ARTICLE 19

Sous surveillance attentive: technologies biométriques et liberté d'expression

2021

Publié pour la première fois par ARTICLE 19 en avril 2021.

ARTICLE 19 œuvre pour un monde où tous les individus, partout dans le monde, peuvent s'exprimer librement et participer activement à la vie publique sans crainte de discrimination.

Pour ce faire, nous travaillons sur deux libertés interdépendantes, qui constituent le fondement de tout notre travail. La Liberté de Parole concerne le droit de chacun d'exprimer et de diffuser des opinions, des idées et des informations par tous les moyens, ainsi que le droit d'etre en désaccord ou questionner les gouvernants. La liberté d'information concerne le droit de demander et de recevoir des informations par les gouvernants pour la transparence, la bonne gouvernance et le développement durable. Lorsque l'une ou l'autre de ces libertés est menacée par l'incapacité des détenteurs du pouvoir à les protéger de manière adéquate, ARTICLE 19 parle d'une seule voix, par le biais des tribunaux, à travers les organisations mondiales et régionales, et à travers la société civile partout où nous sommes présents.

ARTICLE 19
Free Word Centre
60 Farringdon Road
London EC1R 3GA UK

E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org
ISBN: 978-1-910793-43-5

Table of contents

Résumé exécutif **4**
Introduction **6**
Technologies biométriques : le contexte **9**
Terminologie clé 9
Fiabilité des technologies biométriques 10
Déploiement des technologies biométriques : principaux usages et discours dominant 11
Normes internationales des droits humains et technologies biométriques **12**
Normes des droits humains applicables 12
Normes des droits humains relatives aux technologies biométriques 14
Responsabilité du secteur privé en matière de droits humains 17
Technologies biométriques et droits à la liberté d'expression et d'information **18**
Technologies biométriques et droits humains : défis globaux 18
Collecte, stockage et rétention de données 18
Potentielles failles de sécurité 18
Problème de la « boîte noire » 19
Échelle 19
Cadres juridiques nationaux inadéquats ou inexistants 19
Nécessité et proportionnalité 20
Absence de recours en cas de violation des droits humains 20
Répercussions des technologies biométriques sur la liberté d'expression et le droit à l'information 20
Effet dissuasif de la surveillance de masse sur la liberté d'expression 20
Impact sur la liberté d'expression de certaines catégories d'individus 21
Nécessité de transparence et accès à l'information 21
Technologies biométriques et liberté d'expression : études de cas **23**
Reconnaissance faciale 23
Objectifs et utilisation des technologies de reconnaissance faciale 23
Problèmes posés par la reconnaissance faciale en matière de droits humains 24
Problèmes posés par la reconnaissance faciale pour la liberté d'expression et d'information 27
Reconnaissance des émotions 28
Objectifs et utilisation des algorithmes de reconnaissance des émotions 28
Efficacité des algorithmes de reconnaissance des émotions 28
Défis posés par les technologies de reconnaissance des émotions en matière de droits humains 29
Défis posés par les technologies de reconnaissance des émotions en matière de liberté d'expression 29
Recommandations d'ARTICLE **31**
Notes **36**

Résumé exécutif

Dans cette Note d'orientation, ARTICLE 19 explique sa position sur les répercussions du développement et du déploiement des technologies biométriques sur le droit à la liberté d'expression.

Cette note d'orientation répond aux inquiétudes suscitées par l'utilisation rapide et croissante des technologies biométriques par le secteur privé mais aussi par les pouvoirs publics. Les technologies biométriques servent à analyser la façon dont les personnes se comportent, apparaissent et s'expriment dans la sphère publique et privée. Elles sont utilisées à des fins diverses, notamment par les patrouilles aux frontières ou pour déverrouiller un smartphone, mais un fait indéniable est indéniable : leur utilisation est en train de se normaliser. Ces technologies ont le pouvoir de modifier la façon dont les individus agissent dans les espaces publics ; elles mettent donc en péril l'existence même de l'espace civique, lequel est un pilier essentiel de la démocratie puisqu'il favorise la participation du public aux affaires d'intérêt public.

Le développement et le déploiement des technologies biométriques doivent se faire dans le respect droits humains afin de protéger les droits fondamentaux des individus. Nous tenons à mettre en lumière les préoccupations suivantes :

La surveillance de masse grandissante des espaces publics par le biais de technologies biométriques telles que la reconnaissance faciale ou la reconnaissance des émotions engendrera avec certitude un effet dissuasif important sur la liberté d'expression et la participation du public.

De nombreuses technologies biométriques sont actuellement développées et déployées sans cadre ni base juridiques appropriés. Ce problème est très préoccupant, ces technologies étant très intrusives et ayant un impact très large sur les droits humains, en particulier la protection de la vie privée et des données et de la liberté d'expression.

Aucun mécanisme efficace n'a été mis en place par les acteurs publics et privés pour permettre à des victimes potentielles de demander réparation. Si ces victimes subissent des discriminations du fait de l'utilisation de la reconnaissance faciale, par exemple, nul ne sait aujourd'hui comment ce problème serait traité. Il y a un manque grave de responsabilisation.

Enfin, la disponibilité d'une technologie biométrique particulière ne doit pas justifier automatiquement son utilisation. Ces technologies ont des défaillances, elles sont exposées à des failles de sécurité et révèlent plusieurs biais.

Pour ces raisons, ARTICLE 19 met en garde contre leur utilisation, notamment à des fins de sécurité nationale et de lutte contre le terrorisme, en l'absence de cadre législatif suffisamment solide pour protéger les droits humains. Nous estimons qu'une approche

basée sur les droits humains est nécessaire et nous appelons à un moratoire sur le développement et le déploiement de toutes ces technologies par les États ainsi que les acteurs privés tant qu'ils ne peuvent garantir une protection intégrale de la liberté d'expression et un respect total des normes internationales des droits humains.

Cette note d'orientation comprend cinq parties. Dans la première partie, nous fournissons des informations générales importantes et une terminologie sur les technologies biométriques. La seconde partie offre un aperçu de toutes les normes internationales pertinentes sur la liberté d'expression. Nous consacrons la troisième section aux problèmes généraux des droits de l'homme engendrés par le développement et le déploiement de ces technologies, et plus particulièrement aux préoccupations liées à la liberté d'expression et d'information. Nous proposons ensuite deux études de cas, la première sur les impacts de la reconnaissance faciale sur la liberté d'expression et la seconde sur les impacts de la reconnaissance des émotions sur la liberté d'expression. Enfin, nous dressons une liste de recommandations globales à l'attention des États, des entreprises privées et de toutes les autres parties concernées.

Résumé des recommandations :

- La surveillance de masse biométrique devrait être interdite ;
- La conception, le développement et l'utilisation des technologies de reconnaissance des émotions devraient être interdits ;
- La conception, le développement et l'utilisation des technologies biométriques devraient se faire dans le respect des principes de légalité, proportionnalité et nécessité ;
- Les États devraient définir un cadre législatif adéquat pour la conception, le développement et l'utilisation des technologies biométriques ;
- La conception, le développement et l'utilisation des technologies biométriques devraient être transparents et faire l'objet d'un débat public et ouvert ;
- Des exigences de transparence devraient être imposées au secteur et intégralement mises en œuvre ;
- Les responsabilités et l'accès à des recours devraient être garantis en cas de violations des droits humains fondées sur les technologies biométriques ;
- Le secteur privé devrait concevoir, développer et déployer des systèmes biométriques dans le respect des normes des droits humains.

