Parlement européen

Réglementation de la reconnaissance faciale au sein de l'Union européenne

ANALYSE APPROFONDIE

EPRS | Service de recherche du Parlement européen

Auteurs: Tambiama Madiega et Hendrik Mildebrath
Service de recherche pour les députés
PE 698.021 — septembre 2021

FR

L'intelligence artificielle a favorisé l'utilisation des technologies biométriques, notamment les applications de reconnaissance faciale, qui sont de plus en plus employées à des fins de vérification, d'identification et de catégorisation. Ce document: 1) offre un aperçu des technologies, de l'aspect économique et des différentes utilisations des technologies de reconnaissance faciale; 2) met en lumière les préoccupations résultant des caractéristiques spécifiques des technologies et de leurs éventuelles répercussions sur les droits fondamentaux des personnes; 3) dresse le bilan du cadre juridique, et notamment des règles en matière de protection des données et de non-discrimination actuellement applicables à la reconnaissance faciale au sein de l'Union européenne; et 4) examine la récente proposition de loi de l'Union sur l'intelligence artificielle, réglementant les technologies de reconnaissance faciale. Enfin, 5) le présent document se penche brièvement sur les approches adoptées en dehors de l'Union et à l'échelle internationale en ce qui concerne la réglementation de la reconnaissance faciale.

AUTEURS

Tambiama Madiega et Hendrik Mildebrath, service de recherche pour les députés, EPRS (avec le soutien à la recherche de Fabiana Fracanzino).

Le présent document a été rédigé par le service de recherche pour les députés, au sein de la direction générale des services de recherche parlementaire (EPRS) du secrétariat général du Parlement européen.

Pour contacter les auteurs, veuillez envoyer un courriel à l'adresse suivante: eprs@ep.europa.eu

VERSIONS LINGUISTIQUES

Original: EN

Traductions: DE, FR

Manuscrit achevé en septembre 2021.

PE 698.021
ISBN: 978-92-846-8501-1
DOI:10.2861/788795
QA-01-21-197-FR-N

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
https://www.europarl.europa.eu/thinktank/fr/home.html (internet)
http://epthinktank.eu (blog)

Résumé

L'intelligence artificielle (IA) favorise l'utilisation des technologies biométriques, notamment les applications de reconnaissance faciale, qui sont employées à des fins de vérification, d'identification et de catégorisation par des acteurs privés et publics. Bien que les marchés de la reconnaissance faciale soient appelés à connaître une expansion considérable dans les années à venir, l'utilisation croissante des technologies de reconnaissance faciale (TRF) est devenue un sujet important du débat public mondial sur la surveillance biométrique.

S'il existe de réels avantages à utiliser des systèmes de reconnaissance faciale pour la sûreté et la sécurité publiques, leur généralisation et leur caractère intrusif ainsi que leur propension à l'erreur suscitent un certain nombre d'inquiétudes liées aux droits fondamentaux eu égard, par exemple, à la discrimination contre certains groupes de la population et aux violations du droit en matière de protection des données et de respect de la vie privée. Pour pallier ces effets, l'Union a déjà mis en place des règles strictes au titre de la charte des droits fondamentaux, du règlement général sur la protection des données, de la directive en matière de protection des données dans le domaine répressif et du cadre de l'Union en matière de non-discrimination, qui s'appliquent également aux processus et activités liés aux TRF. Cependant, divers acteurs remettent en question l'efficacité du cadre actuel de l'Union à répondre de manière appropriée aux inquiétudes que suscitent les TRF eu égard aux droits fondamentaux. Même si les tribunaux tentaient de combler les lacunes en matière de protection par une interprétation large du cadre juridique préexistant, des incertitudes et complexités juridiques persisteraient.

Dans ce contexte, le projet de législation de l'Union sur l'IA, dévoilé en avril 2021, vise à limiter l'utilisation des systèmes d'identification biométrique, notamment de reconnaissance faciale, qui pourraient aboutir à une surveillance omniprésente. Outre la législation applicable existante (par exemple, en matière de protection des données et de non-discrimination), le projet de législation sur l'IA propose d'introduire de nouvelles règles régissant l'utilisation des TRF au sein de l'Union et de les différencier selon que leurs caractéristiques d'utilisation présentent un «risque élevé» ou un «risque faible». Un grand nombre de TRF seraient considérées comme des systèmes «à haut risque» qui seraient interdits ou devraient se conformer à des exigences strictes. L'utilisation à des fins répressives de systèmes de reconnaissance faciale en temps réel dans des espaces accessibles au public serait interdite, à moins que les États membres choisissent de l'autoriser pour des motifs importants de sécurité publique, et que les autorisations judiciaires ou administratives appropriées soient délivrées. Un large éventail de technologies de reconnaissance faciale utilisées à d'autres fins que les activités répressives (par exemple, contrôle aux frontières, places de marché, transport public et même établissements scolaires) pourraient être autorisées sous réserve d'une évaluation de conformité et du respect de certaines exigences de sécurité avant d'être mises sur le marché de l'Union. À l'inverse, les systèmes de reconnaissance faciale utilisés à des fins de catégorisation seraient considérés comme des systèmes «à risque faible» et seraient soumis uniquement à des exigences limitées en matière de transparence et d'information. Si les acteurs, les chercheurs et les organismes de réglementation semblent convenir qu'une réglementation s'impose, certains opposants remettent en question la distinction proposée entre les systèmes biométriques à haut risque et ceux à faible risque, et signalent que la législation proposée donnerait lieu à un système de normalisation et d'autoréglementation sans contrôle public approprié. Ils demandent des modifications du projet de texte, notamment en ce qui concerne la liberté d'action des États membres dans la mise en œuvre des nouvelles règles. Certains se prononcent résolument en faveur de règles plus strictes — y compris d'une interdiction pure et simple de ces technologies.

Au-delà de l'Union, on observe une augmentation mondiale de l'utilisation des technologies de reconnaissance faciale, tandis que les préoccupations quant à la surveillance des États grandissent et sont exacerbées par le fait qu'à ce jour, les règles juridiquement contraignantes applicables aux TRF sont très limitées, et ce même au sein de territoires importants comme les États-Unis d'Amérique et la Chine. Les décideurs politiques et les législateurs du monde entier ont la possibilité de discuter — dans un contexte multilatéral, voire bilatéral — de la manière de mettre en place des contrôles appropriés en ce qui concerne l'utilisation des systèmes de reconnaissance faciale.

Table des matières

1. Contexte

1.1. Technologies

1.1.1. Terminologie

1.1.1.1. Biométrie

Les technologies biométriques sont utilisées pour déterminer, vérifier ou confirmer l'identité d'une personne sur la base de ses caractéristiques morpho-physiologiques (apparence extérieure) ou comportementales (manière d'agir)[1]. Les **caractéristiques morpho-physiologiques** sont évaluées au moyen d'identificateurs morphologiques [qui se composent principalement des empreintes digitales, de la forme de la main, du doigt, du réseau veineux, de l'œil (iris et rétine), et de la forme du visage] et d'analyses biologiques (ADN, sang, salive ou urine). Les **caractéristiques comportementales** sont communément évaluées en utilisant la reconnaissance vocale, la dynamique de la signature (vitesse du mouvement du stylo, accélérations, pression exercée, inclinaison), la démarche (c'est-à-dire la façon de marcher de la personne) ou la gestuelle[2].

La biométrie permet d'identifier une personne de manière authentifiée sur la base de données uniques et spécifiques vérifiables. L'**identification biométrique** consiste à déterminer l'identité d'une personne en enregistrant un élément de ses données biométriques (par exemple, une photographie) et en le comparant aux données biométriques de plusieurs autres personnes conservées dans une base de données, de manière à obtenir une réponse à la question «Qui êtes-vous?». L'**authentification biométrique** compare les données relatives aux caractéristiques d'une personne à ses données biométriques afin de déterminer une ressemblance et de répondre à la question «Êtes-vous M. ou M^{me} X?»[3]. Les **technologies biométriques** comprennent la «reconnaissance des empreintes digitales», la «reconnaissance de la signature», la «correspondance ADN», la «reconnaissance des yeux/de l'iris», la «reconnaissance des yeux/de la rétine», l'«identification vocale/du locuteur» la «démarche», la «reconnaissance géométrique de la main» ou la «reconnaissance faciale»[4].

1.1.1.2. Reconnaissance faciale

Les **technologies de reconnaissance faciale (TRF)** sont un type spécifique de technologies biométriques qui se rapportent à une multitude de technologies utilisées à différentes fins, allant de la simple **détection** de présence d'un visage dans une image, à la vérification, l'identification et la catégorisation ou la classification plus complexes de personnes[5]. La **vérification** (comparaison d'un élément par rapport à un autre) permet la comparaison de deux modèles biométriques, généralement supposés appartenir à la même personne. L'**identification** (comparaison d'un élément par rapport à plusieurs autres) signifie que le modèle de l'image faciale d'une personne est comparé à d'autres modèles conservés dans une base de données afin de découvrir si l'image de cette personne y est conservée. Les TRF sont également utilisées pour effectuer une **catégorisation**

---

1 Voir Kak, A. (2020), *Regulating Biometrics: Global Approaches and Urgent Questions*, p. 6.

2 Voir Thales (2021), *Biometrics: definition, use cases and latest news*.

3 Ibid.

4 Voir Biometrics Institute (2021), *Types of Biometrics*.

5 Voir Buolamwini, J., Ordóñez, V., Morgenstern, J., et Learned-Miller, E. (2020), *Facial Recognition Technologies: A Primer*, Algorithmic Justice League, p. 2-6. Voir également: Agence des droits fondamentaux de l'Union européenne (2020), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, p. 7-8.

(ou une classification) d'individus, selon leurs caractéristiques personnelles. À cet égard, un large éventail de logiciels ont été mis au point pour évaluer les attributs d'une personne à partir de son visage, à des fins de «**classification selon les attributs faciaux**» (par exemple, le sexe, la race ou l'ethnie) ou d'«**estimation selon les attributs faciaux**» (par exemple, l'âge). En outre, les TRF peuvent être utilisées pour **classer les expressions faciales** (comme un sourire) ou l'état émotionnel d'un individu (comme «content», «triste» ou «en colère»)[6].

1.1.2. Technologies de reconnaissance faciale et d'intelligence artificielle

Les technologies de reconnaissance faciale ont grandement évolué depuis leur création au début des années 1990 jusqu'à leur première commercialisation, stimulée par la création d'ensembles de données plus importants dans les années 2000 et avec l'intégration de techniques d'apprentissage profond à partir de 2014[7].

À ce jour, les technologies relevant de la sphère de l'IA, telles que l'**apprentissage automatique**, y compris l'**apprentissage profond** et les **algorithmes de vision artificielle**, permettent de plus en plus aux ordinateurs de visualiser, de collecter et de traiter le contenu d'images et de vidéos. Les algorithmes sont habituellement entraînés à apprendre et à extraire des propriétés et caractéristiques faciales à partir de vastes ensembles de données, et l'apprentissage profond est désormais l'approche dominante en matière de détection et d'analyse faciales[8]. L'IA améliore les systèmes traditionnels de reconnaissance faciale en permettant, par exemple, une identification plus rapide et plus précise (notamment en cas de faible éclairage et de cibles en partie cachées). Ce passage aux **systèmes de reconnaissance faciale «basés sur l'IA»** favorise l'apparition d'applications de TRF dans le monde réel[9]. Toutefois, dans le même temps, cette «deuxième vague» de technologies biométriques collecte des données à caractère personnel hautement sensibles[10].

6 Ibid.

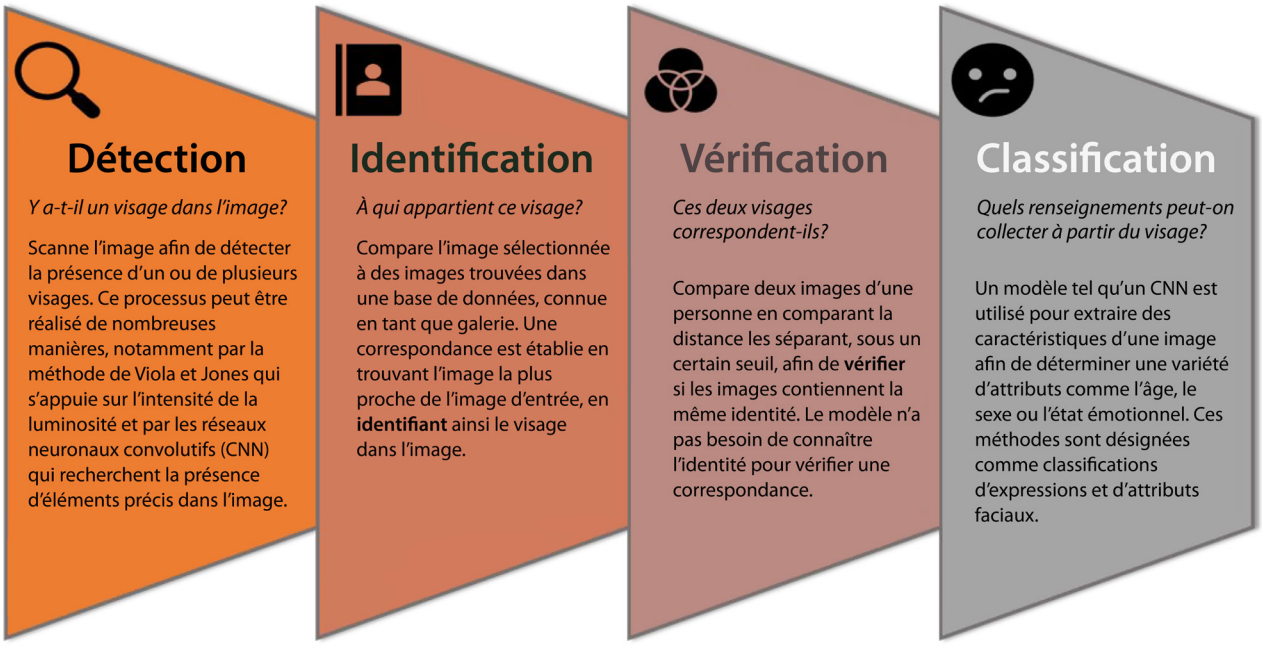
7 Pour un aperçu de l'évolution technologique, voir Raji, I., et Fried, G. (2021), *About Face: A Survey of Facial Recognition Evaluation*.

8 Voir Leslie, D. (2020), *Understanding bias in facial recognition technologies*, The Alan Turing Institute.

9 Voir Wang, M., et Deng, W. (2020), *Deep Face Recognition: A Survey*. Voir également: OCDE (2019), *L'intelligence artificielle dans la société*, p. 88.

10 Voir Commission européenne (2021), *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*, p. 8.

Figure 1 — Techniques de détection et de reconnaissance faciale



Source: The Alan Turing Institute, 2020.

1.2. Utilisation

Des applications biométriques sont utilisées au quotidien dans la vie privée et publique. Les applications de reconnaissance faciale sont notamment devenues populaires auprès des entreprises, des consommateurs et des gouvernements (voir annexe 1) et se diffusent très rapidement[11]. Les utilisations actuelles sont diverses et incluent:

- **Applications grand public**

Un nombre croissant de dispositifs informatiques, tels que les smartphones, les ordinateurs ou les sonnettes intelligentes, sont dotés de technologies de reconnaissance faciale afin d'identifier l'utilisateur. Par exemple, des systèmes de vérification du visage sont utilisés pour accorder l'accès à un ordinateur ou à un téléphone portable. Ces technologies — dont même des enfants se servent — sont de plus en plus utilisées pour **accéder aux services numériques**, comme Snapchat (qui repose sur la vision par ordinateur) ou Facebook (qui détecte les visages sur les photos des utilisateurs)[12]. Les constructeurs automobiles intègrent également ces technologies afin de permettre aux conducteurs **d'accéder aux véhicules** et de les surveiller pour détecter des signes annonciateurs d'endormissement ou d'inattention[13].

[11] Voir Rowe, E. (2021), «Regulating Facial Recognition Technology in the Private Sector», *Stanford Technology Law Review*, vol. 24, nº 1.

[12] Voir Dirin, A., Suomala, J., et Alamäki, A. (2019), *AI-based Facial Recognition in Emotional Detection*.

[13] Voir Buolamwini, J., *et al.* (2020).

Applications commerciales et à des fins de paiement

Dans le secteur bancaire, les technologies de reconnaissance faciale réduisent le besoin d'intervention humaine. Les banques utilisent de tels systèmes pour authentifier l'identité des clients dès qu'ils approchent un distributeur automatique ou lorsqu'ils ouvrent une application de services bancaires sur un appareil mobile, ainsi que pour effectuer des vérifications anti-fraude[14]. Ces technologies facilitent les **services bancaires mobiles** en authentifiant les utilisateurs au moyen de l'empreinte digitale ou de la reconnaissance faciale enregistrée par smartphone[15]. Les commerçants intègrent également des systèmes de paiement fondés sur la reconnaissance faciale, afin d'évaluer les données démographiques des acheteurs à des fins de marketing ou de bloquer l'accès aux locaux commerciaux si le système signale un consommateur «suspect»[16].

Surveillance ou contrôle des accès aux espaces physiques

Les technologies de reconnaissance faciale qui prennent, à distance, les mesures biométriques d'une personne, sans interagir avec elle, offrent de grands avantages par rapport à d'autres solutions de sécurité biométrique, telles que les empreintes palmaires et digitales. À des fins **répressives**, la reconnaissance faciale peut contribuer à identifier une personne ayant un casier judiciaire ou d'autres problèmes juridiques[17]. Les agents des services de répression peuvent utiliser la reconnaissance faciale pour effectuer des comparaisons avec des images de suspects figurant dans les bases de données, à l'appui des enquêtes. De telles TRF sont également déjà largement utilisées pour vérifier l'identification des passeports dans les aéroports et les ports à des fins de **contrôle aux frontières**[18] et pourraient devenir des technologies fondamentales pour l'identification des voyageurs et dans le cas des candidats à l'immigration à l'avenir[19].

Par ailleurs, on observe une tendance à adopter les technologies de reconnaissance et d'identification dans les **espaces publics**[20]. Par exemple, les manifestations ou rassemblements publics peuvent être soumis à l'identification faciale en temps réel, et pour les événements récréatifs (par exemple, événements sportifs et concerts), les opérations de billetterie peuvent utiliser la vérification faciale. Même dans les milieux **du travail et de l'éducation**, des systèmes de reconnaissance faciale sont déjà déployés. Par exemple, des employeurs utilisent des technologies faciales pour limiter l'accès des employés à certains espaces de travail et pour évaluer les candidats lors d'entretiens professionnels, et les TRF sont en cours de déploiement dans les établissements scolaires pour faire l'appel et évaluer l'attention des élèves[21].

---

14 Voir *AI-powered decision making for the bank of the future* (2021), McKinsey.

15 Voir OCDE (2019), p. 57.

16 Voir Fourtané, S. (2020), *AI Facial Recognition and IP Surveillance for Smart Retail, Banking, and the Enterprise*.

17 Salama AbdELminaam, D. (2020), «A deep facial recognition system using computational intelligent algorithms», *PLoS ONE*, vol. 15, nº 12, p. 2.

18 Voir Dumbrava, C. (juillet 2021), *Artificial intelligence at EU borders: Overview of applications and key issues*, EPRS, Parlement européen.

19 Voir gouvernement du Royaume-Uni (2021), *New Plan for Immigration: Legal Migration and Border Control Strategy Statement*. Le Royaume-Uni prévoit d'installer de nouvelles technologies (notamment de biométrie faciale) afin de veiller à ce que la majorité des personnes arrivant aux principaux ports britanniques passent, à des fins d'identité et de sécurité, par une sorte de couloir sans contact ou des portes automatisées.

20 Voir Crawford, K., *et al.* (2020), *AI Now Report*, p. 11. Hong Kong, Delhi, Détroit et Baltimore utilisent déjà la technologie de reconnaissance faciale à des fins de surveillance publique.

21 Voir Buolamwini, J., *et al.* (2020). Voir également Trades Union Congress (2021), *Technology managing people — The worker experience*.

