de ses citoyens au processus démocratique.

Le recours à cette technologie signifie que le simple fait de marcher dans la rue, de prendre le métro ou de se rendre à la boulangerie dans la zone concernée entraînera la collecte de données personnelles, y compris biométriques, par les autorités répressives et, dans le premier scénario, la recherche de concordance avec les bases de données de la police. Il serait manifestement disproportionné de procéder de la même manière en ce qui concerne l'enregistrement des empreintes digitales.

[90] Dans les cas où un projet scientifique visant à effectuer des recherches sur l'utilisation de la technologie de reconnaissance faciale devrait traiter des données à caractère personnel, mais que ce traitement ne relèverait pas de l'article 4, paragraphe 3, de la directive en matière de protection des données dans le domaine répressif ou ne relèverait pas du champ d'application du droit de l'Union, le RGPD serait applicable. Dans le cas de projets pilotes qui seraient suivis d'opérations répressives, la directive resterait applicable.

[91] Réponse du comité européen de la protection des données aux députés européens concernant l'application de reconnaissance faciale développée par Clearview AI, 10 juin 2020, Réf.: OUT2020-0052.

Le nombre de personnes concernées est extrêmement élevé, puisque toutes les personnes qui passent au sein de l'espace public en question sont concernées. En outre, les scénarios supposeraient un traitement massif automatisé des données biométriques, ainsi qu'une recherche de concordance massive des données biométriques avec les bases de données de la police.

Dans l'ensemble de la jurisprudence européenne, la surveillance de masse est interdite (par exemple, dans l'affaire S. et Marper c. Royaume-Uni, la Cour européenne des droits de l'homme a estimé que la conservation indifférenciée des données biométriques était une «atteinte disproportionnée» au droit à la vie privée, étant donné qu'elle ne peut pas être considérée comme «nécessaire dans une société démocratique»).

L'identification biométrique à distance est tellement susceptible de donner lieu à une surveillance de masse qu'il n'existe aucun moyen fiable de la limiter. Elle est fondamentalement différente de la vidéosurveillance en tant que telle. En effet, l'utilisation possible de séquences vidéo sans identification biométrique constitue déjà une ingérence forte, mais en même temps limitée, alors que si la technologie de reconnaissance faciale est utilisée, le système de vidéosurveillance déjà largement répandu en tant que principale source de données subira un changement de qualité. En outre, notamment en ce qui concerne les effets dissuasifs implicites, les restrictions éventuelles dans l'application des installations de vidéosurveillance déjà existantes ne seront pas visibles et ne susciteront donc pas la confiance du public.

L'identification biométrique à distance par les autorités de police fait que tout le monde est traité comme un suspect potentiel. Dans un état de droit, cependant, les citoyens sont présumés vertueux jusqu'à ce que leur mauvaise conduite soit prouvée. Ce principe est également partiellement reflété dans la directive en matière de protection des données dans le domaine répressif, qui souligne la nécessité d'établir une distinction, dans la mesure du possible, entre le traitement des personnes condamnées ou soupçonnées d'activités criminelles, pour lesquelles les autorités répressives doivent avoir «des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale» (article 6, point a) de la directive) et celui des personnes qui ne sont pas condamnées ou soupçonnées d'activités criminelles.

Appliquée aux points nodaux des transports ou aux espaces publics, l'utilisation par les autorités répressives d'une technologie capable d'identifier une personne de manière unique, de suivre et d'analyser ses déplacements et ses mouvements révélera ses informations les plus sensibles (même les préférences sexuelles, la religion, les problèmes de santé). Il en résulte un risque énorme d'accès et d'utilisation illicites des données.

La mise en place d'un système qui permet de découvrir le cœur même du comportement et des caractéristiques d'une personne a des effets dissuasifs importants. Elle pousse les gens à se demander s'ils doivent se joindre à telle ou telle manifestation, ce qui porte préjudice au processus démocratique. De même, il pourrait être considéré comme dangereux de fréquenter et d'être vu en public avec un ami connu pour ses démêlés avec la police ou pour son comportement particulier, étant donné que cela attirerait l'attention de l'algorithme du système et, donc, des forces de l'ordre.

Il est impossible de protéger les personnes concernées vulnérables, telles que les enfants. En outre, les personnes qui ont un intérêt professionnel, et souvent une obligation légale correspondante, à préserver la confidentialité de leurs contacts, tels que les journalistes, les avocats et le clergé, sont concernées. Cette situation pourrait, par exemple, conduire à la révélation de la source et du journaliste, ou au fait qu'une personne consulte un avocat de défense pénale. Le problème ne concerne pas seulement les lieux public dans lesquels les journalistes et leurs sources, par exemple, se

rencontrent, mais également, les espaces publics à traverser pour approcher et accéder aux institutions ou aux professionnels à cet égard.