Introduction

Partout dans le monde, les systèmes d'identification et de vérification reposent de plus en plus sur des données biométriques – des empreintes digitales et échantillons d'ADN aux technologies biométriques plus avancées visant à identifier les individus selon leurs traits physiques, leurs comportements ou leurs activités.[1] Les acteurs publics et privés utilisent désormais ces technologies dans divers contextes pour mesurer et analyser en temps réel l'apparence, la voix, les mouvements et les comportements des individus. Ces technologies sont désormais utilisées dans des domaines tels que la criminalité et les contrôles aux frontières, la publicité ou le marketing[2] ; elles servent à déverrouiller un smartphone, à accéder à un compte bancaire en ligne, voire même à des espaces physiques et d'autres espaces en ligne.[3] Toutefois, leur utilisation massive ne se limite pas nécessairement à l'identification des personnes. Elles permettent également de dresser des profils et de classer les personnes en fonction de leur âge, leur sexe, leur couleur de peau, de ce qu'elles font, avec qui, ce qu'elles ressentent et même la manière dont elles pourraient se comporter dans le futur.

Le développement rapide des technologies biométriques ces dernières années s'explique par deux facteurs. Premier facteur, la disponibilité **d'un nombre sans précédent de grands fichiers de données** – recueillies principalement par des acteurs privés en se basant sur des modèles commerciaux de plus en plus axés sur les données et soutenus par un discours anxiogène sur la lutte contre le terrorisme et la sécurité publique. Second facteur : la disponibilité croissante, à un coût moindre, **de l'apprentissage automatique**, à la fois en terme de matériel (puissance et infrastructure informatique) et de logiciels purs (notamment des bibliothèques, plus de talent et de financement dans l'apprentissage automatique). Ces deux facteurs sont étroitement liés, le second ayant besoin du premier pour fonctionner. Ces avancées ont favorisé une large diffusion des systèmes de surveillance et le passage d'un monde où le traçage et l'identification étaient une exception à un univers où ils sont devenus une norme.

Alors que ces technologies ont évolué et se sont progressivement répandues, les cadres législatifs concernés n'ont pas évolué au même rythme. Si de nombreux pays ont créé des cadres réglementaires spécifiques aux technologies biométriques dites de « première génération », on ne peut pas en dire autant des technologies développées plus récemment, qui en réalité fonctionnent pour la plupart sans aucune base juridique spécifique. Ces évolutions sont très inquiétantes, car les technologies biométriques impactent de plusieurs manières les droits humains et ont des effets encore plus intrusifs sur le droit à la vie privée et à la protection des données,[4] la dignité humaine,[5] la non-discrimination,[6] l'autodétermination et le droit d'accès à un recours efficace.

L'utilisation toujours croissante, omniprésente et souvent invisible des technologies biométriques par les pouvoirs publics et les entités privées, associée à leur capacité à identifier et pister des personnes et leurs comportements, a déjà un impact sur le droit à la liberté d'expression, en particulier la capacité à rester anonyme. Elle a également un impact considérable sur l'espace civique : le lieu où les individus exercent leurs droits, participent à la vie publique, s'expriment, se rassemblent et s'informent. L'espace civique étant un pilier fondamental de la démocratie, le déploiement et l'utilisation généralisés de ces technologies mettent en péril son existence même.[7] De plus, nous constatons un grave manque de transparence, notamment sur la question de savoir qui, comment et pourquoi ces technologies sont développées et déployées. Ce manque de transparence empêche la tenue d'un débat public et ouvert sur leur utilisation par les secteurs public et privé.

Récemment, la pandémie **de COVID-19 a renforcé** les appels à des solutions technologiques, donnant ainsi une impulsion supplémentaire aux acteurs publics et privés pour poursuivre le développement et le déploiement de ces technologies considérées comme « essentielles » dans la lutte contre la pandémie.[8] Il s'agit notamment de diverses applications de quarantaine ou de traçage de contacts,[9] de casques de surveillance utilisés par la police pour contrôler la température des personnes circulant dans les espaces publics.[10] Fait inquiétant : des acteurs tant publics que privés ont promu un discours mettant en opposition les droits humains et la protection de la santé publique,[11] poussant les populations à accepter un niveau sans précédent de surveillance de masse. Les mesures visant à protéger la population contre la COVID-19 sont certes indispensables et pourraient être facilitées par les technologies biométriques, mais ces dernières ne sont probablement pas le remède miracle annoncé. Quoiqu'il en soit, compte tenu de leur capacité à impacter les droits fondamentaux, ces technologies doivent rester sous surveillance attentive et respecter les normes internationales, et elles ne doivent jamais être normalisées.

Pour ARTICLE 19, il est essentiel de contribuer aux débats actuels sur l'impact de la biométrie sur la liberté d'expression et les droits de l'homme en général, et sur la manière dont cet impact pourrait être atténué, ou sur la possibilité d'interdire ces technologies. Dans cette note d'orientation, nous analyons les implications des technologies biométriques sur la liberté d'expression et la liberté d'information et nous formulons des recommandations à l'attention des États, des acteurs privés et de toute autre partie prenante concernée sur la manière de protéger et promouvoir la liberté d'expression dans ce contexte.

Cette note d'orientation est structurée comme suit :

- Premièrement, nous présentons quelques concepts fondamentaux utilisés dans le contexte des technologies biométriques ;
- Deuxièmement, nous présentons les normes internationales applicables en matière de droits humains dans le contexte de la biométrie ;
- Troisièmement, nous évaluons l'impact des technologies biométriques sur la liberté d'expression ;
- Quatrièmement, nous examinons deux études de cas spécifiques sur la biométrie et la liberté d'expression – l'une sur la reconnaissance faciale et l'autre sur la reconnaissance des émotions ;

Enfin, nous formulons des recommandations à l'attention des États, des acteurs privés et toute partie prenante concernée sur la manière de garantir la protection de la liberté d'expression dans la conception, le développement et le déploiement des technologies biométriques.

Nos recommandations aux États, aux acteurs privés et à toutes les parties prenantes concernées s'accompagnent d'un appel sincère à ne pas soustraire du débat public l'une des batailles les plus importantes pour définir les droits à la liberté d'expression et la liberté de réunion et l'existence même de l'espace civique pour notre génération et celles à venir.

Technologies biométriques : le contexte

Terminologie clé

Le terme « **biométrie** » se réfère généralement à l'analyse des caractéristiques physiologiques et comportementales propres à une personne. Il s'agit, entre autres, des empreintes digitales, de la voix, du visage, des modèles d'iris et de rétine, de la géométrie des mains, la démarche et même l'ADN d'une personne.