Autres

Il existe de nombreuses autres applications de TRF, notamment à des fins de **marketing numérique**, de **soins de santé** (à savoir pour le triage des patients), et **d'organisation des élections** (à savoir pour le vote électronique)[22]. En outre, ces dernières années, la reconnaissance faciale est devenue une technologie fondamentale pour permettre l'**analyse des sentiments**. Au-delà de l'identification des personnes, de nouveaux systèmes sont mis au point pour recueillir des caractéristiques démographiques, des états émotionnels et des traits de personnalité. Ces «**technologies de reconnaissance des émotions**» sont de plus en plus utilisées pour analyser les expressions faciales et autres données biométriques en vue de suivre l'état sentimental et de mesurer les émotions humaines[23]. La reconnaissance des émotions a même été présentée comme une prochaine étape naturelle dans l'évolution des applications biométriques, menant à l'intégration de la connaissance des émotions dans des lieux où la reconnaissance faciale a déjà été mise en place[24]. Les utilisations potentielles de cette technologie englobent un large éventail d'applications, notamment pour l'analyse du comportement des clients, la publicité et les soins de santé (par exemple, la détection de l'autisme)[25]. Une autre évolution notable dans ce domaine concerne l'utilisation actuellement à l'essai de la technologie de reconnaissance faciale pour **évaluer l'orientation politique des personnes**[26].

1.3. Aspect économique

Étant donné que les technologies de reconnaissance faciale pénètrent rapidement de nombreux aspects de notre vie quotidienne, le **marché de la reconnaissance faciale est appelé à croître rapidement**[27]. La reconnaissance faciale est de plus en plus largement utilisée comme technologie clé pour l'authentification lors de paiements. Le nombre d'utilisateurs d'une reconnaissance faciale basée sur logiciel pour sécuriser les paiements par téléphone portable devrait augmenter considérablement et dépasser 1,4 milliard à l'échelle mondiale d'ici 2025, compte tenu des obstacles relativement réduits à son introduction sur ce marché (à savoir qu'il ne faut qu'une caméra frontale et un logiciel approprié) et de la mise en place de cette technologie à grande échelle par de grandes plateformes (par exemple, FaceID par Apple)[28]. Un certain nombre d'entreprises conçoivent et proposent des solutions biométriques aux gouvernements, aux autorités publiques et aux entités privées dans les domaines de l'identité civile et de la sécurité publique. Elles fournissent des services pour les contrôles aux frontières, la sécurité publique et les activités répressives, notamment la médecine légale et la reconnaissance faciale en temps réel[29].

---

22 Voir i-SCOOP, *Facial recognition 2020 and beyond — trends and market*.

23 Voir Dirin, A., *et al.* (2019). Voir également Crawford, K. (2020), *et al.*, *AI Now Report*.

24 Voir article 19 (2021), *Emotional Entanglement: China's emotion recognition market and its implications for human rights*, Londres, p. 18.

25 Voir *Facial Emotion Recognition* (mai 2021), site internet du contrôleur européen de la protection des données.

26 Voir Kosinski, M. (janvier 2021), «Facial recognition technology can expose political orientation from naturalistic facial images», *Scientific Reports* 11, nº 100.

27 Voir i-SCOOP (2020), *Facial recognition 2020 and beyond — trends and market*. Voir également Fortune Business Insights (2021), *Facial recognition market, Global Industry Analysis, Insights and Forecast, 2016-2027*. Le rapport a révélé que la taille du marché mondial de la reconnaissance faciale passera de 4,35 milliards de dollars américains en 2019 à près de 13 milliards de dollars américains d'ici 2027.

28 Voir *Mobile payment authentication: Biometrics, Regulation & forecasts 2021-2025* (2021), Juniper Research. Voir également *Facial Recognition for Payments Authentication to Be Used by Over 1.4 Billion People Globally by 2025* (2021), communiqué de presse, Juniper Research.

29 Voir, par exemple, les services proposés par l'entreprise Thales.

En corollaire, les investissements dans les technologies de reconnaissance faciale augmentent au fur et à mesure que les technologies progressent. Une étude de Stanford a montré qu'après les secteurs des véhicules autonomes et de la santé, la reconnaissance faciale a reçu **la troisième plus grande part des investissements mondiaux dans l'IA** en 2019, avec près de 4,7 milliards de dollars américains[30]. La crise de la COVID-19 semble avoir accéléré l'investissement massif dans les systèmes de reconnaissance faciale, qui font l'objet d'un usage croissant dans les soins de santé numériques et sont perçus comme complémentaires à d'autres technologies, telles que l'IA, l'internet des objets (IDO) et la 5G[31].

1.4. Principales conclusions

Ces dernières années, d'importants progrès technologiques ont été réalisés dans le domaine de la reconnaissance faciale. L'IA a favorisé l'utilisation des technologies biométriques, notamment des applications de reconnaissance faciale, qui sont de plus en plus employées à l'heure actuelle afin d'assurer la vérification et l'identification des clients, pour des applications commerciales et de paiement, et à des fins de surveillance par des acteurs privés ou publics. L'investissement dans les technologies de reconnaissance faciale devrait également augmenter dans les années à venir, car l'utilisation de celles-ci fera un bond et se diversifiera, et le nombre de déploiements et d'expérimentations en matière de systèmes de TRF croît rapidement.

2. Inquiétudes suscitées par la reconnaissance faciale

En dépit des réels avantages associés à la vérification de l'identité en matière de sûreté publique, de sécurité et d'efficacité[32], l'évolution de la reconnaissance faciale suscite un certain nombre de préoccupations découlant d'une combinaison de caractéristiques spécifiques à cette technologie et de ses éventuelles répercussions sur les droits fondamentaux.

2.1. Caractéristiques techniques et précision de la technologie de reconnaissance faciale

Le fait que la technologie de reconnaissance faciale soit **omniprésente**, alors que **le contrôle humain est difficile à mettre en place**, constitue l'une des principales sources de préoccupation. La technologie de reconnaissance faciale enregistre des caractéristiques du corps humain qu'une personne ne peut modifier (contrairement aux identifiants de téléphone portable), un grand nombre d'images sont déjà disponibles (par exemple sur l'internet), et des images faciales peuvent être prises à distance à l'insu d'une personne, tandis qu'il est très difficile d'obtenir le consentement d'un individu lorsque la technologie est utilisée dans les espaces publics[33]. En outre, l'utilisation de techniques d'apprentissage profond permet la collecte d'informations extrêmement sensibles concernant un très grand nombre de personnes, et rend la vérification et la catégorisation manuelles presque impossibles, car les ensembles de données ne cessent de croître[34]. Par ailleurs,

30 Voir Université de Stanford (2019), *The AI Index 2019 Annual Report*.

31 Voir i-SCOOP et Fortune Business Insights ci-dessus.

32 Pour un aperçu des avantages, voir «Facial Recognition Technology», *Snapshot Series*, Centre for Data Ethics and Innovation, p. 21.

33 Voir Castelluccia, C., et Le Métayer Inria, D. (2020), *Impact Analysis of Facial Recognition*, Centre for Data Ethics and Innovation, p. 7-8.

34 Hao, K. (2021), «This is how we lost control of our faces», *MIT Technology review*.

les **risques en matière de sécurité** posés par la collecte et par la conservation des données de reconnaissance faciale, ainsi qu'un risque de violation et d'utilisation abusive de ces données, ont été soulignés[35].

De plus, le **risque d'erreur** a été mis en exergue. Des études empiriques[36] montrent que les performances techniques de la majorité des systèmes de reconnaissance faciale demeurent quelque peu limitées et que les logiciels de détection faciale sont susceptibles de commettre deux types d'erreurs. Un **faux négatif** se produit lorsque le logiciel de reconnaissance faciale ne parvient pas à détecter un visage présent sur une image. Un **faux positif** se produit lorsqu'un détecteur facial identifie comme étant un visage un élément qui n'en est pas un[37]. Les taux d'erreur peuvent être importants, en particulier lorsque les photographies qui sont comparées contiennent différents éclairages, ombres, arrière-plans, poses ou expressions, ou en cas d'utilisation d'images à faible résolution. Les systèmes de TRF sont également moins précis lorsqu'il existe un écart d'âge important (par exemple, entre l'image d'une personne jeune et l'image de cette même personne dix ans plus tard)[38]. L'**insuffisance des données d'apprentissage** constitue une autre cause de biais algorithmique dans les logiciels de reconnaissance faciale[39]. Ces risques peuvent être lourds de conséquences sur les droits fondamentaux.

Des entreprises se retirent du marché des TRF

Le risque d'erreur a amené certaines entreprises à se retirer du marché des TRF. **Axon**, fournisseur majeur de caméras embarquées pour les forces de police aux États-Unis, a décidé de ne pas commercialiser de technologie de mise en correspondance des visages, compte tenu des graves préoccupations éthiques et des limites technologiques constatées[40]. De même, **Microsoft** et **Amazon** ont annoncé des moratoires sur leur production de logiciels et de services de reconnaissance faciale, et **IBM** a déclaré ne pas poursuivre cette activité[41].

2.2. Inquiétudes en matière de protection des données et de la vie privée

L'utilisation des technologies de reconnaissance faciale entraîne la collecte, la comparaison ou l'enregistrement d'images faciales à des fins d'identification. L'utilisation des technologies de reconnaissance faciale basées sur l'IA, notamment les techniques biométriques de «deuxième vague», fait appel à des technologies et des algorithmes plus élaborés, qui collectent des données à caractère personnel hautement sensibles[42]. La combinaison croissante des technologies d'IA et de l'IDO signifie que davantage de données, y compris des données à caractère personnel, sont constamment collectées et analysées par des dispositifs (par exemple, des caméras de surveillance ou des véhicules autonomes), l'utilisation de technologies d'IA améliorées (comme la

35 Voir Turner Lee, N., Resnick, P., et Barton, G. (2019), *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, Brookings. Voir Rowe, E. (2021), p. 32-34.

36 Voir Grother, P., *et al.* (2019), *Face Recognition Vendor Test (FRVT)*.

37 Voir Buolamwini, J., *et al.*, p. 3.

38 Voir Lynch, J. (2020), *Face Off: Law Enforcement Use of Face Recognition Technology*, Electronic Frontier Foundation, p. 11-12.

39 Voir Turner Lee, N., Resnick, P., et Barton, G. (2019), *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, Brookings.

40 Voir Smith, R. (2019), *The future of face matching at Axon and AI ethics board report*.

41 Voir Leslie, D. (2020), p. 22. Voir également Smith, R. (2019), *The future of face matching at Axon and AI ethics board report*.

42 Voir Commission européenne (2021), *Study supporting the impact assessment of the AI regulation*.

reconnaissance faciale) s'avérant plus invasive en ce qui concerne la protection de la vie privée et des données des personnes[43]. De telles pratiques suscitent de vives préoccupations en ce qui concerne le **droit à la protection des données à caractère personnel** établi à l'**article 8** de la charte des droits fondamentaux de l'Union européenne (ci-après «la charte») et le **droit au respect de la vie privée** en vertu de l'**article 7** de la charte (voir section 3 ci-dessous)[44]. Les inquiétudes portent essentiellement sur la **difficulté de s'assurer du consentement explicite** à l'utilisation des TRF. Il a été signalé qu'un certain nombre de fournisseurs ont mis la main sur des images faciales disponibles publiquement, provenant d'autres sites internet, pour alimenter leurs bases de données biométriques[45], et que même les chercheurs en TRF ont progressivement renoncé à demander aux personnes concernées si elles donnaient leur consentement[46].

2.3. Inquiétudes quant aux biais et à la discrimination

La discrimination désigne une situation dans laquelle une personne est, a été ou serait traitée moins favorablement qu'une autre dans une situation comparable[47]. Une discrimination dans la prise de décision algorithmique peut survenir lors de la conception, des essais et de la mise en place des algorithmes utilisés pour la reconnaissance faciale, par les biais incorporés dans l'algorithme même, ou en raison de la manière dont les résultats sont transmis par la personne ou l'autorité qui exécute la reconnaissance faciale[48]. La technologie de reconnaissance faciale peut donner lieu à des taux très élevés de faux positifs/faux négatifs et les biais peuvent aboutir à différents types de discrimination à l'encontre de certaines catégories de la population. Des **biais quant au sexe et à la race** ont notamment été signalés, car la précision de la technologie de reconnaissance faciale varie énormément et celle-ci est moins précise pour les femmes et les personnes de couleur que pour les hommes blancs[49].

Les études empiriques montrent que le risque de traitement discriminatoire concernant les populations/personnes de couleur est plus élevé dans le contexte des activités répressives[50]. L'utilisation de données d'apprentissage qui incorporent un échantillon biaisé est un problème typique pour de nombreuses technologies de reconnaissance faciale qui sont moins performantes avec les personnes noires qu'avec les personnes blanches — et encore moins avec les femmes noires. Il a été constaté qu'aux États-Unis, le nombre de faux positifs est disproportionné en ce qui concerne les personnes de couleur et **modifie la présomption d'innocence ordinaire** dans les affaires pénales, en compliquant encore la tâche des suspects et des accusés qui doivent prouver qu'ils ne sont pas les personnes identifiées par le système[51]. Cela porte atteinte à l'article 21 de la charte, qui interdit toute discrimination fondée sur le sexe, la race, la couleur, les origines ethniques

43 Voir également OCDE (2019), *L'intelligence artificielle dans la société*, p. 88.

44 Voir Agence des droits fondamentaux de l'Union européenne (2020), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*.

45 Kak, A., «Introduction», dans Kak, A. (septembre 2020), *Regulating Biometrics*, AI now, p. 7.

46 Hao, K. (2021), «This is how we lost control of our faces», *MIT Technology review*.

47 Voir Agence des droits fondamentaux de l'Union européenne (2020).

48 Ibid, p. 27.

49 Voir Buolamwini, J., et Gebru, T. (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. Voir également Cavazos, J. (2021), *et al.*, «Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?», *IEEE Transactions on Biometrics, Behaviour and Identity Science*.

50 Voir Amnesty International (2021), *Il faut interdire les technologies de reconnaissance faciale qui amplifient le risque de racisme lors des opérations policières*. Voir également Hardesty, L. (2018), *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News.

51 Voir Lynch, J. (2020), *Face Off: Law Enforcement Use of Face Recognition Technology*, Electronic Frontier Foundation.

ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle[52].

Par ailleurs, des universitaires ont souligné l'existence d'incidences plus vastes et de préjudices moraux subis par les personnes dont les vies sont directement touchées par les risques de mauvaises utilisations et d'utilisation abusive des TRF. Ces préoccupations sont liées à l'«**injustice distributive**», par exemple lorsque des membres d'un groupe social victime de discrimination se voient refuser l'accès à des avantages, à des ressources ou à des possibilités en raison de leur appartenance à ce groupe. Les inquiétudes portent également sur l'«**injustice en matière de reconnaissance**», par exemple lorsque les affirmations que les membres d'un groupe social victime de discrimination formulent quant à leur identité sont niées ou bafouées d'une manière qui confirme et accroît leur marginalisation[53].

2.4. Surveillance de masse et inquiétudes relatives aux droits fondamentaux

Les risques liés à une éventuelle généralisation de l'utilisation des technologies de reconnaissance faciale ont également été mis en exergue. La possibilité d'**étendre l'utilisation des systèmes de reconnaissance faciale** au-delà de leur finalité initialement autorisée et contrôlée comporte certains risques à moyen ou à long terme. Un tel élargissement peut consister, par exemple, à utiliser les données collectées sur les réseaux sociaux ou dans des bases de données créées à l'origine pour d'autres finalités, à utiliser une base de données au-delà de sa finalité autorisée ou à introduire de nouvelles fonctionnalités dans un système existant (par exemple, en élargissant la reconnaissance faciale utilisée pour le contrôle des passeports aux paiements effectués dans un aéroport puis dans toute la ville)[54]. Selon certains, un tel élargissement pourrait faire partie d'une stratégie délibérée des promoteurs, qui utilisent des systèmes de reconnaissance faciale d'abord dans des contextes dans lesquels la finalité semble légitime, puis qui élargissent progressivement leur utilisation (à savoir, l'**argument de la «pente glissante»**)[55].

Les systèmes d'identification biométrique à distance font l'objet d'un usage croissant dans des espaces accessibles au public, et la reconnaissance faciale semble devenir rapidement la norme au sein de l'Union. Les enquêtes de la Commission européenne montrent que, quel que soit le lieu où un tel système est utilisé, il est possible de suivre les allées et venues des personnes figurant dans la base de données de référence, ce qui a des conséquences sur leurs données à caractère personnel, leur vie privée, leur autonomie et leur dignité[56]. Par conséquent, de nouvelles inquiétudes sociales, telles que l'**impossibilité de se déplacer de manière anonyme dans l'espace public ou un conformisme** au détriment du libre arbitre, pourraient découler de ce mécanisme de surveillance de masse créé par l'utilisation de systèmes de reconnaissance faciale. En ce sens, l'autorité de protection des données italienne a déclaré que le traitement automatisé des données biométriques

---

52 Voir Agence des droits fondamentaux de l'Union européenne (2020).

53 Voir Leslie, D. (2020), p. 21-25. On peut citer l'exemple d'un système automatisé, créé dans le but d'améliorer l'efficacité d'un processus administratif, qui atteint systématiquement ses objectifs pour un ou plusieurs groupes sociaux privilégiés, mais obtient l'effet contraire pour les groupes marginalisés (c'est-à-dire qu'il accroît la quantité de temps et d'efforts requis pour réaliser le même processus).

54 Voir Castelluccia, C., et Inria, D. (2020), p. 8-9.

55 Ibid, p. 17.

56 Voir Commission européenne (2021), *Impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council*, p. 18.

pour la reconnaissance faciale était susceptible de constituer une forme de **surveillance de masse indifférenciée**[57].

En outre, l'utilisation des TRF suscite de nouvelles préoccupations eu égard à un certain nombre d'autres libertés civiles, notamment la **liberté de religion**[58] et les **droits des enfants** — en tant que population vulnérable méritant un niveau de protection plus élevé, notamment lorsque les TRF sont utilisées à des fins répressives et pour d'autres finalités en matière de gestion des frontières[59], compte tenu de la précision moindre avec laquelle la technologie détecte les visages jeunes qui changent rapidement[60]. Il a également été souligné que les technologies de reconnaissance faciale utilisées pour traiter des images faciales enregistrées par des caméras vidéo dans des espaces publics étaient susceptibles de porter atteinte à la **liberté d'opinion et d'expression** d'une personne et d'avoir des incidences négatives sur sa **liberté de réunion et d'association**[61]. L'utilisation de la technologie de reconnaissance faciale pour identifier des personnes lors de rassemblements présente des effets particulièrement dommageables sur les droits au respect de la vie privée, à la liberté d'expression et à la liberté de réunion pacifique, selon un rapport du Conseil des Droits de l'homme des Nations unies[62]. De plus, l'identification et la traçabilité automatiques des personnes peuvent avoir de lourdes conséquences sur le comportement social et psychologique des citoyens, et soulèvent d'importantes **questions éthiques** liées à l'utilisation de cette technologie[63]. Les conséquences peuvent être encore plus graves lorsqu'elles comportent le risque d'assister à la hausse d'un racisme structurel enraciné et qui menace les formes démocratiques modernes ou la solidarité sociale existante en raison d'infrastructures de surveillance faciale[64]. Toutes ces préoccupations se traduisent par une attitude assez prudente des citoyens de l'Union envers la technologie de reconnaissance faciale.

---

57 Mentionné dans une question avec demande de réponse écrite du Parlement européen, *Question for written answer E-002182/2021*.

58 Voir Rowe, E. (2021), p. 31.

59 Voir Agence des droits fondamentaux de l'Union européenne (2020), p. 28.

60 Voir Rowe, E. (2021), p. 26.

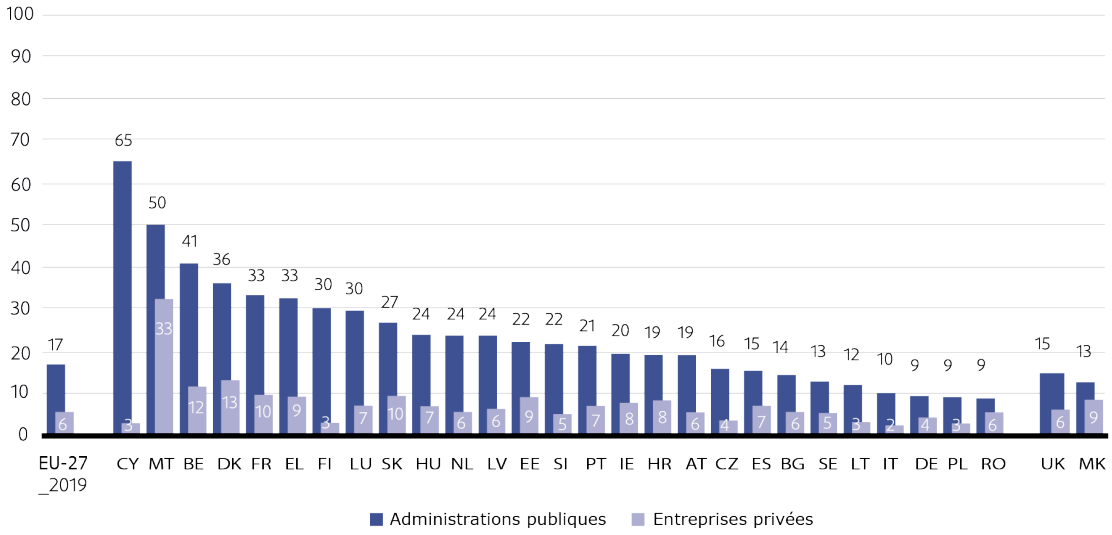
61 Voir Agence des droits fondamentaux de l'Union européenne (2020), p. 29-30.