En outre, le sentiment d'inconfort des personnes face à la technologie de reconnaissance faciale peut les amener à modifier leur comportement, à éviter les endroits ayant mis en place cette technologie et à se retirer ainsi de la vie sociale et des événements culturels. En fonction de l'ampleur du déploiement de cette technologie, l'incidence sur les personnes peut être si importante qu'elle affecte leur capacité à vivre dans la dignité[92].

Par conséquent, il existe une forte probabilité d'affecter l'essence, à savoir le noyau intouchable, du droit à la protection des données à caractère personnel. Des indications solides (voir la section 3.1.3.2 des présentes lignes directrices) sont notamment les suivantes: à grande échelle, les caractéristiques biologiques uniques des personnes sont automatiquement traitées par les autorités répressives au moyen d'algorithmes fondés sur la plausibilité et dont les résultats ne peuvent être expliqués que de manière limitée. Les limitations aux droits au respect de la vie privée et à la protection des données sont imposées indépendamment du comportement de la personne ou des circonstances la concernant. Statistiquement, la quasi-totalité des personnes concernées par cette atteinte sont des personnes respectueuses de la loi. Les possibilités de fournir des informations à la personne concernée sont limitées. Dans la plupart des cas, un recours juridictionnel ne sera possible qu'ultérieurement.

Le recours à un système fondé sur la plausibilité et dont les résultats ne peuvent être expliqués que de manière limitée peut conduire à une dispersion de la responsabilité et à un manque dans le domaine des recours, et peut constituer une incitation à la négligence.

Une fois que ce système, qui peut également être appliqué aux caméras de CCTV existantes, est mis en œuvre, et ce, avec très peu d'efforts et sans être visible pour les personnes, il peut être utilisé à mauvais escient et permettre de dresser systématiquement et rapidement des listes de personnes en fonction de leur origine ethnique, de leur genre, de leur religion, etc. Le principe du traitement des données à caractère personnel sur la base de critères prédéterminés, tels que le lieu où se trouve une personne et l'itinéraire qu'elle a emprunté, est déjà appliqué[93] et est susceptible de donner lieu à des discriminations.

En raison de la sensibilité, de l'expressivité et de la quantité de données traitées, les systèmes de reconnaissance faciale à distance installés dans les lieux accessibles au public sont susceptibles d'être utilisés à mauvais escient, avec des conséquences néfastes pour les personnes concernées. Ces données peuvent également être facilement collectées et utilisées à des fins abusives pour exercer une pression sur les acteurs clés en ce qui concerne le principe de l'équilibre des pouvoirs, comme l'opposition politique, les fonctionnaires et les journalistes.

Enfin, les systèmes de reconnaissance faciale ont tendance à ajouter une grande partialité en ce qui concerne la race et le genre: les résultats faussement positifs affectent de manière disproportionnée

---

92 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, page 20.

93 Voir l'article 6 de la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, et l'article 33 du règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 1077/2011, (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226.

les personnes de couleur et les femmes[94],ce qui entraîne une discrimination. Les mesures prises par la police à la suite d'un résultat faussement positif, telles que les perquisitions et les arrestations, stigmatisent encore davantage ces groupes.

5.4. Conclusion

Les scénarios susmentionnés concernant le traitement de données biométriques à distance dans des espaces publics à des fins d'identification ne permettent pas de trouver un juste équilibre entre les intérêts privés et publics concurrents, ce qui constitue une atteinte disproportionnée aux droits de la personne concernée au titre des articles 7 et 8 de la charte.

6 SCENARIO 6

6.1. Description

Une entité privée conçoit une application qui consiste à extraire des images faciales de l'internet pour créer une base de données. L'utilisateur, par exemple la police, peut ensuite télécharger une image. L'application tentera alors, avec l'identification biométrique, de la faire concorder avec les images faciales ou les modèles biométriques dans sa base de données.

Un service de police local mène une enquête sur un délit filmé en vidéo pour lequel un certain nombre de témoins et de suspects potentiels ne peuvent être identifiés en comparant les informations collectées avec des bases de données internes ou des renseignements. Selon les informations collectées, les personnes concernées ne sont enregistrées dans aucune base de données policière existante. La police décide d'utiliser un outil tel que décrit ci-dessus, qui est fourni par une entreprise privée, pour identifier les personnes grâce à l'identification biométrique.