Les données biométriques sont définies comme « des données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou dactyloscopiques » (empreintes).[12] Les données biométriques changent irrévocablement la relation entre le corps et l'identité, car elles rendent les caractéristiques du corps humain « lisibles par une machine » et sujettes à une utilisation ultérieure.[13]

Le terme **technologie biométrique** correspond donc à une variété de technologies qui mesurent et analysent des caractéristiques humaines uniques, dont l'ADN, les empreintes digitales, les modèles de voix, les dimensions de la main, la rétine ou l'iris, et les signatures cardiaques.[14]

Plus récemment, les technologies biométriques comprennent, entre autres, la biométrie multimodale, la biométrie comportementale, la reconnaissance dynamique des visages, la reconnaissance de l'iris à distance et un certain nombre d'autres applications à différents stades de développement.[15]

La **reconnaissance faciale/du visage** relève d'une catégorie plus large de technologies biométriques et peut être définie comme le « traitement automatique d'images numériques qui contiennent les visages des personnes à des fins d'identification, d'authentification/de vérification ou de catégoration de ces personnes ».[16]

La **reconnaissance des émotions** correspond à une technologie biométrique basée sur l'apprentissage automatique et visant à identifier les états émotionnels des personnes et de les classer dans des catégories distinctes telles que la colère, la peur, la surprise, la joie, etc. Les données d'entrée peuvent inclure des images de visages, des mouvements corporels, le ton de la voix, les mots prononcés ou dactylographiés et des signaux physiologiques (par ex., la fréquence cardiaque, la pression artérielle, la fréquence respiratoire, le langage corporel ou le ton de la voix).[17]

Fiabilité des technologies biométriques

La précision et la fiabilité des applications biométriques de reconnaissance des émotions et des comportements restent encore à prouver. Un grand nombre d'études scientifiques alertent sur le fait que les expressions du visage et autres comportements extérieurs ne sont pas des indicateurs fiables des états émotionnels intérieurs.[18] Ces études mettent en garde contre des technologies souvent inexactes, qui peuvent conduire à des discriminations à l'encontre de minorités raciales, ethniques ou autres, voire à des postulats racistes à la base de ces technologies.[19] Des systèmes plus précis ne résoudraient pas ces problèmes ni les questions juridiques en vue. Et même si ces technologies biométriques se révélaient efficaces et précises (ou quand elles le seront), elles sont particulièrement invasives pour la sphère privée des individus et la protection des droits humains.

De plus, notons que nombre de technologies et applications biométriques actuelles reposent sur une perception historique inaugurée par les études sur les phénotypes inspirées par une classification des races et des postulats racistes (angle facial, cranioscopie/phrénologie, physiognomonie, anthropométrie).[20] Ces techniques ont été créées pour construire la prétendue « théorie scientifique des races » chère au monde colonial.[21] Bien que la validité scientifique de ces méthodes n'ait jamais été prouvée, l'application de ces techniques a marqué l'évolution de ce domaine d'étude, principalement dans l'application du profilage, de la classification et l'identification des stéréotypes utilisés dans l'anthropologie criminelle et les paramètres eugéniques.[22] Pour comprendre les enjeux liés à leur utilisation aujourd'hui, il est essentiel de se référer à l'histoire sociale des technologies biométriques.

En d'autres termes, cela signifie que l'acceptabilité du déploiement de la biométrie doit être fermement liée à un exercice d'équilibrage entre, d'une part, l'intérêt légitime de l'utilisation de la technologie, et d'autre part, la nécessité de garantir la protection des droits humains.

Déploiement des technologies biométriques : principaux usages et discours dominants

Les technologies biométriques sont actuellement utilisées de diverses manières et pour atteindre des objectifs divers. Les objectifs principaux sont les suivants :

- La protection de la **sécurité nationale, la lutte antiterroriste et la prévention et le contrôle de la criminalité** ont été invoqués pour justifier le déploiement des technologies biométriques dans divers contextes depuis deux décennies, notamment le contrôle et la gestion des frontières[23] les systèmes d'identification nationaux de la population.[24] Outre les discours sur la protection de la sécurité et la sûreté, les organes de maintien de l'ordre se sont servis de la reconnaissance faciale comme un outil ayant le potentiel d'aider à prévenir et déceler la criminalité, préserver la sécurité publique et poursuivre en justice des criminels[25], mais aussi prévenir la fraude ou le vol ou surveiller les mouvements des minorités.[26]
- Les pouvoirs publics ont également utilisé les technologies biométriques pour gérer et accéder à divers services de l'État et à la **fourniture de services publics**[27], notamment des systèmes de e-santé et des registres électoraux.[28] Ces technologies sont également utilisées à des fins privées ou sous la direction du secteur privé, notamment le **développement de projets de « villes intelligentes »**, les transports publics, l'accès aux écoles ou à des espaces physiques et en ligne.[29]

Le déploiement des technologies biométriques est généralement justifié par les nombreux avantages qu'elles sont censées procurer, notamment un accès rapide et sans encombre, des solutions économiques, la précision et la fiabilité, une sécurité renforcée, l'amélioration des prestations de bien-être. Cependant, la plupart de ces avantages ne sont pas prouvés, et l'évaluation de ces technologies ne tient pas suffisamment compte des larges compromis consentis en termes de protection des droits humains.

En outre, nous avons laissé libre cours au discours selon lequel la disponibilité d'une technologie suffit à justifier son utilisation. Nous devons résister fortement à cette approche. Les technologies biométriques ne sont pas neutres. Au niveau technique, la biométrie fait de nombreuses hypothèses ; au niveau institutionnel, elle est utilisée de manière fondamentalement discriminatoire et exacerbe les inégalités sociales et les discriminations historiques. Globalement, les technologies biométriques fonctionnent comme des systèmes sociotechniques et reflètent des valeurs et des hypothèses qui, comme débattu dans cette note d'orientation, sont très éloignées, voire incompatibles avec les droits humains.[30]

Normes internationales des droits humains et technologies biométriques

Normes des droits humains applicables

Il n'existe pas de normes internationales explicites en matière de technologies biométriques. Toutefois, leur déploiement et leur usage engagent un certain nombre de droits humains, notamment :

Le **droit à la liberté d'expression**, protégé par l'Article 19 de la Déclaration universelle des droits de l'homme (DUDH),[31] et entré en vigueur par l'Article 19 du Pacte international relatif aux droits civils et politiques (PIDCP)[32] ainsi que des traités régionaux des droits humains.[33] En vertu des normes internationales des droits humains, les restrictions de la liberté d'expression sont autorisées uniquement dans des circonstances très particulières (le dénommé test en trois parties) ; toutes les restrictions doivent être strictement et étroitement adaptées et ne doivent pas mettre en péril le droit lui-même.[34]

Le **droit d'accès à l'information** est reconnu en tant qu'élément du droit à la liberté d'expression. Le Comité des droits de l'homme des Nations Unies a interprété la portée et les limites du droit à l'information en 2011, déclarant que l'Article 19 du PIDCP garantissait le droit à l'information détenue par les organismes publics. Il exige que les États diffusent de manière proactive des informations dans l'intérêt du public et que l'accès soit « aisé, rapide, effectif et pratique ».[35] Le Comité a également stipulé que les États devaient mettre en place des « procédures nécessaires » telles qu'un texte de loi donnant effet au droit à l'information, que les frais à acquitter pour les requêtes d'information devaient être limités, que les réponses à ces requêtes devaient être fournies en temps opportun, que les autorités devaient fournir des explications en cas de rétention de l'information, et que les États devaient mettre en place des mécanismes d'appel.[36]