62 Voir le rapport de la haute-commissaire des Nations unies aux Droits de l'homme (2020), *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*.

63 Voir Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle (2019), *Lignes directrices en matière d'éthique pour une IA digne de confiance*, p. 33.

64 Voir Leslie, D. (2020).

Figure 2 — Disposition à partager des images faciales à des fins d'identification avec les autorités publiques et les entreprises privées, par pays



Source: Agence des droits fondamentaux de l'Union européenne (2020), *Your rights matter: Data protection and privacy*.

Au vu de ce qui précède, il est fondamental de définir les conditions dans lesquelles l'IA peut être utilisée pour l'identification automatisée des personnes et d'établir une distinction entre l'identification et le traçage d'une personne et entre la surveillance ciblée et la surveillance de masse afin d'établir le cadre approprié (voir section 4 ci-dessous)[65].

2.5. Principales conclusions

Les préoccupations soulevées par l'évolution de la reconnaissance faciale résultent d'une combinaison de caractéristiques techniques et du manque de précision de ces technologies, qui peuvent donner lieu à de graves menaces pour les libertés civiles. Bien qu'il existe de réels avantages, du point de vue de la sûreté publique, de la sécurité et de l'efficacité, à utiliser des systèmes de reconnaissance faciale à des fins de vérification de l'identité, le risque d'erreur algorithmique est élevé. La technologie de reconnaissance faciale peut être assortie de taux très élevés de faux positifs et de faux négatifs, et aboutir à des biais et à différents types de discrimination à l'encontre de certaines populations. L'utilisation croissante de systèmes d'identification biométrique à distance dans des espaces accessibles au public est une question particulièrement sensible.

3. Cadre juridique actuel au sein de l'Union

3.1. Interaction et fonctionnement du cadre à plusieurs niveaux de l'Union

Dans l'ordre juridique de l'Union, les règles en matière de protection des données, de respect de la vie privée et de non-discrimination ainsi que la proposition de règlement en matière d'IA définissent

[65] Voir Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle (2019), p. 33.

des paramètres essentiels pour la mise au point et pour l'utilisation des TRF. Les règles pertinentes sont réparties sur plusieurs niveaux de l'ordre juridique de l'Union. Plus particulièrement, les droits fondamentaux à la protection des données, au respect de la vie privée et à la non-discrimination inscrivent un ensemble de garanties de base dans la charte, c'est-à-dire dans le droit primaire. Bien que la charte s'adresse aux institutions de l'Union et aux États membres lorsqu'ils mettent en œuvre le droit de l'Union (article 51, paragraphe 1, de la charte), elle peut avoir des répercussions sur les relations entre parties privées («effet horizontal»)[66]. Le droit dérivé, qui donne effet aux droits fondamentaux et aux réglementations sectorielles, régit plus en détail l'élaboration et le déploiement des technologies émergentes. Dans ce cadre à plusieurs niveaux, le droit dérivé et sa mise en œuvre doivent être cohérents avec le droit primaire.

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

Étant donné que l'utilisation des TRF entraîne le traitement des données à des fins d'identification, son utilisation par les autorités publiques constitue une ingérence dans le **droit à la protection des données**, tel qu'établi à l'article 8 de la charte, et le **droit au respect de la vie privée**, au titre de l'article 7 de la charte. Plus particulièrement, l'enregistrement vidéo initial, la conservation ultérieure des images et la comparaison de ces dernières avec les enregistrements figurant dans des bases de données à des fins d'identification (correspondance) constituent des ingérences dans ce droit ou des limitations à l'exercice de celui-ci. Toute restriction de l'exercice de ces droits fondamentaux doit être strictement nécessaire et proportionnée, conformément à l'article 52, paragraphe 1, de la charte[67].

Toutefois, dans la pratique, ces droits fondamentaux en sont encore à leurs débuts[68] et leur application aux relations privées n'a pas encore été délimitée[69]. En soi, ils fournissent tout juste des orientations pratiques sur l'utilisation des TRF et, souvent, ne permettent qu'indirectement d'endiguer et de résoudre les conflits qui éclatent entre la protection des données et les technologies émergentes. C'est davantage leur «expression» dans le droit dérivé qui présente un cadre exploitable[70]. La **directive en matière de protection des données dans le domaine répressif** [directive (UE) 2016/680] et le **règlement général sur la protection des données** (RGPD) s'appliquent au traitement automatisé de données à caractère personnel et au traitement manuel de données à caractère personnel contenues dans un fichier, conformément à l'article 2, paragraphe 1, du RGPD et à l'article 2 de la directive (UE) 2016/680[71]. Toutefois, la directive (UE) 2016/680 est un régime plus spécifique que le RGPD (*lex specialis*) et est applicable lorsque les autorités publiques traitent des données à caractère personnel à des fins de prévention et de

---

66 Voir Frantziou, E. (2020), «The Horizontal Effect of the Charter», *Cambridge Yearbook of European Legal Studies*, vol. 22.

67 En ce qui concerne la protection des données, les exigences visées à l'article 8, paragraphe 2, de la charte doivent être respectées.

68 Pour une introduction, voir Fuster, G., et Hijmans, H. (2019), *The EU rights to privacy and personal data protection: 20 years and 10 questions*, atelier international intitulé «Exploring the Privacy and Data Protection connection».

69 Voir l'arrêt rendu par la CJUE le 13 mai 2014 dans l'affaire C-131/12, Google Spain.

70 Un analyste va jusqu'à dire que «le droit dérivé en matière de protection des données joue [...] un rôle clé, non seulement pour informer du droit fondamental en matière de protection des données, mais également pour établir les conditions et les limites de son application», voir Ivanova, Y., «The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World», dans Hallinan, D. (2020), *et al.*, *Data Protection and Privacy*, vol. 13, p. 5-6.

71 Alors que la directive (UE) 2016/680 s'applique aux traitements de données dans les États membres de l'espace Schengen, le RGPD s'applique aux traitements de données dans l'Espace économique européen (EEE).

détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales [considérants 11 et 12 de la directive (UE) 2016/680 et considérant 19 du RGPD]. Conformément aux principaux principes juridiques en matière de protection des données [article 5 du RGPD et article 4 de la directive (UE) 2016/680], le traitement des images faciales doit:

- être licite, loyal et transparent;
- suivre une finalité déterminée, explicite et légitime (clairement définie dans le droit de l'État membre ou de l'Union);
- être conforme aux exigences de minimisation des données, d'exactitude des données, de limitation de la conservation, de sécurité des données et de responsabilité.

Les responsables du traitement des données (et indirectement, les fabricants) devraient concevoir les activités de traitement des données qu'ils prévoient dans le respect total des principes de protection des données [«protection des données dès la conception et protection des données par défaut», article 25 du RGPD et article 20 de la directive (UE) 2016/680][72].

3.2.1. Traitement licite, loyal et transparent des données

Conformément à l'article 5, paragraphe 1, point a), du RGPD, et à l'article 4, paragraphe 1, point a), de la directive (UE) 2016/680, ainsi qu'au considérant 26 de cette dernière, tout traitement des données à caractère personnel doit être licite, loyal et transparent au regard de la personne concernée.

3.2.1.1. Licéité

Pour être licite, le traitement doit répondre aux exigences des **bases juridiques spécifiques** [considérant 40 du RGPD et considérant 35 de la directive (UE) 2016/680]. La vidéosurveillance peut avoir, pour base juridique, l'article 6 du RGPD[73] ou les transpositions nationales de l'article 8 de la directive (UE) 2016/680; néanmoins, si elle est utilisée dans le cadre du traitement de catégories particulières de données, le responsable du traitement doit (en outre) satisfaire aux strictes exigences visées à l'article 9 du RGPD ou à l'article 10 de la directive (UE) 2016/680[74]. Étant donné que les TRF traitent généralement automatiquement les données liées aux caractéristiques physiques, physiologiques ou comportementales afin d'identifier une personne de manière unique, leur utilisation est considérée comme un traitement des données biométriques[75] au sens de l'article 3, paragraphe 13, de la directive (UE) 2016/680 et de l'article 4, paragraphe 14, du RGPD[76]. Par conséquent, un tel traitement devra satisfaire aux strictes exigences de l'article 9 du RGPD et de l'article 10 de la directive (UE) 2016/680. Les décisions fondées exclusivement sur le traitement

---

72 Voir Comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 30; voir Conseil de l'Europe (2021), *Lignes directrices sur la reconnaissance faciale*, p. 15; voir Comité européen de la protection des données (2020), *Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par défaut*, p. 17-18.

73 Pour plus d'informations, voir Comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 9-14; voir également *Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen* (17 juillet 2020), conférence des autorités allemandes de protection des données (DSK), p. 7-15.

74 Voir Comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 17. Plusieurs analystes considèrent que l'article 9 du RGPD prévaut sur l'article 6 du RGPD, en tant que *lex specialis*, tandis que le comité européen de la protection des données admet leur application concomitante.

75 Kindt, E. J. (2018), «Having yes, using no? About the new legal regime for biometric data», *Computer Law & Security Review*, vol. 34, nº 3.

76 Voir Comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 18-21.

automatisé peuvent être prises uniquement si les exigences visées à l'article 22, paragraphes 2 et 4, du RGPD ou à l'article 11, paragraphes 1 et 2, de la directive (UE) 2016/680 sont satisfaites. Le comité européen de la protection des données considère que «l'utilisation de la vidéosurveillance comprenant une fonctionnalité de reconnaissance biométrique installée par des entités privées pour servir leurs propres intérêts (par exemple, à des fins de marketing, de statistiques, voire de sécurité) nécessitera, dans la majorité des cas, le **consentement explicite** de toutes les personnes concernées [article 9, paragraphe 2, point a), du RGPD][77]. Une autre base juridique invoquée à maintes reprises dans le contexte des TRF est l'article 9, paragraphe 2, point g), du RGPD, qui autorise le traitement des données à caractère personnel fondé sur le droit de l'Union ou d'un État membre si celui-ci «est nécessaire pour des motifs d'intérêt public important»[78].

Le déploiement de la reconnaissance faciale basée sur la biométrie par les services répressifs est soumis à des conditions similaires en vertu de l'article 4, paragraphe 1, point a), et de l'article 10 de la directive (UE) 2016/680[79]. Dans le contexte des **activités répressives**, les services de police invoquent généralement les codes de procédure pénale[80] ou les codes et les législations policières en matière de surveillance[81] en tant que bases juridiques. Certaines opérations d'essai ont été fondées sur le consentement[82]. Dans une affaire britannique, la Cour d'appel a annulé une décision de première instance, notamment parce que le cadre juridique n'était pas considéré comme une base juridique, en ce sens qu'il était imprécis et accordait trop de pouvoirs aux agents de police quant aux personnes dont les noms pouvaient être ajoutés à une liste de surveillance et sur les lieux où les TRF pouvaient être déployées[83]. Dans une affaire allemande, l'autorité de protection des données de Hambourg a considéré que la vidéosurveillance indifférenciée ainsi que l'extraction et la conservation des données biométriques lors du sommet du G20 de 2017 n'étaient pas fondées sur des bases juridiques suffisantes[84]. Après l'annulation, par un jugement de première instance, de l'ordonnance demandant la suppression de la base de données policière des modèles biométriques, l'autorité de protection des données de Hambourg a fait valoir, en appel, que l'absence de bases juridiques suffisamment définies constituait également une violation de l'article 8, paragraphe 2, de la charte, ainsi que de l'article 4, paragraphe 1, point a), de la directive (UE) 2016/680 et de sa

---

77 Voir Comité européen de la protection des données (2020), p. 18. Voir également Center for Democracy & Technology (2019), *CDT response to consultation on EDPB Guidelines 3/2019*, qui salue cette approche. Le Centre for Information Policy Leadership (CIPL) suggère que d'autres bases juridiques devraient être prises attentivement en considération [voir *CIPL response to consultation on EDPB Guidelines 3/2019* (6 septembre 2019), p. 10-11]. En ce qui concerne les exigences relatives au consentement, voir Comité européen de la protection des données (2020), *Lignes directrices 05/2020 sur le consentement au sens du règlement (UE) 2016/679*. En ce qui concerne les obstacles au consentement, voir Selinger, E., et Hartzog, W. (2020), «The Inconsentability of Facial Surveillance», *Loyola Law Review*, vol. 66, nº 1.

78 Voir Agence des droits fondamentaux de l'Union européenne (2020), *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (2020), p. 24, et Contrôleur européen de la protection des données (2019), *Facial recognition: A solution in search of a problem?*

79 Voir Agence des droits fondamentaux de l'Union européenne (2020), p. 24; voir Groupe de travail «Article 29» sur la protection des données (2017), *Avis sur certaines questions clés de la directive (UE) 2016/680 (directive «police»)*, p. 7-6.

80 *Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg* (31 août 2018), autorité de protection des données de Hambourg, p. 10.

81 Information Commissioner's Office du Royaume-Uni (2019), avis intitulé: *The use of live facial recognition technology by law enforcement in public places*, p. 9.

82 Bundespolizeipräsidium Potsdam (28 septembre 2018), *Abschlussbericht Biometrische Gesichtserkennung*, p. 22-23.

83 Arrêt rendu par la Cour d'appel le 11 août 2020 dans l'affaire C1/2019/2670, points 90-96.

84 *Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg* (31 août 2018), autorité de protection des données de Hambourg, p. 9-27.

transposition nationale[85]. Des questions particulières se posent également lorsque des opérateurs mettent la main sur des données publiques ou accèdent à des données collectées par des tiers, afin de développer leurs systèmes de TRF[86].

Encadré 2 — Principe de proportionnalité

Tant l'application directe des droits fondamentaux à la vie privée et à la protection des données[87] qu'une interprétation cohérente avec la charte du RGPD et de la directive (UE) 2016/680 requièrent que le traitement des données lié aux TRF par les institutions et les États membres de l'Union soit proportionné[88]. Les poursuites judiciaires et administratives allemandes et britanniques contre le déploiement des TRF par les services répressifs portent sur des inquiétudes en matière de proportionnalité. En renvoyant aux affaires de la Cour de justice de l'Union européenne (CJUE) Digital Rights Ireland (DRI)[89] et Tele2 Sverige[90], l'autorité de protection des données de Hambourg a considéré que la base juridique invoquée par les services de police n'était pas suffisamment précise et définie, et dès lors qu'elle ne répondait pas aux exigences de proportionnalité au sens de l'article 8 de la charte ni au droit à l'autodétermination informationnelle en vertu du droit fondamental[91]. Même si la base juridique était applicable, l'autorité de protection des données a conclu que l'application pratique des TRF ne répondait pas à l'exigence de stricte nécessité et de proportionnalité requise par la législation applicable[92]. Dans l'affaire britannique, il apparaît que la Cour d'appel aurait considéré le déploiement des TRF comme étant proportionné si celui-ci n'avait pas été illicite en raison de bases juridiques indéterminées, d'une analyse d'impact insuffisante quant à la protection des données et de l'absence d'évaluation de l'éventuelle discrimination algorithmique conformément à l'obligation d'égalité du secteur public[93].

3.2.1.2. Transparence

Conformément au principe de transparence [article 5, paragraphe 1, point a), du RGPD], «[l]e fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées,

---

85 *Antrag auf Zulassung der Berufung §§ 124, 124a VwGO* (13 mars 2020), autorité de protection des données de Hambourg, p. 5-6.

86 Voir Comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 15-16; et Comité européen de la protection des données (2020), *Response to MEPs inquiry on Clearview AI*; ce thème est également amplement débattu par les universitaires.

87 Voir Agence des droits fondamentaux de l'Union européenne (2018), *Manuel — Application de la charte des droits fondamentaux de l'Union européenne dans le processus législatif et l'élaboration des politiques à l'échelle nationale*, Office des publications de l'Union européenne, p. 38.

88 Cette interprétation est appuyée par la primauté de l'article 7, de l'article 8 et de l'article 52, paragraphe 1, de la charte ainsi que par le respect implicite, par le RGPD/la directive (UE) 2016/680, du principe de proportionnalité tel qu'il est mis en évidence par des exigences plus strictes eu égard à des ingérences plus profondes [voir par exemple l'article 6 et l'article 9 du RGPD, ainsi que l'article 8 et l'article 10 de la directive (UE) 2016/680] et la codification fragmentée du principe dans l'ensemble du RGPD et de la directive (UE) 2016/680 [par exemple, considérant 26, troisième phrase, de la directive (UE) 2016/680, et considérant 39, neuvième phrase, article 5, paragraphe 1, point c), article 6, paragraphe 1, points b) à f), et article 35, paragraphe 7, point b), du RGPD]. Voir également le raisonnement de l'autorité de protection des données de Hambourg dans sa procédure en recours du 13 mars 2020, p. 5, 6 et 8. Il conviendrait de garder à l'esprit que les droits fondamentaux influent uniquement de manière exceptionnelle sur les relations entre les entités privées; toutefois, voir l'arrêt rendu par la CJUE le 13 mai 2014 dans l'affaire C-131/12, Google Spain, et Frantziou, E. (2020), «The Horizontal Effect of the Charter», *Cambridge Yearbook of European Legal Studies*, vol. 22.

89 Arrêts rendus par la CJUE le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, Digital Rights Ireland.

90 Arrêt rendu par la CJUE le 21 décembre 2016 dans l'affaire C-203/15, Tele2 Sverige.

91 *Antrag auf Zulassung der Berufung §§ 124, 124a VwGO* (13 mars 2020), autorité de protection des données de Hambourg, p. 8 et suiv.

92 *Antrag auf Zulassung der Berufung §§ 124, 124a VwGO* (13 mars 2020), autorité de protection des données de Hambourg, p. 19-20; Ordonnance au titre de l'article 6 de la HmbRI(EU)2016/680UmsAAG et de l'article 43, paragraphe 1, point 5, de la HmbJVollzDSG (18 décembre 2018), autorité de protection des données de Hambourg, p. 22.

93 Arrêt rendu par la Cour d'appel le 11 août 2020 dans l'affaire C1/2019/2670, points 90-96, 152, 153 et 199-202.

consultées ou traitées d'une autre manière et **la mesure dans laquelle ces données sont ou seront traitées** devraient être transparents à l'égard des personnes physiques concernées» (considérant 39 du RGPD)[94]. Cela n'interdit pas en soi aux autorités compétentes[95] de mener des activités telles que des enquêtes discrètes ou de la vidéosurveillance (considérant 26 de la directive en matière de protection des données dans le domaine répressif. Toutefois, conformément à l'article 13, paragraphe 3, de la directive (UE) 2016/680, les États membres peuvent introduire des **exceptions**, afin d'éviter de gêner ou de nuire aux enquêtes en cours; ou de protéger la sécurité publique et la sécurité nationale. De telles exonérations peuvent s'avérer instrumentales pour les activités répressives, étant donné que la divulgation des TRF au suspect peut miner leurs mesures de répression. Parce que cela empêcherait les personnes concernées d'exercer leurs droits, de solides justifications sont requises pour l'application de ces exceptions[96].

Pour la vidéosurveillance au titre du RGPD, le comité européen de la protection des données recommande une approche à deux niveaux en vue de se conformer aux exigences en matière de transparence[97]. Les informations les plus importantes devraient être fournies au moyen d'un **panneau d'avertissement** placé de sorte que «la personne concernée [visée] puisse aisément reconnaître les circonstances de la surveillance avant de pénétrer dans la zone surveillée». Des indications obligatoires supplémentaires peuvent être communiquées par d'autres moyens facilement accessibles (par exemple, une affiche et un site internet), auxquels le premier niveau fait clairement référence (par exemple, un code QR ou une adresse de site internet). De même, le Conseil de l'Europe adopte une approche à plusieurs niveaux dans ses lignes directrices sur la reconnaissance faciale[98]. De plus, les organismes de réglementation, les acteurs et les universitaires discutent de la mesure dans laquelle une personne dispose du **droit à une explication** de la décision prise à l'issue d'une évaluation algorithmique, y compris «des informations utiles concernant la logique sous-jacente» [considérant 71, articles 13 à 15 et article 22 du RGPD, et considérant 38, article 11, article 13 et article 14 de la directive (UE) 2016/680][99]. Ce droit pourrait bien s'appliquer aux décisions automatisées fondées sur les TRF, mais sa mise en œuvre demeure incertaine.