Source d'informations:

- Types de personnes concernées: ☒ tous les citoyens (témoins) ☒ les condamnés ☒ les suspects
- Source de l'image: ☒ séquence vidéo provenant d'un lieu public ou recueillie ailleurs dans le cadre d'une enquête préliminaire
- Lien avec le crime: ☒ pas nécessaire
- Mode de saisie de l'information: ☒ à distance
- Contexte – incidence sur d'autres droits fondamentaux: oui, à savoir: ☒ liberté de réunion ☒ liberté d'expression ☒ divers: __

Base de données de référence (à laquelle les informations saisies sont comparées):

- Spécificité: ☒ bases de données générales alimentées à partir de l'internet

Algorithme:

- Type de traitement: ☒ identification en mode un à plusieurs

Résultat:

- Incidence: ☒ directe (par exemple, la personne concernée est arrêtée ou interrogée, comportement discriminatoire)
- Décision automatisée: ☒ NON

Analyse juridique:

[94] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

- Type d'information préalable de la personne concernée: ☒ non

6.2. Cadre juridique applicable

Lorsqu'une entité privée offre un service qui comprend un traitement de données à caractère personnel dont elle détermine la finalité et les moyens (dans le cas présent, l'extraction d'images à partir de l'internet pour créer une base de données), elle doit disposer d'une base juridique pour ledit traitement. En outre, l'autorité répressive qui décide d'utiliser ce service à ses fins doit disposer d'une base juridique pour le traitement dont elle détermine les finalités et les moyens. Pour que l'autorité répressive soit en mesure de traiter des données biométriques, il doit exister un cadre juridique précisant l'objectif, les données à caractère personnel à traiter, les finalités du traitement et les procédures visant à préserver l'intégrité et la confidentialité des données à caractère personnel, ainsi que les procédures à suivre pour leur destruction.

Ce scénario suppose une collecte massive de données à caractère personnel de personnes qui ne sont pas au courant de ladite collecte. Un tel traitement ne pourrait être licite que dans des circonstances très exceptionnelles. En fonction de l'emplacement de la base de données, l'utilisation de ce service peut entraîner le transfert de données à caractère personnel et/ou de catégories particulières de données à caractère personnel en dehors de l'Union européenne (par la police, par exemple en «envoyant» l'image faciale de la vidéo de surveillance ou collectée d'une autre manière). Ce transfert nécessiterait des conditions spécifiques, voir l'article 39 de la directive en matière de protection des données dans le domaine répressif.

Dans ce scénario, il n'existe pas de règles spécifiques autorisant ce traitement par les autorités répressives.

6.3. Nécessité et proportionnalité

L'utilisation du service par les autorités répressives signifie que les données à caractère personnel sont partagées avec une entité privée qui se sert d'une base de données dans laquelle les données à caractère personnel sont collectées de manière illimitée et à grande échelle. Aucun lien n'existe entre les données personnelles collectées et l'objectif poursuivi par les autorités répressives. Le partage de données par l'autorité répressive à l'entité privée implique également un manque de contrôle de l'autorité sur les données traitées par l'entité privée et une grande difficulté pour les personnes concernées d'exercer leurs droits, étant donné qu'elles n'auront pas connaissance du fait que leurs données sont traitées de cette manière. Les conditions à remplir pour qu'un tel traitement puisse avoir lieu sont très strictes. Il est douteux qu'un objectif quelconque puisse satisfaire aux exigences de la directive, étant donné que les dérogations et les limitations aux droits à la vie privée et à la protection des données ne sont applicables qu'en cas de stricte nécessité. L'intérêt général de l'efficacité dans la lutte contre les crimes graves ne peut en soi justifier un traitement lorsque des quantités aussi importantes de données sont collectées de manière arbitraire. Ce traitement ne satisferait donc pas aux exigences de nécessité et de proportionnalité.

6.4. Conclusion

L'absence de règles claires, précises et prévisibles répondant aux exigences des articles 4 et 10 de la directive en matière de protection des données dans le domaine répressif, et l'absence d'éléments prouvant que ce traitement est strictement nécessaire pour atteindre les objectifs visés, permettent de conclure que l'utilisation de cette application ne satisferait pas aux exigences de nécessité et de proportionnalité et constituerait une atteinte disproportionnée aux droits des personnes concernées

au respect de leur vie privée et à la protection de leurs données à caractère personnel en vertu de la charte.