Le **droit à la liberté de réunion pacifique** est garanti par l'Article 20 par. 1 de la DUDH et il est entré en vigueur en vertu de l'Article 21 du PIDCP, de l'Article 5(d) de la Convention sur l'élimination de la discrimination raciale[37] et de certains traités régionaux.[38] En vertu de ces normes, les conditions d'une restriction admissible doivent satisfaire au même test en trois parties que les restrictions au droit à la liberté d'expression.[39]

Le **droit à la vie privée** est garanti par l'Article 12 de la DUDH et l'Article 17 du PIDCP et des traités régionaux.[40] En vertu de ces normes, la vie privée est un concept large lié à la protection de l'autonomie individuelle et à la relation entre un individu et la société, y compris les gouvernements, les entreprises et d'autres individus. Le droit à la vie privée est communément reconnu comme un droit fondamental garantissant la dignité humaine et d'autres valeurs. Les restrictions du droit à la vie privée doivent également satisfaire aux exigences du test en trois parties.[41]

Les droits à la liberté d'expression et à la vie privée se renforcent mutuellement ; a fortiori à l'ère du numérique.[42] Le respect de la vie privée est une condition préalable à l'exercice de la liberté d'expression : sans cela, les individus n'ont plus d'espace pour penser, s'exprimer et développer leur voix. Il s'ensuit que, si des États développent ou utilisent la biométrie de manière à entraver le droit à la vie privée, cette utilisation doit être soumise au test en trois parties de légalité, nécessité et proportionnalité.

De plus, la **protection des données à caractère personnel** (protection des données) est reconnue par le Comité des droits de l'homme (CDH), l'organe chargé d'interpréter le PIDCP, comme un élément fondamental du droit à la vie privée.[43] La Résolution de l'Assemblée générale des Nations Unies sur les Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel[44] adoptée en 1990 énonce 6 principes fondamentaux de la protection des données fondés sur des pratiques d'information loyales. Au niveau régional, la protection des données personnelles est également garantie par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe (Convention 108)[45], par la Charte de l'UE,[46] la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention sur la cybersécurité de l'UA)[47] et les Principes sur la vie privée et la protection des données personnelles de l'Organisation des États américains.[48]

Le droit international des droits de l'homme reconnaît également que les personnes souhaitant savoir si, et pourquoi, des technologies biométriques ont été utilisées par l'administration publique à leur endroit sont habilitées à le faire en vertu de la législation sur la protection des données. Parmi ces droits figure celui d'être informé lorsque des données à caractère personnel sont collectées auprès de la personne concernée, contraignant le responsable du traitement à fournir certaines informations.[49] Ce droit a été largement intégré dans le droit international, ainsi que dans les principaux accords régionaux sur la protection des données. Dans son Observation générale n° 16, le Comité des droits de l'homme a noté que ce droit était nécessaire pour garantir le respect du droit à la vie privée.[50] Ce droit a été largement intégré dans le droit international, ainsi que dans les principaux accords régionaux sur la protection des données.[51] Selon le Règlement général sur la protection des données (RGPD)[52], chaque personne a un droit bien établi d'être informée et deux cas distincts sont envisagés : d'une part, si les données personnelles sont directement obtenues auprès de la personne concernée (Article 13) et d'autre part, si les données personnelles n'ont pas été collectées auprès de la personne concernée (Article 14).

L'importance de garantir le droit d'accès aux données biométriques et leur transparence a été mise en évidence en Europe par l'Agence des droits fondamentaux (FRA), notamment en ce qui concerne la collecte de données à caractère personnel incluant les empreintes digitales de demandeurs d'asile et de visa, ainsi que de migrants en situation irrégulière.[53] Certains États ont également instauré la protection de ces droits et des protections de la vie privée dans leur législation nationale.[54]

Les organes internationaux de défense des droits de l'homme ont également progressé dans la reconnaissance d'un **droit à l'anonymat** en tant qu'élément important du droit à la liberté d'expression et à la vie privée. Cette reconnaissance a des implications sur les technologies biométriques servant à identifier les individus à leur domicile et dans les espaces publics. Par conséquent, l'immixtion de l'État dans l'anonymat devrait être soumise au test en trois parties de légalité, nécessité et proportionnalité, comme pour toute autre immixtion dans ces droits.[55]

Le **droit à la non-discrimination et le droit à l'égalité** sont protégés par l'Article 2 et l'Article 7 de la DUDH, et mis en application à travers l'Article 2 et l'Article 26 du PIDCP, l'Article 2(2) du Pacte international relatif aux droits économiques, sociaux et culturels (PIDESC), ainsi que des traités et instruments régionaux.[56] Le droit à l'égalité implique que « toutes les personnes sont égales devant la loi et ont droit d'être protégées sans discrimination, notamment de race, de couleur, de sexe, de langue, de religion, d'opinion politique et de toute autre opinion, d'origine nationale ou sociale, de fortune, de naissance ou de toute autre situation ».[57]

Normes des droits humains relatives aux technologies biométriques

Bien qu'il n'existe pas de normes internationales portant explicitement sur les technologies biométriques, il existe un corpus émergent de normes qui sont pertinentes pour leur développement et leur déploiement.

Premièrement, les organes de défense des droits de l'homme reconnaissent de plus en plus fréquemment l'impact des nouvelles formes de traitement des données sur les droits humains. S'agissant du profilage, par exemple, qui peut impliquer l'utilisation de systèmes biométriques pour obtenir, déduire ou prédire des informations sur des personnes afin d'évaluer ou apprécier certains aspects les concernant, le Conseil des droits de l'homme s'est inquiété en mars 2017 que :

> Le traitement automatique des données à caractère personnel aux fins de l'établissement de profils individuels peut aboutir à une discrimination ou à des décisions pouvant avoir des conséquences sur l'exercice des droits de l'homme, notamment les droits économiques, sociaux et culturels…[58]

Deuxièmement, concernant plus spécifiquement les données biométriques :

- La Convention modernisée du Conseil de l'Europe pour la protection des données à l'égard du traitement automatisé des données à caractère personnel (la Convention 108+) stipule que les données biométriques identifiant de manière unique une personne ne peuvent être autorisées que lorsque des garanties appropriées sont inscrites dans la loi, complétant celles de la Convention 108.[59]

- Le Règlement général sur la protection des données (RGPD) de l'UE interdit le traitement des données biométriques dans le but d'identifier de manière unique une personne physique, sous réserve d'exceptions limitées.[60] En outre, le RGPD traite les données biométriques utilisées à des fins d'identification comme des « données de catégorie spéciale », ce qui signifie qu'elles sont considérées comme plus sensibles et éligibles à plus de protection. La même approche est adoptée dans les Normes de protection des données personnelles des États ibéro-américains.[61]
- La Convention sur la cybersécurité de l'Union africaine impose une autorisation préalable des autorités nationales de protection des données pour le traitement de données à caractère personnel impliquant des données biométriques.[62]

D'autres instruments internationaux fournissent des orientations utiles sur la manière d'évaluer l'usage des technologies biométriques et leur impact sur les droits de l'homme. Par exemple, le Haut-Commissariat des Nations Unies aux droits de l'homme, dans son rapport sur le droit à la vie privée à l'ère du numérique, a souligné les préoccupations concernant l'utilisation de ces données, le risque d'abus graves et la possibilité que des États se lancent dans des projets fondés sur la biométrie sans garanties juridiques et procédurales adéquates.[63] Le rapport recommande que les États, entre autres :