3.2.1.3. Loyauté

Le comité européen de la protection des données a considéré, dans de récentes lignes directrices, que «[l]a loyauté est un principe fondamental selon lequel les données à caractère personnel ne doivent pas être traitées d'une manière injustifiablement préjudiciable ou illégalement discriminatoire, inattendue ou trompeuse pour la personne concernée»[100]. Le principe est sujet à ambiguïté, et certains analystes le considèrent comme **un principe passe-partout**, qui peut être utilisé dans les cas où le traitement serait autrement autorisé, mais celui-ci semble déloyal en

---

94 Pour plus d'informations, voir groupe de travail «Article 29» (2016), *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679* (approuvées par le comité européen de la protection des données).

95 Article 3, paragraphe 7, de la directive (UE) 2016/680.

96 Voir Agence des droits fondamentaux de l'Union européenne (2020), p. 24.

97 Voir comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 26-27.

98 Voir Conseil de l'Europe (2020), *Lignes directrices sur la reconnaissance faciale*, T-PD(2020)03rev4, p. 11-12.

99 Voir Goodman, B., et Flaxman, S. (2017), «European Union regulations on algorithmic decision-making and a "right to explanation"», *AI Magazine*, vol. 38, nº 3; Wachter, S., *et al.* (2017), «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», *International Data Privacy Law*, vol. 7, nº 2; et divers autres.

100 Voir comité européen de la protection des données (2020), *Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par défaut*, p. 17-18.

l'espèce[101]. Des universitaires suggèrent «que la loyauté constitue un outil correctif pour rééquilibrer des relations asymétriques ou déséquilibrées (c'est-à-dire des situations de vulnérabilités provoquées) entre les responsables du traitement et les personnes concernées»[102]. Bien que la définition de ce principe évolue constamment, des analystes proposent de freiner la discrimination algorithmique au moyen d'une interprétation progressive[103]. Quoiqu'il soit trop tôt pour tirer des conclusions définitives sur le contenu normatif du principe, il devrait être gardé à l'esprit comme un leitmotiv contraignant par les développeurs lors de l'élaboration des TRF et par les opérateurs lors de la conception des plans de mise en œuvre.

Comme indiqué par la conférence des autorités allemandes de protection des données (DSK), un traitement discriminatoire peut simultanément enfreindre l'exigence d'une finalité légitime (voir les informations sur le principe de limitation des finalités ci-dessous)[104]. De même, on pourrait prétendre une ingérence dans le principe de licéité (voir les informations qui précèdent), lorsque le droit fondamental à la non-discrimination n'est pas suffisamment protégé [article 9, paragraphe 2, point g), du RGPD].

3.2.2. Finalité déterminée, explicite et légitime

Le principe de limitation des finalités prévoit que les données à caractère personnel ne peuvent être traitées que pour une **finalité précisément déterminée, explicite et légitime** et qu'un **traitement ultérieur**, c'est-à-dire l'utilisation des données dans un but incompatible avec la finalité déterminée initialement, n'est possible que dans des conditions strictes [article 5, paragraphe 1, point b), du RGPD, et article 4, paragraphe 1, point b), de la directive (UE) 2016/680][105]. La finalité visée doit être formulée de manière suffisamment précise pour que la personne concernée soit en mesure d'envisager la finalité pour laquelle ses données feront l'objet d'un traitement[106]. Étant donné que les TRF comportent un risque important de «détournement d'usage»[107], les systèmes et processus associés devraient inclure des garanties, telles qu'une architecture compartimentée, afin de prévenir leur utilisation pour des finalités non autorisées[108]. Même si l'accès visé était inclus dans le champ

---

101 Voir Kramer, P., «Artikel 5 DSGVO» dans Eßer, M., et al. (2020), *Auernhammer DSGVO BDSG*, point 15; Herbst, T., «Artikel 5 DS-GVO», dans Kühling, J., et Buchner, B. (2018), DS-GVO BDSG, point 17.

102 Voir Malgieri, G. (janvier 2020), «The concept of fairness in the GDPR», *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. De même, Herbst, T., «Artikel 5 DS-GVO», dans Kühling, J., et Buchner, B. (2018), *DS-GVO BDSG*, point 17.

103 Voir Hacker, P. (2018), «Teaching fairness to artificial intelligence», *Common Market Law Review*, vol. 55, nº 4, p. 1172-1173; Malgieri, G. (janvier 2020), *The concept of fairness in the GDPR*, p. 163; CIPL (février 2020), *Report on Artificial Intelligence and Data Protection: Hard Issues and Practical Solutions*, p. 6-12.

104 Voir *Hambacher Erklärung zur Künstlichen Intelligenz* (3 avril 2019), DSK, p. 3-4; Pour plus d'informations sur le RGPD en tant que loi anti-discrimination et ses limites, voir Hacker, P. (2018), p. 1170-1185; Voir également Zuiderveen Borgesius, F. (2018), *Discrimination, intelligence artificielle et décisions algorithmiques*, Conseil de l'Europe, p. 21-25.

105 Pour plus d'informations, voir comité européen de la protection des données (2020), *Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par défaut*, p. 19-20; Voir groupe de travail «Article 29», *Opinion 03/2013 on purpose limitation* (non approuvé par le comité européen de la protection des données), et Agence des droits fondamentaux de l'Union européenne (2018), *Manuel de droit européen en matière de protection des données*, 2018, p. 12-125.

106 Conclusions de l'avocat général Kokott, J. (18 juillet 2007), dans l'affaire C-275/06, Promusicae, CJUE, point 53.

107 Voir Houwing, L. (2020), «Stop the Creep of Biometric Surveillance Technology», *European Data Protection Law Review*, vol. 6, nº 2. Pour des exemples de détournement d'usage dans des contextes liés aux activités répressives, voir Agence des droits fondamentaux de l'Union européenne (2018), *Under watchful eyes — biometrics, EU IT-systems and fundamental rights*, p. 61 et 66.

108 Voir Agence des droits fondamentaux de l'Union européenne (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, p. 21-23. Voir également comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 21; Agence

d'application de la finalité légitime, le principe de proportionnalité (voir encadré 2) et la sécurité des données peuvent restreindre ultérieurement les conditions d'accès et nécessiter des garanties, notamment si un soupçon raisonnable est établi, si les possibilités de recherche sont limitées et/ou si des systèmes en cascade (superposition de mesures, à commencer par la moins intrusive) ont été mis en place[109].

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

Le principe de **minimisation des données** est généralement interprété comme signifiant que la quantité de données devrait être limitée (RGPD) à ce qui est nécessaire ou non excessive (LED) au regard des finalités pour lesquelles elles sont traitées [article 5, paragraphe 1, point c), du RGPD, et article 4, paragraphe 1, point c), de la directive (UE) 2016/680]. Selon des autorités de protection des données et des analystes, cela englobe l'anonymisation des données lorsque cela est possible[110]. L'autorité française de protection des données, par exemple, a considéré que le déploiement d'un système de contrôle des accès fondé sur la reconnaissance faciale au sein des établissements scolaires constituait une violation des principes de proportionnalité et de minimisation des données, étant donné que les objectifs de réduction de la durée des contrôles et de sécurisation de l'entrée pourraient avoir été atteints par des moyens moins intrusifs, par exemple, par un système de badge[111]. Le contrôleur européen de la protection des données (CEPD) constate que les systèmes de TRF pourraient ne pas être conformes au principe de minimisation des données[112].

Tant le RGPD que la directive «police» intègrent le principe de **limitation de la conservation**. Le principe énonce que les données ne devraient pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles les données à caractère personnel sont traitées [article 5, paragraphe 1, point e), du RGPD, et article 4, paragraphe 1, point e), de la directive (UE) 2016/680][113]. Plusieurs organismes de protection des données ont publié des avis sur les limitations de conservation concernant les données issues d'enregistrements vidéo au titre du RGPD. Par exemple, les images de surveillance à des fins de détection d'actes de vandalisme devraient être détruites, idéalement automatiquement, au bout de quelques jours. «Plus la durée de conservation fixée est longue (notamment lorsqu'elle dépasse 72 heures), plus il convient de développer le raisonnement

---

des droits fondamentaux de l'Union européenne (2018), *Under watchful eyes — biometrics, EU IT-systems and fundamental rights*, p. 59-62 et p. 66.

109 Voir Agence des droits fondamentaux de l'Union européenne (2018), *Under watchful eyes — biometrics, EU IT-systems and fundamental rights*, p. 64-68 en référence à l'arrêt rendu par la CJUE le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, Digital Rights Ireland et Seitlinger e.a., point 51.

110 *Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen* (17 juillet 2020), DSK, p. 10; voir comité européen de la protection des données (2020), *Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par défaut*, p. 21-23.

111 Commission nationale de l'informatique et des libertés (2019), *Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position*. Dans sa décision dans l'affaire nº 1901249 du 27 février 2020, le tribunal administratif de Marseille a annulé la décision du conseil régional Provence-Alpes-Côte d'Azur dans la mesure où celui-ci a lancé l'expérimentation du dispositif de contrôle d'accès basé sur des TRF au sein des lycées «Ampère» (Marseille) et «Les Eucalyptus» (Nice), au motif que le traitement visé des données biométriques ne relevait pas des exceptions au titre de l'article 9, paragraphe 2, du RGPD, rendant la décision du conseil régional illégale (voir point 13).

112 CEPD (2019), *Facial recognition: A solution in search of a problem?* Pour plus d'informations sur les tensions entre les technologies et le principe de minimisation des données, voir Roßnagel, A., «Artikel 5 DSGVO», dans Simits, S., *et al.* (2019), *Datenschutzrecht*, Nomos, points 133-135.

113 La directive «police» exige que les États membres fixent des délais précis de conservation et d'examen [article 5 de la directive (UE) 2016/680], voir groupe de travail «Article 29» (29 novembre 2017), *Avis sur certaines questions clés de la directive (UE) 2016/680 (directive «police»)* (non approuvé par le comité européen de la protection des données), p. 3-6.

justifiant la légitimité de la finalité poursuivie et le caractère nécessaire de la conservation»[114]. En principe, trois jours, c'est-à-dire 72 heures, suffisent à déterminer si les données enregistrées doivent être conservées plus longtemps, tandis que les éléments superflus peuvent être supprimés[115]. Les données peuvent être conservées plus longtemps si des finalités de surveillance particulières s'appliquent[116]. Selon le comité européen de la protection des données, «les responsables du traitement doivent s'assurer que les données extraites d'une image numérique pour construire un modèle ne sont pas excessives et ne contiennent que les informations nécessaires à l'accomplissement de la finalité spécifiée, de manière à éviter tout traitement ultérieur éventuel»[117]. De plus, selon la finalité, une fois qu'un modèle facial a été généré, il se peut qu'il soit nécessaire de supprimer les données brutes sous-jacentes[118].

Le principe d'**exactitude des données** exige que les données soient exactes factuellement et temporellement [article 5, paragraphe 1, point d), du RGPD, et article 4, paragraphe 1, point d), de la directive (UE) 2016/680]. Il en résulte que certaines données doivent être tenues à jour. «[L]e caractère exact et complet de données à caractère personnel doit être apprécié au regard de la finalité pour laquelle ces données ont été collectées»[119]. En outre, certaines erreurs insignifiantes peuvent ne pas retentir sur leur exactitude (par exemple, un seul point de données erronées sur un million dans un génome séquencé qui pourrait tout de même servir d'identificateur biométrique)[120]. L'Agence des droits fondamentaux de l'Union européenne considère que «l'exactitude est généralement interprétée comme la justesse des données à caractère personnel d'une personne (par exemple, le fait de savoir si l'âge d'une personne dans la base de données est correct), toutefois le terme "exactitude" pourrait être interprété plus largement»[121]. Selon les lignes directrices du Conseil de l'Europe sur la reconnaissance faciale, les développeurs «devront éviter les erreurs d'étiquetage en testant suffisamment leurs systèmes et en identifiant et éliminant les disparités dans la précision, notamment en ce qui concerne les variations démographiques de la couleur de la peau, l'âge et le sexe, et éviter ainsi toute discrimination involontaire»[122]. Les responsables du traitement ou les sous-traitants auraient besoin de vérifier la qualité des images et des modèles biométriques insérés dans les listes de surveillance afin de prévenir de fausses correspondances éventuelles, étant donné que des images de faible qualité peuvent entraîner une augmentation du nombre d'erreurs[123]. Dans ses lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, le groupe de travail «Article 29» semble suggérer que, même lorsque des déductions erronées sont tirées de données brutes exactes par l'utilisation de l'intelligence artificielle, cela peut constituer une violation du principe d'exactitude des données (ce qui est

---

114 Comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 28.

115 DSK (2020), *Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen*, p. 22-23. Voir également *Videoüberwachung auf Bahnhöfen*, site internet du Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

116 Voir DSK (2020), *Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen*, p. 22-23.

117 Voir comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 21.

118 Ibid.

119 Arrêt rendu par la CJUE le 20 décembre 2017 dans l'affaire C434/16, Nowak, point 53.

120 Hallinan, D., et Borgesius, F. (2020), «Opinions can be incorrect (in our opinion)!On data protection law's accuracy principle», *International Data Privacy Law*, vol. 10, nº 1.

121 Voir Agence des droits fondamentaux de l'Union européenne (2019), *Data quality and artificial intelligence — mitigating bias and error to protect fundamental rights*, p. 9.

122 Conseil de l'Europe (2021), *Lignes directrices sur la reconnaissance faciale*, p. 9.

123 Ibid, p. 12-13. De plus, «[e]n cas de fausses correspondances, les entités prendront toutes les mesures raisonnables pour les corriger à l'avenir et garantir l'exactitude des images numériques et des modèles biométriques».

discutable)[124]. Par conséquent, ce principe exigerait non seulement des données d'entrée exactes[125], mais aussi que les algorithmes soient entraînés sur un ensemble de données représentatif et qu'ils contiennent le moins de biais dissimulés possible[126]. Cet aspect normatif demeure incertain et contestable.

Conformément au **principe de sécurité des données**, les données doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées [article 5, paragraphe 1, point f), du RGPD, et article 4, paragraphe 1, point f), de la directive (UE) 2016/680]. L'article 32 du RGPD et l'article 29 de la directive (UE) 2016/680 disposent (indirectement) que le responsable du traitement et le sous-traitant devraient mettre en place des mesures techniques et organisationnelles proportionnées qui empêchent la divulgation de données à caractère personnel à des personnes ou à des organes non autorisés, ainsi que leur accès à ces données. Le comité européen de la protection des données suggère que le responsable du traitement soit tenu de protéger le système et les données à toutes les étapes du traitement, à savoir lors de la conservation, de la transmission et du traitement[127]. À cette fin, le responsable du traitement prend les mesures suivantes: compartimentation des données lors de la transmission et de la conservation, enregistrement des modèles biométriques et des données brutes ou données d'identité dans des bases de données distinctes, chiffrement des données biométriques, notamment des modèles biométriques, et définition d'une politique de chiffrement et de gestion des clés, intégration d'une mesure organisationnelle et technique pour la détection des fraudes, attribution d'un code d'intégrité aux données (par exemple, signature ou code de hashage) et interdiction de tout accès extérieur aux données biométriques. Ces mesures devront évoluer avec l'avancement des technologies[128]. Le Conseil de l'Europe adopte une approche plus générale, mais indique précisément la nécessité de «mesures pour prévenir les attaques spécifiques aux technologies, y compris les attaques de présentation et les attaques de morphing»[129].

Conformément au **principe de responsabilité**, le responsable du traitement est tenu de démontrer le respect des principes de traitement des données à caractère personnel [article 5, paragraphe 2, du RGPD, et article 4, paragraphe 4, de la directive (UE) 2016/680][130]. À cette fin, le responsable du traitement doit mettre en place des mesures techniques et organisationnelles appropriées [considérant 84 et article 24 du RGPD, et considérant 53 et article 19 de la directive (UE) 2016/680]. Lorsque le responsable du traitement souhaite déployer des TRF, une **analyse d'impact relative à la protection des données**, comprenant une consultation préalable de l'autorité de protection des

---

124 Groupe de travail «Article 29» (2018), *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679*.

125 En ce qui concerne la gestion des données appropriée, voir Agence des droits fondamentaux de l'Union européenne (2018), *Under watchful eyes — biometrics, EU IT-systems and fundamental rights*, p. 81-97.

126 Concernant les biais, voir Hildebrandt, M., «The Issue of Bias. The Framing Powers of Ml», dans Pelillo, M., et Scantamburlo, T. (2020), *Machine Learning and Society: Impact, Trust, Transparency*; Agence des droits fondamentaux de l'Union européenne (30 mai 2018), *#BigData: Discrimination in data-supported decision making*.

127 Voir comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 28-32; voir également DSK (17 juillet 2020), *Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen*, p. 21.

128 Voir comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 21.

129 Voir Conseil de l'Europe (2021), *Lignes directrices sur la reconnaissance faciale*, p. 13.

130 Pour plus d'informations, voir Agence des droits fondamentaux de l'Union européenne (2018), *Manuel de droit européen en matière de protection des données*, Office des publications de l'Union européenne, p. 135-137.

données, sera très probablement[131] requise [articles 35 et 36 du RGPD et articles 27 et 28 de la directive (UE) 2016/680]. Celle-ci devrait consister en une analyse complète de l'admissibilité juridique et des risques associés à la mise en place des TRF[132]. D'autres mesures de responsabilité incombant aux responsables du traitement comprennent la **tenue d'un registre des activités de traitement** [article 30 du RGPD et article 24 de la directive (UE) 2016/680], la **documentation des violations de données** [article 33, paragraphe 5, du RGPD et article 30, paragraphe 5, de la directive (UE) 2016/680] et **la mise en œuvre de mesures techniques et organisationnelles appropriées** [article 24 du RGPD et article 19 de la directive (UE) 2016/680]. Il s'agit d'outils importants en matière de responsabilité, car ils aident les responsables du traitement à se conformer aux exigences, mais aussi à démontrer que des mesures appropriées ont été prises afin de garantir la conformité.

3.3. Cadre de non-discrimination

3.3.1. Cadre anti-discrimination de l'Union

Comme l'ont démontré plusieurs études, la discrimination présente un facteur-risque considérable associé au déploiement des TRF (voir section 2 ci-dessus)[133]. Étant donné que le cadre de non-discrimination de l'Union s'applique largement aux opérateurs publics et privés des systèmes de TRF basés sur l'IA, leurs conséquences et leur conformité doivent faire l'objet d'un examen. Au sein de l'Union, le droit à la non-discrimination est consacré dans le droit primaire et dans le droit dérivé, et s'applique aux décisions algorithmiques. Une discrimination survient lorsqu'une personne ou un groupe est traité moins favorablement qu'un(e) autre, sur la base de certaines caractéristiques personnelles ou, en d'autres termes, sur la base de «motifs protégés» juridiquement, qui ne peuvent pas servir de base en vue d'un traitement différencié (par exemple, sexe, race et handicap). Une discrimination dans les décisions algorithmiques peut découler, entre autres, de données d'apprentissage non représentatives, de biais dans les programmes d'étiquetage des données, et de fonctions mathématiques erronées/inappropriées[134].

Au **niveau du droit primaire**, les règles en matière de non-discrimination sont établies tout particulièrement à l'article 2 du traité sur l'Union européenne (traité UE), à l'article 10 du traité sur le fonctionnement de l'Union européenne (traité FUE), aux articles 20 et 21 de la charte, et en tant que principe général dans la jurisprudence. L'article 21 de la charte intègre la non-discrimination dans le cadre des règles de fond. Le domaine couvert va au-delà de la portée personnelle et matérielle de la législation dérivée en matière de non-discrimination, car la disposition est neutre du point de vue

---

131 Voir Agence des droits fondamentaux de l'Union européenne (2019), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, p. 26; voir également Information Commissioner's Office (2019), *Opinion on the use of live facial recognition technology by law enforcement in public places*, p. 13-14; comité européen de la protection des données (2020), *Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo*, p. 33.

132 Les autorités policières ont pris des initiatives importantes lors des essais de TRF, voir South Wales Police (11 octobre 2018), *DPIA for Automated Facial Recognition*; Metropolitan Police Service (10 février 2020), *DPIA for Live Facial Recognition*, 01/DPA/20/000467. Voir également Conseil de l'Europe, *Lignes directrices sur la reconnaissance faciale*, ci-dessus, p. 10 et p. 13-15; Castelluccia, C. et Inria, D. (2020); voir Kaminski, E., et Malgieri, G. (2020), «Algorithmic impact assessments under the GDPR: producing multi-layered explanations», *International Data Privacy Law*.