> [veillent] à ce que les systèmes à forte intensité de données, y compris ceux qui impliquent la collecte et la conservation de données biométriques, ne soient instaurés que lorsque les États peuvent démontrer qu'ils sont nécessaires et proportionnés pour atteindre un objectif légitime.[64]

Par ailleurs, trois mandataires spéciaux ont déjà mis en garde contre les systèmes biométriques :

- En 2019, le Rapporteur spécial des Nations Unies sur les droits à la liberté de réunion pacifique et à la liberté d'association a déclaré dans son rapport que "[l]e recours à des techniques de surveillance aux fins de la surveillance indiscriminée et non ciblée des personnes qui exercent leurs droits à la liberté de réunion pacifique et à la liberté d'association devrait être interdit… »[65].
- Le Rapporteur spécial des Nations Unies sur le droit à la vie privée a remis en question la nécessité et la proportionnalité des systèmes biométriques.[66]
- Le Rapporteur spécial des Nations Unies sur la liberté d'expression a soulevé des préoccupations similaires concernant l'impact des systèmes biométriques sur les défenseurs des droits humains, les journalistes, les personnalités politiques et les enquêteurs de l'ONU.[67]

La jurisprudence des instances internationales et des tribunaux régionaux et nationaux fournit également des indications générales sur les normes à appliquer en matière de technologies d'identification biométrique. En particulier, la Cour européenne des droits de l'homme (Cour européenne) a souligné la nécessité de garantir un équilibre entre la protection des droits fondamentaux et le développement de nouvelles technologies, estimant que la conservation « générale et aveugle » de données biométriques était une « immixtion disproportionnée » dans le droit à la vie privée, dans la mesure où elle ne satisfait pas aux exigences de la CEDH et ne peut être considérée comme « nécessaire dans une société démocratique ».[68]

Une approche partiellement différente semble avoir été adoptée dans le domaine de la **lutte contre le terrorisme**. En 2017, le Conseil de sécurité des Nations Unies a décidé que les États devaient développer et mettre en œuvre des systèmes de collecte et de partage de données biométriques à des fins de lutte contre le terrorisme.[69] De même, l'Addendum de 2018 aux Principes directeurs de Madrid note l'utilité des données biométriques.[70] En conséquence, les systèmes biométriques sont considérés comme un outil légitime pour l'identification des suspects de terrorisme.

Néanmoins, même lorsque l'objectif est la lutte contre le terrorisme, l'utilisation des technologies biométriques doit être conforme aux normes internationales, et en particulier aux principes de nécessité et proportionnalité. Le Compendium des Nations Unies sur les pratiques recommandées pour l'usage et le partage responsables de la biométrie pour la lutte contre le terrorisme[71] (Compendium des Nations Unies) pourrait être considéré comme un premier pas vers une approche plus centrée sur les droits de l'homme, mais ce cadre n'est pas suffisamment adéquat.

Responsabilité du secteur privé en matière de droits humains

Si le droit international des droits de l'homme impose aux États des obligations de protéger, promouvoir et respecter les droits humains, il est largement reconnu que le secteur privé a également la responsabilité de respecter ces droits.[72]

Les Principes directeurs relatifs aux entreprises et aux droits de l'homme (Principes directeurs) constituent un point de départ pour définir le rôle du secteur privé dans la protection des droits humains sur Internet.[73] Ces principes reconnaissent la responsabilité des entreprises commerciales de respecter les droits humains, indépendamment des obligations de l'État ou de la mise en œuvre de ces obligations, et invitent les entreprises à adopter plusieurs mesures.[74] Ces mesures recommandent aux entreprises, notamment, d'intégrer dès la conception des garanties des droits humains afin d'atténuer les impacts négatifs, de mobiliser et agir collectivement pour renforcer leur pouvoir vis-à-vis des autorités gouvernementales ; et de prévoir des recours en cas d'impacts négatifs sur les droits humains.

Divers intervenants ont appelé à une réglementation. Dans une certaine mesure, cela est également vrai pour les entreprises technologiques qui, après avoir répondu aux appels initiaux à adopter des normes « éthiques » ou « dignes de confiance » sur les technologies biométriques, ont reconnu qu'un pas de plus était nécessaire, et ont appelé aussi à une réglementation. Cependant, les propositions « éthiques » et réglementaires des entreprises de technologie ont été rarement appropriées, voire jamais. De plus, ce sont des appels à des mesures douces plutôt qu'à des cadres adéquats de protection des droits de l'homme en biométrie.[75]

Enfin, il est de plus en plus reconnu que les droits de l'homme doivent être à la base des **normes et protocoles techniques,** ces derniers pouvant avoir un impact substantiel sur l'exercice des premiers.[76] Toutefois, malgré cette reconnaissance croissante, de nombreuses organisations techniques ou commerciales n'inscrivent ni explicitement ni adéquatement les droits de l'homme dans leurs politiques. Et ce alors qu'elles deviennent rapidement des passerelles et des facilitateurs de l'exercice de la liberté d'expression et de la liberté de réunion dans la mesure où elles développent la majorité des systèmes de technologie biométrique. Des initiatives telles que les Principes de Google en matière d'IA[77] peuvent être considérées comme une première étape dans cette direction, mais elles ont démontré leur lacunes et n'ont pas su, à ce jour, assurer un niveau suffisant de transparence et de responsabilité au niveau des entreprises.
Technologies biométriques et droits à la liberté d'expression et d'information

Technologies biométriques et droits à la liberté d'expression et d'information

Technologies biométriques et droits humains : défis globaux

Avant de discuter des défis soulevés par les technologies biométriques pour la protection du droit à la liberté d'expression et d'information, ARTICLE 19 souhaite rappeler les problèmes posés par ces technologies du point de vue des droits humains :

Collecte, stockage et rétention de données

Le développement et le déploiement des technologies biométriques impliquent la collecte et la génération de grandes quantités de données personnelles sensibles. Les données biométriques sont une catégorie particulière de données personnelles qui, en raison de leur capacité à dévoiler des informations intimes sur une personne (origine raciale ou ethnique, sexe, etc.), nécessitent des garanties supplémentaires et une protection renforcée. D'emblée donc, la technologie biométrique est très invasive. De plus, les bases de données s'appuient souvent sur des méthodes de collecte problématiques (par exemple, échantillons de données pouvant ne pas être représentatifs de l'ensemble de la population) et peuvent avec des biais qui reflètent des modèles existants de stéréotypes sociétaux.[78]

Tout aussi problématique est la pratique répandue de la rétention indiscriminée de données biométriques qui ne répond pas aux critères de nécessité et proportionnalité.[79] Autrement dit, les processeurs de données conservent souvent les données biométriques plus longtemps que nécessaire pour l'objectif visé.

En outre, ces bases de données massives peuvent être réutilisées à d'autres fins, ce qui pose le problème du « dévoiement des missions », ou d'une extension des « technologies » à la collecte de données et/ou l'exécution de fonctions non approuvées à l'origine. Certains faits indiquent déjà que des bases de données biométriques créées à des fins précises sont réutilisées ou utilisées à mauvais escient à d'autres fins ;[80] dans ces cas, même si des personnes ont initialement donné leur consentement à l'utilisation de leurs données biométriques à certaines fins, le consentement ne couvre pas la nouvelle utilisation, qui doit être considéréee comme illégale.

Potentielles failles de sécurité

Les failles de sécurité des bases de données sont difficiles à détecter et extrêmement coûteuses à réparer. Il est encore plus difficile pour les individus de demander réparation lorsqu'ils subissent un préjudice du fait de ces failles. En effet, les données biométriques ne sont pas comme des mots de passe que l'on peut changer en cas de problème ; au contraire, elles peuvent servir à identifier et pister un individu toute sa vie. Les risques de sécurité sont plus élevés dans le cas de bases de données volumineuses et centralisées

et affecteront plus particulièrement des communautés déjà marginalisées ; de ce fait, les bases de données centralisées ne doivent être envisagées qu'en cas de nécessité absolue et en l'absence de toute autre alternative viable disponible.[81]

Enfin, les risques de sécurité sont plus élevés dans les pays où l'industrie de haute technologie et l'infrastructure de sécurité des données ne sont pas – ou pas suffisamment – développées. Dans ce contexte de défiance, la rétention des données biométriques des citoyens par un gouvernement ou d'autres acteurs peut susciter des inquiétudes.

Problème de la « boîte noire »

Les nouvelles applications biométriques reposent de plus en plus sur l'aprentissage automatique, soulevant le problème de la « boîte noire ».[82] L'impénétrabilité des processus et systèmes d'apprentissage automatique est un défi fondamental pour la responsabilisation et la possibilité de réparation dans le contexte de la prise de décisions automatisée. Compte tenu du biais important en faveur de l'automatisation de la prise de décisions, et de l'imperfection et la maladresse fréquente des systèmes techniques, il est difficile, voire impossible, de remettre en question le profilage et la correspondance, notamment lorsque la logique et les hypothèses de base des décisions prises ne sont pas claires. Par conséquent, il est tout aussi difficile, voire impossible, pour les tribunaux de juger de la véracité des allégations de preuves.

Échelle

Les technologies biométriques sont actuellement déployées à une échelle sans précédent, conduisant potentiellement à un état de surveillance massive dans plusieurs parties du monde. Des aéroports aux places publiques, des caméras thermiques aux systèmes d'identification des veines des doigts, l'utilisation de ces technologies à des fins d'identification et de surveillance des individus est en train de se généraliser.[83]

Cadres juridiques nationaux inadéquats ou inexistants

L'absence ou l'inadéquation des cadres juridiques nationaux pour le développement et le déploiement des technologies biométriques est un problème grave. Quoique nécessaire, la législation sur la protection des données (si elle existe en premier lieu) pourrait ne pas être suffisante pour faire face à tous les problèmes qui se posent. Pour y remédier, elle doit contenir des règles précises sur, entre autres, le consentement, la légalité du traitement, la limitation des finalités. De plus, divers cadres de protection des données prévoient des exceptions lorsque le traitement de données à caractère personnel est fait à des fins de maintien de l'ordre. Ces exceptions sont souvent formulées de manière floue et large, sans garanties suffisantes pour la protection des données personnelles. Un cadre législatif approprié et conforme aux normes internationales est nécessaire pour le développement et l'utilisation des technologies biométriques par les acteurs tant publics que privés.

Nécessité et proportionnalité

Les technologies biométriques sont développées et déployées à des fins de plus en plus nombreuses. La disponibilité de la technologie est souvent considérée comme un motif suffisant pour son utilisation, sans évaluation adéquate de la légitimité de l'objectif. Le développement et le déploiement de ces technologies à des fins contraires au respect de la dignité humaine, par exemple à des fins de surveillance numérique totale, d'humiliation ou de manipulation, ne devraient jamais être autorisés.[84] Même lorsqu'un objectif légitime est identifié, le déploiement de ces technologies ne satisfait pas toujours aux critères étroits de nécessité et proportionnalité : la technologie doit être absolument nécessaire pour atteindre l'objectif visé et il ne doit exister aucun autre moyen moins invasif de le faire. Si elle ne répond pas à ces critères, son utilisation ne doit pas être autorisée, indépendamment de sa disponibilité ou de son attractivité.[85]

Absence de recours en cas de violation des droits humains

Aucun acteur public ou privé n'a mis en place des recours efficaces en cas de violations des droits humains du fait de ces technologies. Par exemple, si la technologie biométrique conduit à un résultat discriminatoire, aucune mesure précise n'a été mise en place pour traiter ces cas. De même, si la police utilise la technologie biométrique pour pister des individus participant à des expressions politiques, religieuses ou autres expressions protégées, on ne sait pas comment ces individus pourraient chercher réparation. Dans tous les cas, la condition prélable à un recours efficace est que les personnes soient conscientes que leurs données biométriques sont en cours de traitement ou qu'une décision les concernant a été prise par le biais des technologies biométriques. Ce n'est pas le cas dans une vaste majorité des cas.

Répercussions des technologies biométriques sur la liberté d'expression et le droit à l'information

Certains défis soulevés par les technologies biométriques pour la liberté d'expression et le droit à l'information ne sont pas fondamentalement différents de ceux posés par les technologies précédentes, mais les caractéristiques spécifiques de la biométrie engendrent d'autres préoccupations. Il s'agit notamment de :

Effet dissuasif de la surveillance de masse sur la liberté d'expression

Si la législation des droits de l'homme a évolué au point de reconnaître que les protections contre la surveillance de masse illicite et arbitraire sont principalement garanties par le droit à la vie privée,[86] il est de plus en plus admis que la surveillance de masse a aussi un effet dissuasif sur la liberté d'expression des individus.[87] Si des technologies biométriques sont utilisées à des fins d'identification ou de profilage dans les espaces publics – par exemple, des algorithmes de reconnaissance faciale pour traiter les images faciales enregistrées par des caméras vidéo dans les rues, les places, les métros, les stades ou les salles de concert –, elles réduisent à néant la capacité

des individus à communiquer anonymement en toute confiance, et à rester anonymes dans leurs déplacements et leurs agissements dans les espaces publics ; cela affecte aussi directement la manière dont les ONG fonctionnent en termes de protection de leurs sources et dans leur rôle de « chien de garde ».[88] Selon certaines études, le fait de savoir que l'on est surveillé et pisté peut dissuader certains de participer à des rassemblements publics, ou à la vie sociale et culturelle, et d'exprimer librement leur pensée, leur conscience et leurs croyances religieuses dans les espaces publics.[89]

Impact sur la liberté d'expression de certaines catégories d'individus

Les technologies biométriques peuvent avoir un impact plus grave sur le droit à la liberté d'expression de certaines catégories d'individus susceptibles d'être ciblés dans l'exercice de ce droit, ou sur des minorités. Par exemple, les journalistes pourraient être dissuadés de mener des enquêtes ou de nouer des contacts avec leurs sources d'information s'ils se savent surveillés/espionnés et identifiés par des technologies biométriques dans des espaces publics ou privés.[90] La peur d'être pisté et surveillé peut avoir un effet dissuasif important sur eux, et cela à son tour peut avoir un effet négatif sur la qualité du journalisme et des reportages d'investigation, et entraver le rôle des médias dans nos sociétés. Les activistes et les opposants politiques peuvent partager les mêmes craintes, et donc les mêmes incitations à l'autocensure. Par exemple, ils peuvent être dissuadés d'exercer leur droit de manifester si, du fait des technologies biométriques déployées par l'État, ils sont classés dans des catégories spécifiques, notamment celle de « manifestants réguliers » ou autres catégories similaires.[91]

Nécessité de transparence et accès à l'information

Le déploiement généralisé des technologies biométriques et la mise en place de bases de données à grande échelle conjugués à un manque général de transparence sur le déploiement et l'utilisation de ces technologies soulèvent également des problèmes pour le droit d'accès à l'information des individus. Quand des gouvernements collectent et stockent des quantités massives de données biométriques, il est essentiel que le public ait aussi le droit de savoir comment ces informations sont utilisées par le gouvernement. Cela constitue un véritable problème, notamment lorsque ces technologies sont déployées pour identifier et surveiller des espaces publics.