133 Pour une introduction, voir Leslie, D. (2020). Pour des exemples, voir Gerards, J., et Xenidis, R. (2021), *Algorithmic discrimination in Europe*, Commission européenne, p. 84, 86, 88 et 114.

134 Voir Agence des droits fondamentaux de l'Union européenne (2019), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, p. 27; Voir Agence des droits fondamentaux de l'Union européenne (2018), *#BigData: Discrimination in data-supported decision making*, p. 3-5; Hildebrandt, M., «The Issue of Bias. The Framing Powers of Ml», dans Pelillo, M., et Scantamburlo, T. (2019), *Machine Learning and Society: Impact, Trust, Transparency*, MIT Press.

sectoriel et contient une liste non exhaustive (théoriquement ouverte) de «motifs protégés». Si la portée de l'article 21 de la charte chevauche celle de la législation dérivée, la CJUE s'abstient souvent[135] de mentionner l'article 21 de la charte et applique la logique établie dans les directives (voir ci-après). Dans d'autres cas, la Cour «confirme plus fermement son raisonnement dans le libellé de la charte»[136]. En raison de sa formulation ouverte et de sa large portée, l'article 21 de la charte semble en théorie apte à s'attaquer aux cas de **discrimination algorithmique**.

Au **niveau du droit dérivé**, les lois anti-discrimination les plus pertinentes comprennent la directive 2000/43/CE relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique, la directive 2000/78/CE portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail, la directive 2004/113/CE mettant en œuvre le principe de l'égalité de traitement entre les femmes et les hommes dans l'accès à des biens et services et la fourniture de biens et services, et la directive 2006/54/CE relative à la mise en œuvre du principe de l'égalité des chances et de l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail (refonte). L'interdiction de discrimination en vertu de ces directives s'étend à trois domaines d'action: l'emploi, le système de protection sociale et l'accès aux biens et services (et leur fourniture). Toutefois, les motifs protégés ne sont pas homogènes, ce qui donne lieu à une «hiérarchie des motifs» et à une protection inégale[137]. Une directive anti-discrimination transversale, qui vise à combler les lacunes persistantes, est bloquée au Conseil depuis 2008[138]. Cela mis à part, la législation dérivée contraignante suit dans une large mesure une logique homogène, qui opère une distinction entre la discrimination directe et la discrimination indirecte. La règle ou pratique en question est considérée comme une «**discrimination directe**» lorsque celle-ci opère une distinction explicite fondée sur le «motif protégé» ou un facteur non dissociable de ce dernier, et qui ne peut être justifiée que dans des conditions strictes[139]. À l'inverse, un traitement apparemment neutre (règle, critère ou pratique neutre), qui désavantage considérablement un groupe, serait considéré comme une «**discrimination indirecte**» et pourrait dès lors être justifié de manière plus flexible[140]. La

[135] Voir Ward, A. (2018), «The Impact of the EU Charter of Fundamental Rights on Anti-Discrimination Law: More a Whimper than a Bang», *Cambridge Yearbook of European Legal Studies*, vol. 20, p. 42-53; Eklund, H., et Kilpatrick, C., «Article 21», dans Peers, S., *et al.* (à venir), The EU Charter of Fundamental Rights: A Commentary, Hart Publishing, points 21.65-21.69; Muir, E. (2019), «The Essence of the Fundamental Right to Equal Treatment», *German Law Journal*, vol. 20, nº 6, p. 827-829.

[136] Voir Muir, E. (2019), p. 833-838 (discussion sur les «cas qui présentent des lacunes»). Eklund, H., et Kilpatrick, C., «Article 21», dans Peers, S., *et al.* (à venir), *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, points 21.61-21.64.

[137] Pour une perspective graphique, voir *EU anti-discrimination law*, Academy of European Law, p. 11; *Algorithmic discrimination in Europe* (2021), Direction générale de la justice et des consommateurs, Commission européenne, p. 55; Xenidis, R. (avril 2017), *Shaking the normative foundations of EU equality law*, documents de travail juridiques de l'EUI, p. 23-32; Xenidis, R. (avril 2017), *Algorithmic discrimination in Europe* (2021), direction générale de la justice et des consommateurs, Commission européenne, p. 53-62; Hacker, P. (2018), «Teaching fairness to artificial intelligence», *Common Market Law Review*, vol. 55, nº 4, p. 1154-1157.

[138] Fiche de procédure 2008/0140(APP), observatoire législatif du Parlement européen; pour plus d'informations, voir *Anti-Discrimination Directive*, calendrier du train législatif, EPRS, Parlement européen.

[139] De tels actes peuvent être justifiés sur la base, par exemple, d'exigences professionnelles véritables [article 14, paragraphe 2, de la directive 2006/54/CE relative à la mise en œuvre du principe de l'égalité des chances et de l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail (refonte), article 4 de la directive 2000/43/CE relative à la mise en œuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique, article 4, paragraphe 1, de la directive 2000/78/CE portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail], d'exceptions liées aux institutions religieuses (article 4, paragraphe 2, de la directive 2000/78/CE), et d'exceptions spécifiques à la discrimination fondée sur l'âge (article 6 de la directive 2000/78/CE).

[140] De tels actes peuvent être justifiés s'ils (i) servent une finalité légitime, s'ils (ii) promeuvent effectivement cette finalité légitime, et s'ils (iii) sont nécessaires/proportionnés.

discrimination indirecte diffère principalement de la discrimination directe en ce qu'elle déplace l'attention d'un traitement différencié aux effets différenciés, et en ce que, pour cette raison, elle peut être justifiée plus facilement. Dans les contextes d'apprentissage automatique, la discrimination directe serait moins fréquente que la discrimination indirecte, voire rare[141]. Il semblerait que «[l]a discrimination indirecte englobe un large éventail de sorties algorithmiques d'apparence neutres, mais [en réalité] discriminatoires [...]»[142].

3.3.2. Lacunes dans le cadre anti-discrimination de l'Union

Toutefois, de nombreux chercheurs considèrent que le cadre anti-discrimination actuel de l'Union n'offre pas une protection suffisante contre la discrimination algorithmique. Ils affirment, par exemple, que la législation anti-discrimination de l'Union souffre d'un «problème d'application généralisé»[143] et que la discrimination algorithmique «exacerbe la faiblesse de l'approche axée sur la justice individuelle»[144]. Le domaine couvert par la **législation dérivée** semble indûment restreint et certaines exigences présentent des seuils trop élevés pour obtenir une protection. Mises à part les lacunes existantes dans la législation dérivée de l'Union en matière de lutte contre les discriminations[145] ainsi que dans les actions en justice engagées individuellement[146], les algorithmes peuvent soumettre de nouveaux segments de la population à un traitement différencié qui ne relève pas des motifs préexistants des directives anti-discrimination de l'Union[147]. Bien que déloyaux et problématiques, ces cas ne seraient pas interdits par le droit dérivé. Un chercheur prétend que «la législation de l'Union en matière de lutte contre les discriminations [...] permet de justifier aisément» certaines formes de discrimination algorithmique[148]. Bien que le **droit fondamental à la non-discrimination** puisse constituer une mesure palliative[149], il ne s'applique que lorsque les institutions, organismes, bureaux et agences de l'Union prennent des mesures ou lorsque le droit de l'Union est mis en œuvre par les États membres (article 51 de la charte), son applicabilité aux litiges entre entités privées est incertaine[150], et en s'appuyant sur la jurisprudence, il pourrait s'avérer

---

141 Voir Commission européenne (2021), *Algorithmic discrimination in Europe*, p. 67-73; Xenidis, R. (avril 2017), et Senden, L., «EU non-discrimination law in the era of artificial intelligence: mapping the challenges of algorithmic discrimination», dans Bernitz, U., *et al.* (2020), *General principles of EU law and the EU digital order*, Kluwer Law International, p. 19; Wachter, S., *et al.* (3 mars 2020), *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*», p. 41, 44-45; Hacker, P. (2018), «Teaching fairness to artificial intelligence», *Common Market Law Review*, vol. 55, nº 4, p. 1151.

142 Voir Xenidis, R., et Senden, L., ci-dessus, p. 20-21; Voir Hacker, P., ci-dessus, p. 1154-1160 (en référence à la portée matérielle et personnelle des directives).

143 Hacker, P. (2018), *Teaching fairness to artificial intelligence*, p 1167-1168.

144 Xenidis, R., et Senden, L. (2017), p. 26.

145 Notamment «le manque de clarté et l'insécurité qui en découle pour les requérants» et le niveau de protection inégal offert par le droit dérivé de l'Union («hiérarchie des motifs»).

146 Xenidis, R., et Senden, L. (2017), p. 25: «La recherche comparative sur l'application de la législation en matière d'égalité entre les hommes et les femmes dans les États membres de l'Union révèle une multitude d'autres problèmes persistants qui dissuadent les personnes d'intenter une action en justice pour protéger leur droit à l'égalité. Ceux-ci vont des problèmes institutionnels (par exemple, la durée des procédures, le manque d'expertise et d'assistance, le manque de confiance dans le système judiciaire, l'insuffisance des indemnisations), aux problèmes financiers (par exemple, le coût des procédures, le manque d'aide juridique), en passant par une incertitude concernant les résultats et la crainte de la victimisation, par l'employeur, la famille et la société».

147 Voir Zuiderveen Borgesius, F. (2018), p. 36; de même, Wachter, S., *et al.* (3 mars 2020), *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*», p. 11-12, et divers autres.

148 Hacker, P. (2018), p. 1164-1165; Pour un point de vue opposé, voir Xenidis, R., et Senden, L. (2017), p. 22.

149 Gerards, J., et Zuiderveen Borgesius, F. (à venir, 2021), «Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence», *Colorado Technology Law Journal*, p. 12-13.

150 Pour de plus amples informations, voir *Explications relatives à la Charte des droits fondamentaux* (14 décembre 2007), praesidium de la Convention européenne, Explication ad article 21; Ward, A. (2018), «The Impact of the EU Charter of

moins flexible et transversal que prévu[151]. De plus, des analystes ont recensé un «pêle-mêle de justifications» et un «chassé-croisé de méthodes» dans la jurisprudence et avertissent que le manque de cohérence «atténue» les effets de l'article 21 de la charte et «fait du tort aux personnes que [la charte] vise à protéger»[152].

Même si le champ d'application de la législation anti-discrimination de l'Union était étendu afin d'englober les discriminations sous diverses formes et dans différents domaines d'application de l'IA, celle-ci resterait probablement inefficace contre la discrimination algorithmique. La majorité des chercheurs conviennent que les victimes de discrimination en matière d'intelligence artificielle seraient confrontées à de profonds **problèmes pour détecter et prouver (prima facie) la discrimination**. En raison de l'absence de points de référence (comparatifs) et «des vitesses, de l'échelle et des niveaux de complexité qui défient l'entendement», les décisions algorithmiques peuvent sembler légitimes et la victime peut, dans un premier temps, ne pas s'apercevoir de la discrimination[153]. Même si la victime soupçonne une discrimination, la preuve des décisions algorithmiques incombe à l'opérateur ou au fournisseur, et est dès lors probablement inaccessible pour la victime[154]. Les contrôleurs de système peuvent, par exemple, invoquer leurs droits de propriété intellectuelle et leurs secrets commerciaux en tant que motifs de refus d'accès[155]. Cependant, il convient de noter que les tribunaux peuvent considérer le refus de fournir l'accès en tant que facteur dans le contexte de «l'établissement des faits à partir desquels on peut présumer qu'il y a eu une discrimination directe ou indirecte»[156]. Néanmoins, sans connaissance, au minimum, des résultats algorithmiques, la victime ferait face à des difficultés particulières pour déterminer les groupes de comparaison, prouver les disparités statistiques et réfuter les justifications. Enfin, même si la victime et son conseiller juridique étaient en mesure d'obtenir l'accès, les algorithmes sont difficilement intelligibles pour des non-experts tels que les victimes, juges et législateurs[157]. Certaines formes d'intelligence artificielle sont même généralement «non décomposables» (**phénomène de la «boîte noire»**) et défie tout raisonnement fondé sur le bon sens, empêchant ainsi la détection de décisions discriminatoires ou la compréhension de la fonctionnalité

Fundamental Rights on Anti-Discrimination Law: More a Whimper than a Bang», *Cambridge Yearbook of European Legal Studies*, vol. 20, p. 53-56; En ce qui concerne l'effet horizontal de la charte des droits fondamentaux de l'Union européenne en général, voir Frantziou, E. (2020) «The Horizontal Effect of the Charter», *Cambridge Yearbook of European Legal Studies*, vol. 22. En ce qui concerne l'effet horizontal des dispositions anti-discrimination dans les constitutions des États membres, voir Chopin, I., et Germaine, C. (2019), *A comparative analysis of non-discrimination law in Europe 2019*, Commission européenne, p. 11.

151 Ward, A. (2018), p. 35-39; Voir Gerards, J., et Xenidis, R. (2017), p. 65.

152 Ward, A. (2018), p. 56; Voir Eklund, H., et Kilpatrick, C., «Article 21», dans Peers, S., *et al.* (à venir), *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, point 21.74; Muir, E. (2019), «The Essence of the Fundamental Right to Equal Treatment», *German Law Journal*, vol. 20, nº 6, p. 831-833.

153 Wachter, S., *et al.* (3 mars 2020), *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*», p. 6 et 10; Hacker, P. (2018), p. 1169; voir Gerards, J., et Xenidis, R. (2017), p. 75.

154 Xenidis, R., et Senden, L. (2017), p. 20 et 24 (en référence aux arrêts rendus par la CJUE dans les affaires Meister et Danfoss). Hacker, P. (2018), p. 1169-1170; voir Gerards, J., et Xenidis, R. (2017), p. 75.

155 Wachter, S., *et al.* (2020), p. 10.

156 Arrêt rendu par la CJUE le 19 avril 2012 dans l'affaire C-415/10, Meister, point 47; Hacker, P. (2018), p. 1170, soutient qu'«il y a peu d'espoir qu'un refus de fournir l'accès à des données de sortie aboutisse à une indication claire de présomption de discrimination. Même si ce n'était pas le cas, [...] un tel refus contribue uniquement à établir une présomption, et non pas à réfuter la justification du modèle algorithmique» (voir point précédent).

157 Voir Gerards, J., et Xenidis, R. (2017), p. 75.

technique[158]. Les déficits d'application qui en résultent peuvent dégénérer en un affaiblissement des mesures incitatrices au respect de la conformité[159].

3.3.3. Options pour combler les lacunes en matière de protection

Afin de remédier à ce manque de transparence et de relever les défis que pose l'application, les chercheurs recommandent différentes mesures. Certains proposent une innovation législative, tandis que d'autres s'appuient sur l'exploitation du cadre existant au moyen de l'interprétation. Selon certains analystes, «les législateurs nationaux devraient conserver ou introduire des dispositions générales en matière de non-discrimination qui peuvent agir comme un filet de sécurité», pour les cas où un traitement différencié ne relève pas de la législation anti-discrimination générale (article 21 de la charte), ou spécifique, mais semble déloyal et problématique[160]. À défaut, les règles spécifiques au secteur pour la prise de décision liée à l'IA peuvent constituer une solution viable (voir section 4 ci-dessous)[161]. Un autre chercheur mentionne des instruments législatifs viables pour combler les lacunes, tels que les droits à l'accès et à l'information, l'application par les pouvoirs publics et le recours collectif, mais affirme qu'il est peu probable que le législateur prenne des mesures, notamment eu égard à la directive anti-discrimination horizontale actuellement bloquée au Conseil[162]. Au lieu de cela, le chercheur préconise de tirer profit du RGPD, notamment les droits d'accès des personnes concernées, les règles d'analyse d'impact de la protection des données, le principe de loyauté et les instruments d'application par les pouvoirs publics[163]. D'autres analystes ont élaboré un outil statistique qui permet de détecter et d'évaluer une éventuelle discrimination et qui présenterait dès lors un intérêt pour les juges, pour les requérants et pour les organismes de réglementation, ainsi que pour les opérateurs, pour les fournisseurs et pour les fabricants (par exemple, pour corriger les biais à titre préventif)[164]. Enfin, les chercheurs considèrent l'«approche axée sur la justice individuelle», c'est-à-dire les actions en justice engagées individuellement, comme totalement inappropriée et suggèrent de se concentrer sur la mobilisation des organismes de contrôle de l'Union en matière d'égalité et de non-discrimination et sur la conception d'une approche fondée sur l'«égalité par nature»[165]. «En fonction de leur mandat, les organismes nationaux compétents en matière d'égalité pourraient également jouer un rôle important dans le soutien des plaintes individuelles, en intentant des recours collectifs et en

158 Voir Watcher, S., *et al.* (2020), p. 12; Gerards, J., et Xenidis, R. (2017), p. 75, considèrent qu'«il n'est pas nécessaire d'ouvrir la "boîte noire" algorithmique, mais uniquement de fournir une preuve prima facie».

159 Voir Hacker, P. (2018), p. 1169.

160 Voir Gerards, J., et Zuiderveen Borgesius, F. (à venir), p. 67; voir Gerards, J., et Xenidis, R. (2021), p. 141-142.

161 Voir Zuiderveen Borgesius, F. (2018), p. 69-70.

162 Voir Hacker, P. (2018), p. 1170-1171.

163 Voir Hacker, P. (2018), p. 1170-1185; sur le thème de la réglementation de l'IA via le RGPD, voir Discrimination, intelligence artificielle et décisions algorithmiques (2018), étude du Conseil de l'Europe, p. 21-25 et Mazzini, G., «A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law», dans De Franceschi A., et Schulze, R. (2019), *Digital Revolution — New challenges for Law*, C.H. Beck and Nomos, p. 34-53.

164 Wachter, S., *et al*. (3 mars 2020), *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, p. 44-72; à la note de bas de page 305, ils demandent implicitement que «les données soient collectées et conservées à des fins d'évaluation statistique».

165 Voir Xenidis, R., et Senden, L. (2020), p. 26-29; voir Zuiderveen Borgesius, F. (2018), p. 66, qui insiste sur la nécessité d'octroyer un financement approprié aux organismes chargés de l'égalité et aux autorités de protection des données, et de les doter de suffisamment de pouvoirs d'enquête et d'exécution: «Sans application de la loi, la transparence ne mènera pas nécessairement à la responsabilité».

portant le problème à l'attention du législateur»[166]. En outre, les analyses d'impact pourraient être «davantage élaborées comme des outils de détection et d'application, au-delà de la protection des données dans le domaine de l'égalité et de la non-discrimination», et des agences de certifications pourraient être promues[167]. Enfin, une approche intégrée, combinant des solutions juridiques, technologiques et fondées sur les connaissances, pourrait être adoptée[168].

3.4. Autre législation pertinente

Mis à part le cadre mentionné précédemment, les TRF doivent tenir compte des exigences au titre du droit de l'Union en matière de protection des **droits des enfants** et des **personnes âgées**, de la **liberté d'expression** et de la **liberté de réunion et d'association**, du **droit à une bonne administration**, ainsi que du **droit à un recours effectif**[169]. D'autres préoccupations soulevées par les composantes de l'IA des systèmes de TRF concernent la sécurité du produit, la fiabilité du produit et la protection des consommateurs[170]. Par ailleurs, il convient de prendre en considération un dispositif juridique croissant, au sein de l'Union, régissant les **contrôles aux frontières** dans le contexte des activités répressives.

Encadré 3 — IA et contrôles aux frontières

Un certain nombre de modifications des différents **systèmes d'information centralisés de l'Union sur les contrôles aux frontières** font l'objet de débats en vue de permettre le traitement des technologies de reconnaissance faciale à des fins de vérification ou d'identification. Il a été proposé d'intégrer les technologies de reconnaissance faciale automatique dans le **système d'information Schengen de l'Union** (SIS), le plus grand système d'échange d'informations et également le plus largement utilisé pour la sécurité et pour la gestion des frontières en Europe. En outre, les propositions en suspens de réviser la **base de données européenne des empreintes digitales** (Eurodac), qui appuie la mise en œuvre d'une législation européenne en matière d'asile, et le **système d'information sur les visas** envisagent la mise en place des technologies de reconnaissance faciale[171].