Par ailleurs, trop peu d'informations sont disponibles sur les développeurs de ces technologies, sur le type de technologie qu'ils développent et sur qui les déploie, comment et à quelles fins. On ignore également si les développeurs et les vendeurs exercent une forme quelconque de diligence raisonnable pour évaluer le bilan des acheteurs en matière de droits de l'homme.[92]

Les États et les acteurs privés entretiennent une collaboration étroite sur les marchés des technologies biométriques. Toutefois, la teneur et les conditions des partenariats public-privé et des marchés publics qui approvisionnent les autorités publiques ne sont pas connues du public. En règle générale, les États ne communiquent pas sur leurs

relations avec les développeurs, y compris sur les critères d'évaluation des offres et d'attribution des marchés. C'est donc dans un environnement opaque et confidentiel que ces technologies sont achetées et utilisées, sans faire l'objet d'un examen public, et avec de faibles garanties procédurales et une surveillance inefficace. Comme nous l'avons vu précédemment, les autorités publiques chargées des technologies biométriques semblent ne pas mener des évaluations d'impact adéquates, lesquelles sont une composante importante de la redevabilité.[93]

Les lois sur la liberté d'information/le droit à l'information sont de puissants outils juridiques dont les individus, les journalistes et les activistes peuvent disposer pour renforcer la transparence du gouvernement, et elles peuvent aussi concerner les données biométriques utilisées par les gouvernements.[94] Toutefois, les tentatives d'accès à l'information biométrique détenue par les organismes publics par le biais des lois sur le droit à l'information posent de nombreux problèmes.[95] S'il semble incontestable que des systèmes de stockage et de traitement de quantités importantes de données biométriques présentent un réel intérêt pour le grand public,[96] compte tenu notamment de la quantité de personnes auprès desquelles ces données seront collectées, les organismes publics omettent souvent de divulguer des informations, notamment sur les systèmes d'identification. Ces informations sont fréquemment divulguées après des procédures judiciaires, souvent longues et coûteuses dans la plupart des juridictions, et les demandeurs, dont les journalistes, les scientifiques et les activistes, préfèrent souvent abandonner.

Il convient également de noter que certaines initiatives se sont attaquées au manque de transparence des technologies biométriques en reconnaissant qu'il était nécessaire de concilier les besoins de la police et les préoccupations éthiques et que la mise en œuvre de telles politiques devait être fondée sur l'ouverture et la transparence.[97]

Technologies biométriques et liberté d'expression : études de cas

Reconnaissance faciale

Objectifs et utilisation des technologies de reconnaissance faciale

Par reconnaissance faciale, on entend le traitement automatisé d'images numériques contenant des visages d'individus à trois fins principales :

- **Vérification** : comparaison de deux modèles biométriques en vue de déterminer si la personne apparaissant dans les deux modèles est la même (comparaison un-à-un) ;
- **Identification**, comparaison du modèle d'une personne avec un certain nombre de modèles dans une base de données afin de vérifier si le premier s'y trouve (comparaison un-à-plusieurs). Lorsque la reconnaissance faciale est utilisée en temps réel à cette fin, elle est également appelée « reconnaissance faciale automatique ou en temps réel » (RFA ou RFTR). Bien que les authentifications un-à-un et un-à-plusieurs suscitent toutes les deux des inquiétudes[98], la reconnaissance faciale à des fins d'identification un-à-plusieurs est celle qui entrave le plus le droit à la liberté d'expression ;
- **Catégorisation**, utilisée pour le profilage des personnes en fonction de leurs caractéristiques personnelles, notamment le sexe, l'âge et l'origine ethnique.[99]

Le déploiement de la reconnaissance faciale a régulièrement augmenté ces dernières années. Divers États et municipalités dans le monde envisagent ou mettent en œuvre des règles prévoyant son déploiement massif dans les espaces publics à des fins de maintien de l'ordre.[100] Dans certains pays, la rhétorique de la sécurité publique est largement utilisée pour justifier cette surveillance croissante des espaces publics à des fins de sécurité.[101]

Des acteurs privés utilisent également la reconnaissance faciale à des fins diverses. Par exemple, des milliers de commerçants au détail y ont recours pour vérifier si les clients de leurs magasins apparaissent dans les images de voleurs connus.[102] Certains sont même allés plus loin en examinant les réactions de leurs clients face à certains articles, [103]ou en permettant à leurs clients de réaliser des achats grâce à cette technique.[104] Des sociétés de spectacle vivant l'utilisent pour identifier les détenteurs de billets et faciliter l'accès à des services ou des salles. Des compagnies de transport ont déployé ce système dans des panneaux d'affichage à l'intérieur de stations de métro afin d'identifier les réactions des passants aux publicités (satisfait, insatisfait, surpris et neutre) et en déduire leurs supposées caractéristiques physiologiques (âge et genre) ;[105]

ou pour prévenir les fraudes et vérifier l'identité de leurs chauffeurs.[106] Comme nous l'avons mentionné précédemment, de nombreux fabricants de smartphones permettent à leurs utilisateurs de déverrouiller leur appareil grâce à une fonction de reconnaissance faciale.[107]

En revanche, à l'échelon régional, de nombreuses municipalités prennent la direction opposée et interdisent l'usage de ce système à certaines fins.[108] De même, un certain nombre de développeurs de technologies de reconnaissance faciale ont récemment pris des mesures (quoique limitées) en vue de restreindre ou suspendre leur développement et leur déploiement.[109] La portée de ces engagements n'est pas encore claire, mais ces initiatives peuvent être perçues comme un signal des pressions croissantes en vue de limiter ou interdire l'utilisation indiscriminée de la reconnaissance faciale à des fins de maintien de l'ordre. Toutefois, très peu de voix s'élèvent pour dénoncer ces abus ou elles n'attribuent pas la même importance aux dangers du déploiement purement privé des systèmes de détection faciale. Cette attitude contraste fortement avec l'usage toujours croissant de la reconnaissance faciale par les acteurs privés, soit-il limité et localisé ou largement déployé.[110]

Avec la **pandémie de COVID-19,** les technologies de reconnaissance faciale ont suscité un regain d'intérêt. Les développeurs ont profité de la crise sanitaire pour proposer des usages nouveaux et plus larges à des acteurs publics et privés, et les gouvernements la déploient progressivement à des fins de surveillance, pour veiller au respect des quarantaines ou suivre les chaînes de contamination.[111] L'engouement pour la reconnaissance faciale est tel que les développeurs s'attaquent déjà aux défis techniques soulevés par le port obligatoire ou recommandé des masques de protection. Plusieurs entreprises ont commencé à développer des algorithmes de reconnaissance « périoculaire » qui détectent et reconnaissent des visages en se basant uniquement sur la zone des yeux, entre les pommettes et les sourcils.[112] Pourtant, la reconnaissance faciale est présentée comme une solution à la COVID-19 alors qu'aucune preuve ne confirme l'efficacité de la mesure de surveillance, ou même qu'elle fonctionne sur des personnes masquées. Ces initiatives semblent plutôt participer d'un effort plus large visant à encourager une infrastructure de surveillance en constante expansion en tant que composante essentielle de la réponse à la pandémie.[113]

Problèmes posés par la reconnaissance faciale en matière de droits humains

Tous les usages de la reconnaissance faciale – tant par le secteur public que par le secteur privé – ont un impact sur les droits humains. Parfois, cette technologie est plus dangereuse aux mains des acteurs privés. Les consommateurs sont souvent convaincus de l'utiliser dans leur sphère privée (domicile, relations familiales et amicales ou au travail) à des fins encore plus futiles, et ni justifiées ni proportionnées à la violation des droits humains qu'elle engendre.