3.5 Principales conclusions

Le traitement des données biométriques au moyen de technologies de reconnaissance faciale influe profondément sur le droit des personnes en matière de protection des données et de respect de la vie privée, et son déploiement et sa réglementation sont soumis aux règles strictes de la charte, du RGPD et de la directive (UE) 2016/680. Bien que les exigences spécifiques eu égard à la protection des données continuent de prendre forme, la nature intrusive de ces technologies et l'opposition bruyante d'une grande diversité d'acteurs indiquent que les développeurs et les opérateurs ne devraient pas confondre incertitude et clémence. En définitive, l'acquis en matière de données de

166 Voir Xenidis, R., et Senden, L., ci-dessus, p. 27; concernant les pouvoirs des organismes chargés de l'égalité, voir Lantschner, E. (2020), «Strategic litigation», *European equality law review*, vol. 2020/1, et Kádár, T. (2019), «The legal standing of equality bodies», *European equality law review*, vol. 2019/1.

167 Voir Xenidis, R., et Senden, L., ci-dessus, p. 28.

168 Voir Gerards, J., et Xenidis, R., ci-dessus, p. 140-151.

169 Voir Agence des droits fondamentaux de l'Union européenne (2019), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, p. 28-32.

170 Voir Commission européenne (2021), *Impact Assessment accompanying the Proposal for an AI-framework*, p. 6-9; Mazzini, G. «A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law», dans De Franceschi A., et Schulze, R. (2019), *Digital Revolution — New challenges for Law*, C.H. Beck and Nomos, p. 2-34.

171 Pour un aperçu, voir Dumbrava, C. (juillet 2021), *Artificial intelligence at EU borders, Overview of applications and key issues*, analyse approfondie, EPRS, Parlement européen, p. 13-14.

l'Union exige que l'ensemble du système de reconnaissance faciale, incluant des composantes telles que des bases de données biométriques, des politiques de conservation des données, des procédures et des algorithmes de prise de décision, soit configuré de manière à préserver la vie privée et la protection des données. En outre, les chercheurs s'interrogent sur l'efficacité du cadre de l'Union en matière de non-discrimination face à la discrimination algorithmique associée aux systèmes de TRF. Les opérateurs de systèmes de TRF fondées sur l'IA doivent prendre des mesures organisationnelles et techniques appropriées en vue de réduire la discrimination algorithmique[172]. À l'inverse, les organismes de réglementation devraient prendre en considération le renforcement et l'étendue du cadre de l'Union en matière de non-discrimination, afin de veiller à ce que les opérateurs ne contournent pas la logique sous-jacente[173]. Ces questions liées aux droits fondamentaux constituent désormais des arguments pour une intervention réglementaire de l'Union en vue d'enrayer les risques associés aux applications de l'IA[174]. Selon l'étude de la Commission européenne intitulée «Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe», ces données biométriques de «deuxième vague» comportent des risques importants et sans précédent pour les droits fondamentaux, **et plus particulièrement pour le droit au respect de la vie privée et à la non-discrimination**[175].

4. Proposition de législation européenne relative à l'intelligence artificielle et reconnaissance faciale

4.1. Contexte

En février 2020, la **Commission européenne** a publié un *Livre blanc sur l'intelligence artificielle*[176], qui met en exergue les conséquences de l'utilisation des systèmes d'IA pour l'identification biométrique à distance, et en particulier des technologies de reconnaissance faciale au sein de l'Union sur les droits fondamentaux. Afin de prévenir toute violation des droits fondamentaux et d'éviter la fragmentation du marché intérieur, la Commission propose de déterminer les **circonstances spécifiques**, le cas échéant, qui pourraient justifier une telle utilisation, ainsi que les **garanties communes**. Le groupe d'experts de haut niveau sur l'IA de l'Union, qui se compose d'experts indépendants de l'Union issus de la sphère universitaire, de la société civile et de l'industrie, a demandé (i) une définition claire de si oui ou non, quand et comment l'IA peut être utilisée pour l'identification automatisée des personnes et (ii) une distinction entre l'identification d'une personne et la recherche et le suivi d'une personne, et entre la surveillance ciblée et la surveillance de masse[177]. Dans ce contexte, la Commission a mis en lumière les différents niveaux de précision

---

172 Wachter, S., *et al.* (3 mars 2020), *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*; MacCarthy, M. (6 décembre 2019), *Fairness in algorithmic decision-making*, Brookings.

173 Même si les tribunaux tentaient de combler les lacunes en matière de protection par une interprétation extensive du cadre juridique préexistant, des incertitudes et complexités juridiques persisteraient très longtemps. À moyen terme, cela pourrait favoriser un climat dans lequel les opérateurs dépassent la limite de la licéité, tandis que d'autres adoptent des stratégies prudentes et sont dissuadés par des analyses de cas légales. [De même, voir Commission européenne (2021), *Impact Assessment accompanying the Proposal for an AI-framework*, p. 23 et suiv.]

174 Voir Commission européenne (2021), *Impact Assessment accompanying the Proposal for an AI-framework*, p. 18-21; Voir Commission européenne (2021), *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*, p. 22-43.

175 Voir *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe* (2021), p. 39.

176 Voir Commission européenne, Livre blanc sur l'intelligence artificielle, COM(2020) 65 final.

177 Voir groupe d'experts indépendants de haut niveau sur l'intelligence artificielle (2019), *Lignes directrices en matière d'éthique pour une IA digne de confiance*, p. 33.

des systèmes de reconnaissance faciale, qui peuvent aboutir à des résultats discriminatoires et qui ont donné naissance à un scénario de réglementation de ces pratiques dans l'analyse d'impact annexée à la proposition de loi en matière d'IA[178].

Le **Parlement européen** a demandé à plusieurs reprises de poser des limites à l'utilisation de la reconnaissance faciale au sein de l'Union. Le Parlement a souligné que la collecte et l'utilisation de données biométriques à des fins d'identification à distance (comme la reconnaissance faciale) dans les espaces publics présentaient des risques particuliers pour les droits fondamentaux et a insisté sur le fait que ces technologies ne devraient être déployées et utilisées par les pouvoirs publics des États membres que pour des motifs d'intérêt public substantiels[179]. Le Parlement a également invité la Commission à **prendre en considération un moratoire sur l'utilisation de ces systèmes de reconnaissance faciale dans les espaces publics** par les pouvoirs publics et dans les établissements d'enseignement et de santé[180], et a appelé de ses vœux un **moratoire sur le déploiement des systèmes de reconnaissance faciale à des fins répressives**, jusqu'à ce que les normes techniques puissent être considérées comme pleinement conformes aux droits fondamentaux[181]. Certains législateurs ont exprimé leur souhait d'aller plus loin et d'appuyer **l'interdiction d'utiliser les technologies de reconnaissance faciale** dans des contextes particuliers. Par exemple, le Parlement a recommandé l'interdiction de l'identification biométrique automatisée, telle que la reconnaissance faciale, à des fins éducationnelles et culturelles (sauf dans les cas exceptionnels où la loi l'autorise)[182]. Selon le même raisonnement, un groupe de plus de 100 députés du Parlement a invité la Commission à consacrer une interdiction explicite de la surveillance biométrique de masse dans les lieux publics dans le droit de l'Union[183].

4.2. Proposition de loi relative à l'intelligence artificielle

4.2.1. Caractéristiques principales

En avril 2021, la Commission a dévoilé une nouvelle proposition de cadre réglementaire de l'Union sur l'IA[184]. Le cadre juridique est axé sur l'utilisation spécifique des systèmes d'IA et sur les risques associés. La Commission propose de consacrer **une définition technologiquement neutre des systèmes d'IA** dans le droit de l'Union et d'établir une **classification** pour les systèmes d'IA avec différentes exigences et obligations adaptées à une «**approche fondée sur les risques**».

178 Voir Commission européenne (2021), *Impact Assessment accompanying the Proposal for an AI-framework*, p. 19.

179 Voir Parlement européen, *Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes*, 2020/2012(INL).

180 Voir Parlement européen, *Résolution du Parlement européen du 20 janvier 2021 sur l'intelligence artificielle: questions relatives à l'interprétation et à l'application du droit international dans la mesure où l'Union est concernée dans les domaines des utilisations civiles et militaires ainsi qu'à l'autorité de l'État en dehors du champ d'application de la justice pénale*, 2020/2013(INI).

181 Voir Parlement européen, *Projet de rapport sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales*, 2020/2016(INI).

182 Voir Parlement européen, *Résolution du Parlement européen du 19 mai 2021 sur l'intelligence artificielle dans les domaines de l'éducation, de la culture et de l'audiovisuel*, 2020/2017(INI).

183 Voir la lettre des députés du Parlement à la Commission européenne (8 mars 2021).

184 Voir Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) modifiant certains actes législatifs de l'Union*, 2021/0106(COD). Voir Parlement européen, train législatif, *Proposal for a Regulation on a European approach for Artificial Intelligence*.

- Certaines **pratiques d'IA particulièrement néfastes sont interdites** en raison de leur caractère contraire aux valeurs de l'Union (article 5). Elles sont considérées comme une menace évidente pour la sécurité, pour les conditions de vie et pour les droits des personnes, et sont interdites en raison du «risque inacceptable» qu'elles engendrent. Celles-ci incluent les systèmes qui sont conçus pour manipuler le comportement humain par des techniques subliminales et la notation sociale de la part des gouvernements.
- Certains systèmes d'IA sont considérés comme «**IA à haut risque**», car ils créent des effets néfastes sur la sécurité des personnes ou sur leurs droits fondamentaux[185]. Ces systèmes dits «à haut risque» comprennent les technologies d'IA utilisées dans les infrastructures critiques (par exemple, les transports), l'enseignement ou la formation professionnelle, les composantes de sécurité des produits (par exemple, les applications d'IA dans la chirurgie assistée par robot), l'emploi, les services privés et publics essentiels (par exemple, l'évaluation du crédit qui empêche des citoyens d'obtenir un prêt), les activités répressives, la gestion de la migration, de l'asile et des contrôles aux frontières (par exemple, vérification de l'authenticité de documents de voyage) et l'administration de la justice et des procédures démocratiques. Un certain nombre de systèmes d'IA (tels que les systèmes biométriques) ont été précisément reconnus comme présentant un risque élevé et indiqués, en annexe III, dans une liste que la Commission devrait être habilitée à mettre à jour le cas échéant (article 7). Ces systèmes d'«IA à haut risque» devront faire l'objet d'une **évaluation de conformité** avant d'être mis sur le marché et répondre à une série d'**exigences en matière de sécurité** (concernant, par exemple, la gestion des risques, le contrôle humain et la gouvernance des données). Par ailleurs, **une surveillance et une supervision ex post du marché** doivent être mises en place afin de veiller à la conformité avec les obligations et les exigences pour tous les systèmes d'IA à haut risque déjà commercialisés (article 61).
- Les systèmes d'IA qui présentent un «**risque limité**» devraient être soumis à un ensemble limité d'obligations (par exemple, l'obligation de transparence).
- Tous les autres systèmes d'IA qui présentent un «**risque minime**» pourraient être mis au point et utilisés au sein de l'Union sans autre obligation légale que la législation existante.

4.2.2 Systèmes biométriques et reconnaissance faciale

Le projet de règlement adopte une position technologiquement neutre et vise à être aussi pérenne que possible, en prenant en considération les évolutions rapides des technologies et du marché liés à l'IA. À cette fin, le règlement s'appliquerait à tous les **systèmes d'identification biométrique à distance** — y compris les **technologies de reconnaissance faciale**. Tous ces systèmes opèrent à distance, sans savoir si la personne concernée sera présente dans une zone, enregistrent des données biométriques (notamment par la reconnaissance d'images faciales), comparent ces données avec un échantillon existant ou une base de données sans délai important et sont utilisés précisément pour identifier une personne[186].

4.2.2.1 Systèmes d'identification biométrique «en temps réel» et «a posteriori»

La Commission propose d'établir une distinction entre les systèmes d'identification biométrique à distance «en temps réel» et les systèmes d'identification biométrique à distance «a posteriori» et de

[185] L'article 6 du projet de règlement définit deux groupes de systèmes d'IA à haut risque: les systèmes d'IA qui sont des composantes de sécurité ou des produits qui relèvent d'une législation européenne harmonisée précise (par exemple, les jouets, les véhicules motorisés) et les systèmes d'IA autonomes qui présentent un risque élevé de préjudice pour la santé et la sécurité ou pour les droits fondamentaux des personnes (par exemple, les systèmes d'IA utilisés dans la circulation routière et l'enseignement).

[186] Voir considérant 8 et article 3, paragraphe 33, de Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) modifiant certains actes législatifs de l'Union, 2021/0106(COD).*

les soumettre à différentes séries de règles selon leur utilisation. Les **systèmes d'identification biométrique «en temps réel»** devraient être définis comme des systèmes en mesure d'enregistrer des données biométriques et d'exécuter les processus de comparaison et d'identification instantanément (ou sans délai important), sur la base d'éléments «en temps réel» ou «quasiment en temps réel», tels que des images vidéo, générés par une caméra ou par un autre dispositif. Quant aux **systèmes d'identification biométrique «a posteriori»**, il s'agirait de systèmes permettant l'enregistrement de données biométriques et l'exécution des processus de comparaison et d'identification après un délai important, sur la base d'images fixes ou d'images vidéo générées par des caméras de télévision en circuit fermé ou par des dispositifs privés. Dans ce contexte, différents scénarios de réglementation de la reconnaissance faciale peuvent être mis en évidence[187].

4.2.2.2. Scénarios de réglementation des TRF

i) Systèmes d'identification biométrique à distance en temps réel à haut risque à des fins répressives interdits

Par principe, la Commission propose d'interdire l'utilisation des systèmes d'IA pour l'**identification biométrique à distance «en temps réel»** de personnes physiques **dans des espaces accessibles au public** à des **fins répressives**[188]. Ces systèmes sont particulièrement intrusifs. Plusieurs portent atteinte aux droits et aux libertés des personnes concernées, touchent la vie privée d'une grande partie de la population, peuvent susciter un sentiment de surveillance constante et dissuader indirectement l'exercice de la liberté de réunion et d'autres droits fondamentaux de l'Union. En outre, l'immédiateté de l'identification à distance et les mécanismes de recours disponibles limités pour les individus engendrent des risques accrus pour les droits et les libertés des personnes concernées par les activités répressives[189]. Dans la pratique, l'avant-projet entend interdire l'utilisation des systèmes d'identification biométrique dans des espaces accessibles au public à des fins répressives dans des situations telles que lorsque les autorités policières déploient des **systèmes de reconnaissance faciale** en vue d'identifier des personnes qui participent à une **manifestation publique**, ou afin de localiser des personnes qui ont seulement commis des **infractions mineures**[190]. En raison de leur menace pour les droits fondamentaux et pour les valeurs de l'Union, ces systèmes de TRF devraient être considérés comme des **systèmes «à haut risque»** et faire l'objet d'une **interdiction générale** au sein de l'Union.

ii) Systèmes d'identification biométrique à distance en temps réel à haut risque à des fins répressives autorisés

Toutefois, **trois exceptions**[191], notamment lorsqu'un intérêt public important l'emporte sur les risques pour les droits fondamentaux, sont envisagées pour l'utilisation des systèmes d'identification biométrique à distance dans des espaces accessibles au public à des fins répressives. La première situation comprend la **recherche ciblée de victimes potentielles d'actes criminels**, notamment d'enfants disparus. La deuxième situation concerne la prévention d'une **menace**

---

187 Un autre scénario, non présenté ici, concerne la possibilité selon laquelle les systèmes de reconnaissance faciale relèvent des dispositions de l'article 53 de la proposition de règlement 2021/0106(COD), permettant aux «bacs à sable réglementaires» en matière d'IA de fournir un environnement contrôlé pour le développement, l'essai et la validation de systèmes d'IA innovants pendant une courte période avant leur mise sur le marché.

188 Voir article 5, paragraphe 1, point d); considérant 33 et annexe III, paragraphe 1, point a), de la proposition de règlement 2021/0106(COD).

189 Voir considérant 18 de la proposition de règlement 2021/0106(COD).

190 Voir Christakis, T., et Becuywe, M. (2021), *Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation*, European Law Blog.

191 Voir article 5, paragraphe 1, point d), de la proposition de règlement 2021/0106(COD).

spécifique, substantielle et imminente **pour la vie ou la sécurité physique** des personnes ou la prévention d'une **attaque terroriste**. La troisième situation a trait à la détection, à la localisation, à l'identification ou aux poursuites de l'auteur ou d'une personne soupçonnée d'avoir commis une **infraction pénale** dont il est fait état dans la décision-cadre relative au mandat d'arrêt européen[192]. Cette législation contribue à une procédure d'extradition rapide et efficace entre les États membres de l'Union de personnes ayant commis une **infraction grave**, et permettrait dès lors le traitement en temps réel des données biométriques, et notamment la reconnaissance faciale, dans des espaces publics[193].

Ces exceptions ont été établies, car l'utilisation de systèmes d'identification biométrique à distance dans des espaces publics pourrait être justifiée par des motifs importants de sécurité publique[194]. Cependant, le projet de règlement laisse le soin aux **États membres** de décider s'ils souhaitent ou non mettre en place les exceptions susmentionnées pour utiliser les systèmes d'identification biométrique à distance dans leurs législations nationales[195]. En réalité, la proposition de la Commission prend en considération le fait que les affaires de sécurité nationale relèvent dans une large mesure de la **compétence exclusive** des États membres et tente d'établir un équilibre entre, d'un côté, la sécurité nationale et l'ordre public et, de l'autre, la protection des données et autres droits fondamentaux que les systèmes d'identification biométrique à distance, comme la reconnaissance faciale, mettent à mal[196].

L'utilisation de ces systèmes d'identification biométrique à distance en temps réel serait toujours soumise au respect des principes consacrés dans le RGPD (voir section 3 précédente), ainsi qu'à l'existence de garanties de procédure appropriées. Notamment, le projet de proposition dispose qu'une **autorisation expresse et spécifique** devrait être délivrée par une **autorité judiciaire** ou par une **autorité administrative indépendante** d'un État membre avant toute utilisation des systèmes d'identification biométrique à distance, sauf dans des situations d'urgence dûment justifiées[197].

iii) Autres systèmes d'identification biométrique à distance à haut risque autorisés

Le projet de proposition énonce que les autres systèmes d'identification biométrique à distance en temps réel et «a posteriori» devraient être classés comme «**à haut risque**», étant donné que les imprécisions techniques de ces systèmes pourraient aboutir à des résultats biaisés et donner lieu à des effets discriminatoires, notamment en matière d'âge, d'ethnie, de sexe ou de handicap[198]. Un large spectre de systèmes d'identification biométrique à distance peut relever de cette catégorie. Il s'agit notamment de l'utilisation en temps réel de l'identification biométrique à distance dans des espaces accessibles au public par des autorités publiques à d'autres fins que les activités répressives

---

192 Voir *2002/584/JAI: Décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres — Déclarations de certains États membres sur l'adoption de la décision-cadre*.

193 L'article 2 renvoie à une longue liste d'infractions pénales punies dans l'État membre d'émission d'une peine ou d'une mesure de sûreté privatives de liberté d'un maximum d'au moins trois ans, telles que la participation à une organisation criminelle, le terrorisme, la traite d'êtres humains et l'exploitation sexuelle des enfants et la pédopornographie.

194 Voir Commission européenne (2021), *Impact Assessment*, p. 18. La France, la Finlande, la République tchèque et le Danemark, entre autres, ont appuyé cette option.

195 Voir considérant 22 de la proposition de règlement 2021/0106(COD).

196 Voir, en ce sens, Christakis, T., et Becuywe, M. (2021). Les auteurs affirment que l'article 5, paragraphe 1, point d), a vocation à s'appliquer en tant que *lex specialis* en ce qui concerne les règles sur le traitement des données biométriques visées à l'article 10 de la directive (UE) 2016/680.

197 Voir considérant 21 de la proposition de règlement 2021/0106(COD).

198 Voir considérant 33 et annexe III, paragraphe 1, point a), de la proposition de règlement 2021/0106(COD).

(par exemple, pour contrôler l'accès à un bâtiment); l'utilisation en temps réel de l'identification biométrique à distance dans des espaces accessibles au public par des acteurs privés (par exemple, le fait de scanner les clients lorsqu'ils entrent dans des supermarchés, le contrôle à l'entrée des stades, des établissements scolaires et des transports, et à des fins de santé publique); l'utilisation de l'identification biométrique à distance «a posteriori», notamment par les services répressifs (par exemple, pour identifier une personne ayant commis une infraction); et l'utilisation de l'identification biométrique à distance en temps réel (notamment par les services répressifs) dans des espaces non accessibles au public (c'est-à-dire des lieux privés)[199].

Ces systèmes d'IA, bien qu'ils soient classés comme «à haut risque», ne sont pas interdits par défaut, mais soumis à plusieurs obligations de conformité. Ils devraient être mis sur le marché de l'Union ou mis en service s'ils respectent certaines **exigences obligatoires** afin de veiller à ce que leur utilisation ne présente pas de risques inacceptables pour les intérêts publics importants de l'Union, tels que reconnus et protégés par le droit de l'Union[200]. En vue d'atténuer les risques pour les droits fondamentaux concernés, tous les systèmes d'identification biométrique à distance («en temps réel» et «a posteriori») devraient être soumis à de **strictes exigences préalables à la commercialisation**. Les fournisseurs de systèmes de reconnaissance faciale devraient être tenus, entre autres, de mettre en place des mesures appropriées d'évaluation et d'atténuation des risques, d'utiliser des ensembles de données de qualité, de garantir la transparence et de fournir des informations adéquates aux utilisateurs, de mettre en œuvre des mesures appropriées de contrôle humain et de veiller à ce que ces systèmes soient conçus selon un niveau approprié de précision, de robustesse et de cybersécurité[201]. Par ailleurs, les systèmes d'identification biométrique à distance devraient être soumis à de strictes **procédures d'évaluation de la conformité ex ante**, dont les fournisseurs (y compris les importateurs et les distributeurs) et les utilisateurs de systèmes de reconnaissance faciale devraient s'acquitter[202]. En principe, les systèmes d'IA utilisés pour l'identification biométrique devraient faire l'objet d'une évaluation de la conformité par un organisme indépendant (et non pas remis à une autoévaluation, comme c'est le cas pour les autres types de systèmes d'IA à haut risque), à moins que des normes harmonisées ou des spécifications communes existent (article 43, paragraphe 1)[203]. Une fois qu'un système d'identification biométrique à distance a obtenu une certification, il pourrait être mis sur le marché et utilisé par des acteurs publics ou privés conformément au droit de l'Union existant. Notamment, il devrait rester conforme au regard des **exigences du RGPD**, qui n'autorisent le traitement des données biométriques que dans des conditions strictes (voir section 3 précédente)[204]. De plus, il existerait également un **système de surveillance et de supervision ex post du marché** de ces systèmes d'identification biométrique à distance, par les autorités nationales compétentes désignées par les États membres[205].

---

199 Voir Christakis, T., et Becuywe, M. (2021). Voir également Kind, C. (2021), *Containing the canary in the AI coalmine — the EU's efforts to regulate biometrics*, Ada Lovelace Institute. Voir eDRi (2021), *EU's AI law needs major changes to prevent discrimination and mass surveillance*. Voir Veale, M., et Zuiderveen Borgesius, F. (juillet 2021), *Demystifying the Draft EU Artificial Intelligence Act*.

200 Voir considérant 27 de la proposition de règlement 2021/0106(COD).

201 Voir articles 8 à 15 de la proposition de règlement 2021/0106(COD).

202 Voir articles 16 à 29 de la proposition de règlement 2021/0106(COD). Il est à noter que les règles proposées sont plus strictes pour les systèmes d'identification biométrique à distance (l'évaluation de la conformité ex ante serait obligatoire à moins que des normes harmonisées adoptées par les organismes de normalisation de l'Union soient utilisées) que pour les autres systèmes d'IA à haut risque (évaluation de conformité ex post et contrôles internes).

203 Voir considérant 64 de la proposition de règlement 2021/0106(COD).

204 Voir considérant 24 de la proposition de règlement 2021/0106(COD).

205 Voir article 61 de la proposition de règlement 2021/0106(COD).

iv) Systèmes de catégorisation biométrique

Les technologies de reconnaissance faciale pourraient également, en théorie, être considérées comme des systèmes de catégorisation biométrique (voir section 1). Ces systèmes, définis comme des «système[s] d'IA destiné[s] à affecter des personnes physiques à des catégories spécifiques selon le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, l'origine ethnique ou l'orientation sexuelle ou politique, etc., sur la base de leurs données biométriques»[206], ne sont pas explicitement répertoriés comme destinés à une utilisation à haut risque des données biométriques (lorsqu'ils sont utilisés à d'autres fins que l'identification)[207]. Dès lors — sauf dans le domaine répressif [voir points i) et ii) précédents] — ces systèmes seraient soumis uniquement à des **mesures de transparence** et à l'**information des personnes concernées** (à moins que l'utilisation des systèmes ne soit autorisée par la loi afin de détecter, de prévenir et d'enquêter sur des infractions pénales)[208]».

Tableau 1 — Proposition de règlement en matière d'IA: scénarios de réglementation des systèmes de reconnaissance faciale

TRF RÉGLEMENTÉES[209]	Systèmes de reconnaissance faciale [à distance] en temps réel dans des espaces accessibles au public à des fins répressives		Autres systèmes d'identification (en temps réel ou a posteriori) par reconnaissance faciale [à distance]	Systèmes de reconnaissance faciale à des fins de catégorisation
Règle	interdits par principe (risque inacceptable)	autorisés pour des exceptions spécifiques (haut risque) - recherches de victimes d'actes criminels - menace pour la vie ou pour l'intégrité physique ou menace d'acte de terrorisme - infraction grave (mandat d'arrêt européen)	autorisés (haut risque)	autorisés (risque faible)
Conditions		- autorisation ex ante (autorité judiciaire ou organisme administratif indépendant)	- exigences préalables à la commercialisation - évaluation de conformité ex ante (autoévaluation ou évaluation par un tiers) - surveillance et supervision ex post du marché	- transparence - information

206 Voir considérant 35 de la proposition de règlement 2021/0106(COD).

207 Voir annexe III, paragraphe 1, de la proposition de règlement 2021/0106(COD).

208 Voir article 1 et article 52 de la proposition de règlement 2021/0106(COD).

209 En outre, la législation préexistante, notamment les règles en matière de protection des données et de non-discrimination, s'applique.

4.3. Principaux sujets de discussion stratégiques

4.3.1. Différencier les systèmes biométriques à haut risque et à faible risque

La classification des technologies et de leurs applications dans les catégories à haut risque et à faible risque est contestable. Par exemple, il est **discutable** d'établir une **distinction entre les systèmes d'identification biométrique à distance «en temps réel» et «a posteriori»**, ainsi qu'**entre les systèmes de «catégorisation biométrique» et d'«identification biométrique»**. Une telle différenciation risque d'être arbitraire, car la catégorisation biométrique, qui utilise de multiples fonctionnalités, peut en réalité permettre l'identification (par exemple, la recherche de personnes de couleur ou à la peau plus foncée, d'hommes d'âge moyen qui passent devant une caméra de vidéosurveillance spécifique), mais également parce que l'utilisation de systèmes de catégorisation biométrique à distance et a posteriori dans des espaces publics peut avoir un effet négatif sur les droits fondamentaux, comme l'utilisation de systèmes en temps réel[210]. Par ailleurs, certains chercheurs insistent sur le fait que **les catégorisations biométriques répondent à toutes les conditions pour être considérées comme des systèmes à haut risque** présentant un «risque d'effets néfastes sur les droits fondamentaux» et devraient dès lors être explicitement ajoutées à la liste des systèmes d'IA à haut risque de l'annexe III de la proposition[211]. En outre, l'approche proposée pourrait sous-estimer la **capacité des systèmes biométriques déployés par des acteurs privés d'avoir un effet dissuasif sur l'exercice des droits fondamentaux** (par exemple, si des acteurs privés partagent des informations avec les services répressifs ou collaborent avec ces derniers)[212].

Dans ce contexte, des universitaires ont suggéré, entre autres, de **réviser les définitions proposées**, notamment des «données biométriques» et des «systèmes d'identification biométrique», qui sont perçues comme étant trop restrictives, et de permettre une **adaptation plus flexible de la liste des pratiques d'IA interdites**[213]. Par ailleurs, une **justification plus rigoureuse** de la distinction établie entre les utilisations privées et publiques des systèmes biométriques à distance serait nécessaire afin d'appuyer une différenciation des règles juridiques applicables[214].

4.3.2. Demandes de règles plus strictes

Au titre du projet de règlement, de nombreux systèmes d'identification biométrique à distance resteraient autorisés. Les opposants soulèvent des inquiétudes quant au fait que la proposition d'interdiction des **systèmes de surveillance biométrique à des fins répressives fait l'objet de vastes exceptions** et affirment qu'une telle interdiction ne s'applique pas aux autres autorités (par exemple, les établissements scolaires, les collectivités locales) ni aux entreprises privées (par exemple, les supermarchés, les sociétés transport), en dépit d'éléments de preuve selon lesquels ces acteurs entreprennent déjà des activités de surveillance biométrique de masse[215]. De plus, étant

---

210 Voir Kind, C. (2021), *Containing the canary in the AI coalmine — the EU's efforts to regulate biometrics*, Ada Lovelace Institute. Les auteurs soulignent que certaines des utilisations de technologies de reconnaissance faciale les plus controversées seraient considérées comme des utilisations «a posteriori», comme l'outil d'IA Clearview, vendu aux forces de police à l'échelle internationale.

211 Voir Malgier, G., et Ienca, M. (7 juillet 2021), *The EU regulates AI but forgets to protect our mind*.

212 Voir Smuha, N., et al. (août 2021), *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*.

213 Voir Parlement européen (2021), département thématique des droits des citoyens et des affaires constitutionnelles, *Biometric Recognition and Behavioural Detection*.

214 Voir Smuha, N., *et al.* (2021).

215 Voir EDRi (2021), *EU's AI law needs major changes to prevent discrimination and mass surveillance*.

donné que la proposition d'interdiction s'applique uniquement aux utilisations «en temps réel» dans des espaces accessibles au public à des fins répressives, des cas d'utilisations tout aussi néfastes, telles que le suivi de personnes par les services de police au moyen d'un logiciel controversé ou la surveillance par des acteurs privés pour le compte de gouvernements et d'organismes publics dans des partenariats privés-publics, demeureraient possibles[216]. Les organisations pour les libertés civiles demandent également une interdiction ou un moratoire sur l'utilisation des technologies automatisées dans les scénarios de contrôle aux frontières et de la migration jusqu'à ce qu'elles soient indépendamment évaluées quant à leurs conséquences sur les Droits de l'homme et fassent l'objet d'une autorisation[217].

En outre, le projet de législation permettrait toujours aux autorités policières d'utiliser des technologies de reconnaissance faciale à des fins de **catégorisation biométrique à distance**, bien qu'imposant des garanties très limitées[218]. Par ailleurs, l'utilisation de la catégorisation biométrique à d'autres fins que l'identification n'est pas, à l'heure actuelle, explicitement répertoriée comme une utilisation à haut risque des données biométriques à l'annexe III de la proposition. Des inquiétudes ont été soulevées quant au fait que les forces de police pourraient dès lors utiliser les technologies biométriques pour passer au crible des espaces publics afin de rechercher des personnes d'une ethnie, d'un âge, d'une orientation sexuelle ou politique spécifique, ou encore des personnes qui «semblent suspectes», sans aucune restriction, aucune approche en matière de gestion des risques ou aucun contrôle[219]. L'argument invoqué est le suivant: les systèmes de reconnaissance faciale en temps réel utilisés à des fins de catégorisation biométrique continueraient d'être licites dans l'Union[220] et la proposition de législation en matière d'IA légitimerait, au lieu d'interdire, la surveillance à l'échelle de la population[221]. Dans ce contexte**, des voix s'élèvent pour imposer une interdiction pure et simple des applications permettant la «catégorisation biométrique»** (et non pas simplement soumettre celles-ci à des obligations minimales en matière de transparence, comme proposé par la Commission)[222].

De même, le CEPD a souligné que la proposition ne va pas assez loin eu égard à l'identification biométrique à distance et plaide en faveur d'une **approche plus stricte quant à la reconnaissance automatisée dans les espaces publics**, indépendamment du fait que celle-ci soit utilisée dans un contexte commercial ou administratif à des fins répressives[223]. Dans un avis commun non contraignant, le CEPD et le comité européen de la protection des données **ont demandé l'interdiction générale de toute utilisation de l'IA à des fins de reconnaissance automatisée des caractéristiques humaines dans les espaces accessibles au public** — notamment la reconnaissance des visages, ainsi que de la démarche, des empreintes digitales, de l'ADN, de la voix, du mode de frappe au clavier et autres signaux biométriques ou comportementaux[224]. Les autorités

---

216 Ibid.

217 Voir Access now *et al.* (7 juin 2021), *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance*.

218 Voir article 52 paragraphe 2, de la proposition de règlement 2021/0106(COD). Le projet de législation exempte explicitement les forces de police de divulguer l'utilisation de systèmes de catégorisation.

219 Voir Kind, C. (2021), *Containing the canary in the AI coalmine — the EU's efforts to regulate biometrics*, Ada Lovelace Institute.

220 Voir considérant 70 de la proposition de règlement 2021/0106(COD). En ce sens, voir Kind, C. (2021).

221 Voir Veale, M., et Zuiderveen Borgesius, F. (2021), p. 9.

222 Voir EDRi (2021). Voir également Smuha, N., *et al.* (2021).

223 Voir CEPD (2021), *Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary*.

224 Voir comité européen de la protection des données — CEPD (18 juin 2021), *Joint opinion 5/2021*.

de protection des données soulignent qu'il n'existe pas de solution adéquate pour informer de manière appropriée les personnes d'un traitement biométrique ainsi que pour garantir l'exercice effectif et opportun des droits des personnes. De plus, elles estiment que le caractère intrusif du traitement ne dépend pas toujours de l'identification en temps réel, et que l'utilisation de systèmes biométriques à des fins de sécurité privée menace tout autant les droits fondamentaux au respect de la vie privée et familiale et à la protection des données à caractère personnel. Par ailleurs, le CEPD et le comité européen de la protection des données recommandent une interdiction (destinée tant aux autorités publiques qu'aux entités privées) relative aux systèmes d'IA (y compris la reconnaissance faciale) qui sont utilisés pour catégoriser les personnes en fonction de leur ethnie ou de leur sexe, ainsi que de leur orientation politique ou sexuelle, car cela peut aboutir à une discrimination déloyale[225].

4.3.3. Liberté d'action des États membres quant à la mise en œuvre

Le projet de proposition laisse le soin aux États membres de décider s'ils souhaitent ou non mettre en œuvre les exceptions d'interdiction d'utiliser les systèmes de reconnaissance faciale en temps réel dans des espaces accessibles au public à des fins répressives [indiquées en détail à l'article 5, paragraphe 1, point d)] dans leur législation nationale et adopter des «règles détaillées du droit national» à cet égard[226]. La question se pose de savoir **ce qu'on entend exactement par «règles détaillées du droit national»** et, en particulier, si, au-delà de simples actes législatifs votés au Parlement, ces règles pourraient prendre la forme d'actes non législatifs (par exemple, des mesures réglementaires adoptées par d'autres autorités, telles que les ministres des affaires intérieures ou les ministres de la justice)[227]. Dès lors, des précisions seraient nécessaires eu égard aux actes juridiques requis à l'échelle nationale pour utiliser les systèmes d'identification biométrique à distance dans des espaces accessibles au public à des fins répressives.

4.3.4. Normalisation et autoévaluation

La normalisation jouera un rôle essentiel dans la fourniture de solutions techniques visant à assurer la conformité au regard de la proposition de règlement. Notamment, au titre de l'avant-projet, les systèmes d'IA à haut risque qui sont conformes aux **normes harmonisées** seraient présumés conformes aux exigences obligatoires communes applicables à la conception et à la mise au point de systèmes d'IA et dès lors autorisés à être commercialisés[228]. Toutefois, le processus de normalisation proposé suscite de nombreuses questions. La pratique de la Commission qui consiste à déléguer l'élaboration de la réglementation aux organismes de normalisation régis par le droit privé a fait l'objet de critiques pendant des années, essentiellement en raison de l'absence de contrôle démocratique, de la participation inappropriée des acteurs concernés, de l'absence de contrôle juridique adéquat sur les normes harmonisées et du fait que le Parlement n'a aucun droit de veto contraignant sur les normes harmonisées mandatées par la Commission[229]. En outre, bien qu'en théorie, au titre de l'avant-projet, les organismes spécifiques notifiés soient tenus d'évaluer la conformité des systèmes d'identification à distance à haut risque, dans la pratique, seule une

---

225 Ibid.

226 Considérants 22 et 23 de la proposition de règlement 2021/0106(COD).

227 Voir Christakis, T., et Becuywe, M. (2021). Voir également Muller, C. et Dignum, V. (2021), *Artificial intelligence act, analysis and recommendations*.

228 Voir article 40 de la proposition de règlement 2021/0106(COD).

229 Voir Veale, M., et Zuiderveen Borgesius, F. (2021), p. 13-14. Pour un aperçu du processus de normalisation en matière d'IA, voir Nativi, S., et De Nigris, S. (2021), *AI Standardisation Landscape: state of play and link to the EC proposal for an AI regulatory framework*. Voir également Ebers, M. (2021), *Standardizing AI — The Case of the European Commission's Proposal for an Artificial Intelligence Act*.

autoévaluation serait requise à l'issue de la création de normes harmonisées relatives à ces systèmes[230].

L'industrie soutient fortement l'autoréglementation[231]. Toutefois, une telle approche a fait l'objet de vives critiques eu égard à la liberté d'action jugée excessive des développeurs de l'IA et des acteurs privés, qui ont un intérêt personnel majeur dans le déploiement de ces systèmes[232]. Les experts soulignent également que la proposition de normalisation des systèmes d'IA n'est pas une question de décisions purement techniques, mais qu'elle requiert un certain nombre de décisions éthiques et juridiques, qui ne devraient pas être confiées à des entités privées[233]. Dans ce contexte, il a été demandé d'apporter des modifications au processus de normalisation européenne, entre autres, afin de garantir des droits de participation effective aux organisations des parties prenantes européennes et de faire du processus un système de normalisation plus transparent et plus inclusif[234].

4.4. Principales conclusions

Le projet de règlement en matière d'IA proposé en avril 2021 vise à limiter l'utilisation des systèmes d'identification biométrique, y compris la reconnaissance faciale, au sein de l'Union, et repose sur le principe selon lequel ces technologies présentent les plus grandes menaces pour les droits fondamentaux lorsqu'elles sont utilisées «en temps réel» et à des fins d'«identification». Outre la législation applicable existante (par exemple, en matière de protection des données et de non-discrimination), le projet de loi sur l'IA propose d'introduire de nouvelles règles régissant l'utilisation des TRF au sein de l'Union et de les différencier selon que leurs caractéristiques d'utilisation présentent un «risque élevé» ou un «risque faible». Un grand nombre de TRF seraient considérées comme des systèmes «à haut risque» qui feraient l'objet d'une interdiction ou devraient respecter des exigences strictes. L'utilisation de systèmes de reconnaissance faciale en temps réel dans des espaces accessibles au public à des fins répressives serait interdite, à moins que les États membres choisissent de les autoriser pour des motifs importants de sécurité publique, et que des autorisations judiciaires ou administratives appropriées soient garanties. Toutefois, un large éventail de technologies de reconnaissance faciale utilisées à d'autres fins que les activités répressives (par exemple, contrôle aux frontières, places de marché, transport public et même établissements scolaires) pourraient être autorisées sous réserve d'une évaluation de la conformité au regard de certaines exigences de sécurité avant d'être mises sur le marché de l'Union. En outre, les systèmes de reconnaissance faciale utilisés à des fins de catégorisation seraient considérés comme des systèmes à «faible risque» et seraient soumis uniquement à des exigences limitées en matière de transparence et d'information. Bien que les législateurs de l'Union commencent à évaluer le projet de loi sur l'IA, les opposants remettent en question certains aspects de la proposition, notamment la distinction entre les systèmes «à haut risque» et les systèmes «à faible risque», la liberté d'action des États membres dans la mise en œuvre de l'exception à l'interdiction des systèmes de reconnaissance faciale à distance à des fins répressives, et l'absence de contrôle public approprié sur les processus proposés de normalisation et d'autoévaluation. Certains se prononcent

230 Ibid.

231 Voir Forum économique mondial (2021), *What to know about the EU's facial recognition regulation — and how to comply*.

232 Voir AlgorithmWatch (avril 2021), AlgorithmWatch's response to the European Commission's proposed regulation on artificial intelligence — A major step with major gaps.

233 Voir Ebers, M. (2021*), Standardizing AI — The Case of the European Commission's Proposal for an Artificial Intelligence Act*.

234 Ibid.

résolument en faveur de règles plus strictes — y compris une interdiction pure et simple de ces technologies.

5. Aspects internationaux

5.1. Hausse de la surveillance par reconnaissance faciale dans le monde

On observe une hausse de la surveillance biométrique, et notamment de la technologie de reconnaissance faciale, dans différentes parties du monde. Selon un rapport d'Amnesty International, au moins 64 pays utilisent activement des systèmes de reconnaissance faciale dans le monde à ce jour[235]. La Chine, notamment, est l'un des principaux utilisateurs de cette technologie. Par exemple, les établissements scolaires chinois utilisent la reconnaissance faciale pour contrôler les prêts de bibliothèque et dresser des rapports annuels sur la nutrition de chaque élève[236]. Il a été signalé que les autorités chinoises utilisent l'identification biométrique, y compris la technologie de reconnaissance faciale, pour limiter les mouvements et les activités de la minorité ouïgoure[237]. Les entreprises chinoises proposent en amont des normes techniques internationales pour les applications de l'IA, y compris la reconnaissance faciale, par exemple dans l'Union internationale des télécommunications (UIT) des Nations unies[238].

L'utilisation croissante de caméras à reconnaissance faciale dans des espaces publics a été particulièrement documentée dans un certain nombre de pays et de régions du monde, notamment au Kirghizstan, en Inde, en Amérique latine, en Israël, aux États-Unis, en Australie et en Russie[239]. On rapporte qu'en Russie, les outils de surveillance assistée par l'IA sont de plus en plus utilisés à l'encontre des dissidents politiques et des militants des Droits de l'homme, et que la pandémie a accéléré l'installation d'un réseau de 100 000 caméras à reconnaissance faciale afin de suivre la trace de personnes placées en quarantaine[240]. Dans ce contexte, les responsables politiques du monde entier débattent de la possibilité de mettre en place des cadres juridiques plus ou moins stricts en vue de contrôler l'utilisation des systèmes de reconnaissance faciale.

5.2. Approche des États-Unis quant à la réglementation des TRF

Outre les règles généralement applicables en matière de vie privée, il n'existe actuellement aux États-Unis aucune législation fédérale réglementant l'utilisation de la reconnaissance faciale par des entreprises privées ou dans le contexte des activités répressives. Toutefois, la commission américaine du commerce (FTC), dans le droit-fil de son mandat de protection des consommateurs, a publié des lignes directrices qui énoncent que les entreprises ne devraient pas induire en erreur

---

235 Voir Feldstein, S. (2019), *The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace working paper*.

236 Voir article 19 (2021), *Emotional Entanglement: China's emotion recognition market and its implications for human rights*, p. 33.

237 Voir Parlement européen (2021), *Digital technologies as a means of repression and social control*, département thématique des relations extérieures, direction générale des politiques externes de l'Union, p. 15.

238 Voir Gross, A., Murgia, M., et Yang, Y. (1er décembre 2019), «Chinese Tech Groups Shaping UN Facial Recognition Standards», *Financial Times*.

239 Voir Parlement européen (2021), *Digital technologies as a means of repression and social control*, p. 16.

240 Ibid p. 16.

leurs clients quant à la manière dont elles utilisent les algorithmes de reconnaissance faciale[241]. De plus, des interdictions, restrictions ou moratoires éventuels sur l'utilisation de ces technologies sont en discussion dans le pays, aux échelles étatiques et locales[242]. Certaines villes des États-Unis, comme San Francisco, Boston et Portland, ont interdit la technologie de reconnaissance faciale dans les espaces publics[243], et l'État de Californie a adopté une loi qui impose un moratoire de trois ans sur la technologie de reconnaissance faciale utilisée dans les caméras des organes de police à compter du 1er janvier 2020[244]. Néanmoins, l'ensemble disparate de lois et réglementations étatiques et locales existant n'offre pas de certitude juridique aux pouvoirs publics, à l'industrie et aux citoyens. Par ailleurs, l'absence d'approche fédérale cohérente est un fardeau pour les agences de sécurité nationale [comme l'agence centrale du renseignement (Central Intelligence Agency, CIA)], qui recourent de manière croissante aux TRF[245].

Dans ces conditions, des voix s'élèvent pour réglementer l'utilisation des technologies de reconnaissance faciale aux États-Unis au moyen d'une législation fédérale, notamment dans le contexte de la surveillance à des fins répressives et en particulier en vue de proposer une solution unique aux problèmes émergents en matière de respect de la vie privée qui découlent de l'utilisation de la technologie de reconnaissance faciale en temps réel[246]. Une série de propositions ont été présentées à cet égard, notamment la proposition d'adopter une loi sur la protection de la vie privée en matière de reconnaissance faciale commerciale de mars 2019, qui interdirait en règle générale aux entreprises d'utiliser des technologies de reconnaissance faciale pour collecter des données de reconnaissance faciale sans en informer ni obtenir le consentement des personnes concernées[247]. Plusieurs autres projets de loi fédéraux visant à réglementer les technologies de reconnaissance faciale ont été proposés et sont toujours à l'étude[248].

5.2. Approche de la Chine quant à la réglementation des TRF

En Chine, il n'existe à ce jour aucune loi ou réglementation en vigueur qui régit expressément les TRF. La reconnaissance faciale est indirectement réglementée par la loi sur la cybersécurité, qui énonce certaines exigences pour la collecte, l'utilisation et la protection des informations personnellement identifiables, y compris les données biométriques. Toutefois, en avril 2021, le Comité technique chinois de normalisation de la sécurité nationale de l'information a publié un projet de norme sur les exigences de sécurité des données de reconnaissance faciale, qui vise à définir des exigences non obligatoires pour la collecte, le traitement, le partage et le transfert de données utilisées pour la reconnaissance faciale en Chine[249]. En outre, il est signalé que les législateurs chinois œuvrent actuellement sur l'adoption d'une nouvelle loi relative à la confidentialité des données avec un fort accent sur la biométrie, et que le secteur privé chinois tente de s'attaquer aux problèmes de respect de la vie privée soulevés par l'utilisation des systèmes de

241 Voir Jillson, E. (2021) *Aiming for truth, fairness, and equity in your company's use of AI*.

242 Voir service de recherche du Congrès (27 octobre 2020), *Federal Law Enforcement Use of Facial Recognition Technology*. Voir également Rowe, E. (2021), «Regulating Facial Recognition Technology in the Private Sector», *Stanford Technology Law Review*, vol. 24, nº 1.

243 Voir Metz, R. (2020), «Portland passes broadest facial recognition ban in the US», *CNN Business*.

244 Voir Dunn, G. (2020), *2019 Artificial Intelligence and Automated Systems Annual Legal Review*.

245 Voir National Security Commission on Artificial Intelligence (2021), Final report.

246 Voir Ringrose, K. (2019), «Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns», *Virginia Law Review Online*, vol. 105, nº 1.

247 Voir Congrès des États-Unis, S.847 — *Commercial Facial Recognition Privacy Act* de 2019.

248 Voir Dunn, G. (2020).

249 Voir National Law Review (2021), *China Publishes Draft Security Standard on Facial Recognition*.

reconnaissance faciale au moyen de l'autoréglementation, notamment avec la publication d'orientations et de normes du secteur[250].

5.3. Discussions sur les normes à l'échelle mondiale

À l'heure actuelle, la réglementation de l'IA est une question universelle[251]. La manière d'aborder les TRF a fait l'objet d'un examen particulier dans le contexte de deux **forums internationaux**. En 2020, le **Conseil des Droits de l'homme des Nations unies** a adopté une résolution condamnant particulièrement l'utilisation des TRF dans le contexte de manifestations pacifiques, dès lors que ces technologies créent un effet dissuasif sur l'exercice du droit de manifester en renforçant les capacités des gouvernements à identifier, contrôler, harceler, intimider et poursuivre en justice les manifestants[252]. Le Conseil a invité les États à s'abstenir d'utiliser les technologies de reconnaissance faciale pour contrôler les personnes qui participent à des manifestations pacifiques. En janvier 2021, le **Conseil de l'Europe**, l'organisation européenne des Droits de l'homme basée à Strasbourg, a adopté des lignes directrices sur la reconnaissance faciale[253]. Ces lignes directrices établissent des mesures que les gouvernements, les développeurs, les fabricants, les fournisseurs de services de reconnaissance faciale, ainsi que les entités qui utilisent des TRF devraient respecter et appliquer afin de veiller à ce que celles-ci ne portent pas atteinte aux Droits de l'homme ni aux libertés fondamentales de quiconque, y compris le droit à la dignité humaine et à la protection des données à caractère personnel. Les lignes directrices ont une portée générale et englobent l'utilisation des TRF dans les secteurs privé et public. Elles demandent l'interdiction de l'utilisation de TRF particulièrement intrusives et suggèrent l'adoption de garanties. Les travaux à venir du Conseil de l'Europe sur la création d'un cadre juridique pour l'IA devraient également aborder la question des normes applicables à la reconnaissance faciale[254]. En outre, une **coopération bilatérale** existe par exemple avec le **Conseil du commerce et des technologies** que l'Union et les États-Unis ont décidé d'établir en tant que plateforme de collaboration transatlantique et de normalisation pour les technologies émergentes, telles que l'intelligence artificielle[255].

5.4. Principales conclusions

L'utilisation des technologies de reconnaissance faciale augmente considérablement à l'échelle mondiale et les inquiétudes liées à la surveillance par les États s'intensifient. Au-delà des frontières de l'Europe, les préoccupations sont exacerbées par le fait qu'il n'existe à l'heure actuelle que des règles juridiquement contraignantes limitées applicables aux TRF, même sur des territoires importants comme les États-Unis et la Chine. Les responsables de l'élaboration des lois et des politiques du monde entier ont la possibilité de discuter — dans un contexte multilatéral, voire bilatéral — de la manière de mettre en place des contrôles plus ou moins stricts en ce qui concerne l'utilisation de systèmes de reconnaissance faciale. Il est fondamental pour l'Union, qui a déclaré son

---

250 Voir Lee, S. (2020), *Coming into Focus: China's Facial Recognition Regulations*. Voir également Levine, A. S. (8 juillet 2021), «"Deeply alarmed": China outpaces US on privacy law», *Politico Pro*.

251 Voir Observatoire OCDE des politiques de l'IA qui fournit des informations en temps réel et des analyses d'initiatives en matière de politiques de l'IA dans le monde.

252 Voir Conseil des Droits de l'homme des Nations unies (2020), *Résolution sur la promotion et la protection des Droits de l'homme dans le contexte des manifestations pacifiques*, A/HRC/44/L.11.

253 Voir Conseil de l'Europe (2021), *Lignes directrices sur la reconnaissance faciale*.

254 Voir Conseil de l'Europe (21 mai 2021), *CAHAI — Comité ad hoc sur l'intelligence artificielle, 131e Session du Comité des Ministres*.

255 Voir Commission européenne (2020), *UE — États-Unis:* «un nouveau programme transatlantique pour un changement planétaire», communiqué de presse.

ambition de prendre l'initiative quant aux normes mondiales en matière d'IA[256], de participer à ces discussions sur la réglementation des TRF.

6. Perspectives

Les universitaires, acteurs et responsables politiques partagent en grande partie les préoccupations sur le respect des droits fondamentaux — notamment des droits à la protection des données et à la non-discrimination — qui découlent de l'utilisation croissante des technologies de reconnaissance faciale. Toutefois, les avantages apportés par ces technologies en matière de sécurité, notamment par une authentification plus précise, sont indéniables. Dans ce contexte, les législateurs se heurtent au défi d'encourager des utilisations légitimes de la reconnaissance faciale, tout en empêchant les abus et en protégeant les droits fondamentaux des personnes. Compte tenu des préoccupations sociales liées à l'utilisation de ces technologies basées sur l'IA et du risque de fragmentation du marché intérieur en l'absence de mesures, la Commission propose de préciser les circonstances qui peuvent justifier une telle utilisation et d'énoncer les garanties nécessaires au sein d'une réglementation de l'IA. À cette fin, l'approche de l'Union quant à la biométrie, et notamment à la reconnaissance faciale, reposerait sur une distinction entre les applications biométriques «à haut risque» et celles «à faible risque», aboutissant à l'application d'un régime juridique plus ou moins strict. L'approche de l'Union en ce qui concerne l'IA semble compléter les règles strictes déjà applicables en matière de protection des données et de non-discrimination par une nouvelle strate de règles régissant la mise sur le marché des technologies de reconnaissance faciale. Bien que les acteurs, les chercheurs et les organismes de réglementation semblent convenir d'un besoin en matière de réglementation, certains opposants remettent en question la distinction proposée entre les systèmes biométriques à haut risque et ceux à faible risque, et avertissent que la législation proposée donnerait lieu à un système de normalisation et d'autoréglementation sans contrôle public approprié. Ces derniers demandent des modifications de l'avant-projet, notamment eu égard à la liberté d'action accordée aux États membres dans la mise en œuvre des nouvelles règles. Certains sont en faveur de règles plus strictes — y compris une interdiction pure et simple de ces technologies.

[256] Voir Commission européenne (2020), Façonner l'avenir numérique de l'Europe — Questions et réponses.

Références

Buolamwini, J., et Gebru, T (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*.

Castelluccia, C., et Le Métayer Inria, D. (2020), *Impact Analysis of Facial Recognition*, Centre for Data Ethics and Innovation.

Christakis, T., et Becuywe, M. (2021), «Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation», *European Law Blog*.

Parlement européen, département thématique des droits des citoyens et des affaires constitutionnelles (2021), *Biometric Recognition and Behavioural Detection*.

Agence des droits fondamentaux de l'Union européenne (2020), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, Office des publications de l'Union européenne.

Gerards, J., et Xenidis, R. (2021), *Algorithmic discrimination in Europe*, Commission européenne.

Leslie, D. (2020), *Understanding bias in facial recognition technologies*, The Alan Turing Institute.

Nativi, S., et De Nigris, S. (2021), *AI Standardisation Landscape: state of play and link to the EC proposal for an AI regulatory framework*.

Rowe, E. (2021), «Regulating Facial Recognition Technology in the Private Sector», *Stanford Technology Law Review*.

Smuha, N., *et al*. (août 2021), *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*.

Xenidis, R., et Senden, L., «EU non-discrimination law in the era of artificial intelligence: mapping the challenges of algorithmic discrimination», dans Bernitz, U., *et al*. (2020), *General principles of EU law and the EU digital order*, Kluwer Law International.

Annexe 1 — Exemples d'utilisation des TRF dans quelques États membres de l'Union[257]

Pays	Cas d'utilisation	Jurisprudence, décisions administratives et législations pertinentes
France	**Projets-pilotes de TRF dans des établissements scolaires à Nice et à Marseille:** La TRF a été testée afin d'aider des agents de sécurité à contrôler l'accès au sein de deux lycées, en vue d'empêcher toute intrusion et tout vol d'identité et de réduire la durée de ces contrôles. **Solution d'identité numérique Alicem:** En 2020, le ministère français de l'intérieur a mis en service *Alicem* (Authentification en LIgne CErtifiée sur Mobile), une application mobile qui utilise la TRF pour permettre aux personnes de prouver leur identité sur internet de manière sécurisée, à l'aide de leur smartphone et de leur passeport ou de leur permis de séjour.	Le tribunal administratif de Marseille a annulé la décision de la municipalité de Marseille d'autoriser des essais de TRF dans les deux établissements scolaires de Nice et de Marseille. L'autorité française de protection des données (CNIL) a publié un avis positif sur un projet de décret autorisant la création du système *Alicem*.
Allemagne	**Prévention de la criminalité dans une gare:** En 2019, les services de police ont piloté l'utilisation de la TRF afin de détecter des comportements suspects à la **gare** de Berlin Südkreuz.	
	Enquête criminelle au sommet du G20: lors du **sommet du G20 de 2017**, les autorités policières de la ville de Hambourg ont déployé des TRF pour la détection et l'enquête relatives à des actes criminels.	Dans le contexte du G20, un tribunal de première instance a annulé l'ordonnance de l'autorité de protection des données de Hambourg de supprimer la base de données de modèles biométriques des services de police. L'autorité de protection des données de Hambourg a fait appel. Les autorités policières se sont initialement appuyées sur les articles 161 et 163, lus en conjonction avec l'article 98c du **code de procédure pénale allemand**. Par la suite, elles se sont reportées aux articles 161 et 163 ou, en alternative, à l'article 483 du code de procédure pénale allemand.

[257] Ce tableau non exhaustif vise uniquement à fournir une impression générale des cas d'utilisation des TRF et de l'environnement juridique dans certains États membres. Il repose en partie sur les informations contenues dans L. Montag et al., The Rise and rise of biometrics mass surveillance in the EU, A legal analysis of biometrics mass surveillance practices in Germany, the Netherlands, and Poland (Une surveillance de masse biométrique en pleine expansion dans l'UE, Une analyse juridique des pratiques de surveillance biométrique de masse en Allemagne, aux Pays-Bas et en Pologne), EDRi — European Digital Rights, 2021.

Pays	Cas d'utilisation	Jurisprudence, décisions administratives et législations pertinentes
	Contrôle d'accès dans un zoo: les médias ont signalé que le **zoo de Berlin** prévoyait d'introduire la TRF afin de faciliter les contrôles d'accès. L'autorité de protection des données de Berlin mène actuellement une enquête à ce sujet.	
	Marché de la ville sécurisé: au moins 19 villes allemandes se sont dotées de caméras biométriques. La préfecture de police de Cologne a déployé des caméras «biométriques» à technologie de reconnaissance faciale en temps réel.	Dans une décision du 18 janvier 2021, le tribunal administratif de Cologne a rendu une ordonnance à l'encontre des forces de police de Cologne afin de mettre fin à la surveillance vidéo de Breslauer Platz et de ses rues adjacentes à Cologne.
Espagne	**Surveillance à un arrêt de bus:** en 2016, un système de reconnaissance faciale en temps réel a été déployé à la station de bus «Estación Sur» de Madrid afin de lutter contre les actes de vandalisme et la petite délinquance.	
	Aéroport: depuis 2019, Aena et Iberia utilisent un système de reconnaissance faciale dans le processus d'embarquement.	
	Immigration: la technologie de reconnaissance faciale est utilisée afin d'améliorer le contrôle aux frontières et d'accroître la sécurité aux passages frontaliers à Ceuta.	
	Supermarchés: la chaîne de supermarchés espagnole Mercadona a déployé la TRF afin de détecter les personnes qui ont reçu une ordonnance restrictive ou qui ont été interdites des locaux des supermarchés par un tribunal.	
Italie	**Système de reconnaissance automatique d'image:** depuis 2019, un système de reconnaissance automatique d'image est utilisé par les forces de police à des fins d'identification.	Le 16 avril 2021, l'autorité de protection des données italienne a publié un avis selon lequel le système de reconnaissance automatique d'image constituerait une forme de surveillance indifférenciée/de masse en cas d'utilisation dans sa forme d'origine. Dans un projet de loi, un moratoire a été proposé sur l'utilisation des technologies de reconnaissance faciale dans des espaces publics.

Pays	Cas d'utilisation	Jurisprudence, décisions administratives et législations pertinentes
Irlande	**Carte de services publics:** le service de protection sociale a déployé un système de reconnaissance faciale afin de prévenir la fraude en matière d'aide sociale.	
Pays-Bas	**Contrôle lors des événements:** les municipalités utilisent la technologie de reconnaissance faciale lors des carnavals et autres grands événements. **Contrôle de police:** depuis 2016, les services de police néerlandais utilisent un système de technologie de reconnaissance faciale appelé CATCH, destiné à identifier des suspects ou des personnes condamnées pour des actes criminels grâce à une base de données sur la justice pénale. Les autorités policières testent également l'utilisation de la technologie de reconnaissance faciale en temps réel via des images de smartphone, des caméras incorporées et le nuage.	L'autorité de protection des données néerlandaise a publié une recommandation dans laquelle elle s'oppose au cadre juridique actuel en matière de biométrie [*Wet Biometrie Vreemdelingenketen* (Wbvk)] et désapprouve l'extension de sa période d'application.

L'Union européenne prend en considération la réglementation de la reconnaissance faciale dans la proposition de loi sur l'intelligence artificielle, actuellement à l'étude. Cette publication du service de recherche du Parlement européen dresse l'état de la situation et met en exergue les préoccupations soulevées par l'utilisation des technologies de reconnaissance faciale et leurs effets potentiels sur les droits fondamentaux des personnes. Dans ce contexte, le document examine le cadre juridique actuel de l'Union applicable à la reconnaissance faciale et étudie de manière approfondie les récentes propositions de réglementation des technologies de reconnaissance faciale à l'échelle de l'Union.

QA-01-21-197-FR-N

Ce document est une publication du service de recherche pour les députés.
EPRS | Service de recherche du Parlement européen

PE 698.021
ISBN 978-92-846-8501-1
doi:10.2861/788795