Beaucoup de problèmes suscités par le déploiement et l'utilisation de la reconnaissance faciale sont similaires à ceux précédemment mentionnés pour potentiellement la quasi-totalité des technologies biométriques. Cette technologie est souvent déployée sans base juridique, en l'absence de cadre législatif spécifique ou de garantie adéquate des droits humains, et sans consultation préalable du public. Toutefois, compte tenu de ses caractéristiques spécifiques, elle pourrait poser des problèmes plus particuliers pour les droits humains et la liberté d'expression que ceux mis en évidence pour les technologies biométriques en général. Cela s'explique par le fait que la reconnaissance faciale a deux particularités qui la différencient des autres. D'une part, ses données peuvent être collectées à l'insu d'une personne, et d'autre part, elle peut marquer des caractéristiques protégées en vertu du droit international (race, religion, sexe et autres).

On peut mentionner les préoccupations clés suivantes :

- **Consentement** : Les technologies de reconnaissance faciale ne nécessitent pas de contact ni de comportement actif de la cible. Pour cette raison, les cibles peuvent faire aisément l'objet d'une reconnaissance faciale à leur insu ou sans leur consentement.[114] Par exemple, certaines plates-formes de médias sociaux, en particulier Facebook (parmi les premières à avoir développé des algorithmes de reconnaissance faciale), ont largement utilisé les images de visages de leurs usagers pour alimenter et « entraîner » leur système de reconnaissance faciale, sans informer leurs usagers ni chercher leur consentement.[115] Même lorsque l'utilisation de la reconnaissance faciale est dévoilée, il est parfois difficile de déterminer quand un consentement valide est fourni. Par exemple, des études ont fait valoir que l'utilisation de la reconnaissance faciale par Facebook violait dans tous les cas les normes du consentement en occultant le risque et en détruisant l'autonomie collective.[116]
- **Manque de transparence** : Alors que le manque de transparence est une préoccupation générale en matière de technologies biométriques, la reconnaissance faciale suscite des inquiétudes encore plus importantes en raison de son caractère hautement intrusif. Comme nous l'avons expliqué précédemment, l'image d'un visage peut être collectée sans que la cible en soit consciente. Conjugué au manque de transparence sur le déploiement de la technologie par les acteurs tant publics que privés, ce problème laisse les individus dans l'obscurité, et les expose totalement à des abus ou des utilisations à mauvais escient.
- **Exactitude** : À l'instar des autres technologies biométriques, la reconnaissance faciale est basée sur une estimation statistique de correspondance entre les éléments comparés ; elle est de ce fait intrinsèquement faillible. De nombreuses études démontrent que la reconnaissance faciale manque totalement d'exactitude, notamment dans le contexte de groupes sous-représentés ou historiquement défavorisés. Pour que la reconnaissance faciale soit exempte de tout biais, des questions comme la qualité des données et l'exhaustivité des bases de données «d'entraînement» sont essentielles. Si la qualité des données n'est pas garantie, ou si les bases de données d' « entraînement » sont sur ou sous-représentatives de certaines

caractéristiques, la reconnaissance faciale ne peut jamais être fiable.[117] Cela pose, en particulier, un problème dans les cas de biais raciaux.[118] L'exactitude de ces algorithmes est excesssivement importante, car une erreur d'identité est plus qu'un inconvénient et peut avoir de graves conséquences. Par exemple, un faux négatif dans une recherche un-à-un pourrait ne pas permettre à un individu d'accéder à des services ou des locaux. Un faux positif dans une recherche un-à-plusieurs établit une correspondance incorrecte sur une liste de candidats qui justifient un examen plus approfondi ou qui sont étiquetés d'une certaine manière. Quand cela se produit, il semble souvent difficile, voire impossible, de renverser la situation.[119]

- **Peu ou pas de contrôle** : À quelques exceptions près, l'utilisation de la reconnaissance faciale par les forces de l'ordre fait l'objet de peu de surveillance, voire aucune, dans plusieurs pays. Dans la plupart des endroits, rien n'empêche explicitement les pouvoirs publics de l'utiliser sur les flux d'images de caméras en direct, transformant tous les passants en suspects potentiels d'une parade d'identification virtuelle de la police ; aucune règle ne régit la détention des données collectées par le biais de la reconnaissance faciale. Le recours à cette technologie par des acteurs privés suscite également des inquiétudes : en l'absence de controle approprié, les entreprises déploient la reconnaissance faciale à des fins et par des moyens qui sont contraires aux normes des droits humains.
- **Absence de normes** : Les normes et les meilleures pratiques en matière de déploiement de la reconnaissance faciale sont encore en cours d'élaboration.[120] Des appels ont également été lancés pour concevoir un code de conduite statutaire.[121] Malgré l'absence de normes, les technologies de reconnaissance faciale continuent d'être utilisées dans les espaces publics et commerciaux du monde entier. Ce vide juridique dangereux ne peut être comblé par des appels **à une utilisation éthique** : les préoccupations éthiques doivent être traitées par un cadre réglementaire adéquat conforme aux normes internationales des droits humains.[122]
- **Double usage** : Une grande majorité des systèmes de reconnaissance faciale commercialisés par des acteurs privés peuvent être utilisés à d'autres fins que celles pour lesquelles ils ont été conçus ou prévus. En d'autres termes, le potentiel d'abus est stupéfiant. L'absence de cadre réglementaire offrant des garanties contre le double usage, une définition des responsabilités et prévoyant des recours, le cas échéant, ne fait qu'amplifier les risques.
- Manque de nécessité et de proportionnalité : De nombreuses cas d'utilisation de la reconnaissance faciale ont déjà été considérées comme non conformes au test de nécessité et de proportionnalité. Entre autres, l'utilisation dans les écoles, pour contrôler l'accès des élèves, a été condamnée tant par les autorités chargées de la protection des données que par des tribunaux.[123]

Problèmes posés par la reconnaissance faciale pour la liberté d'expression et d'information

Du point de vue de la liberté d'expression, le déploiement et l'utilisation de la reconnaissance faciale soulèvent les problèmes supplémentaires suivants :

- **Le droit à l'anonymat** : L'utilisation de la reconnaissance faciale dans les espaces publics, notamment la reconnaissance en temps réel, est un problème évident pour l'anonymat. Elle limite la possibilité de circulation et d'utilisation anonymes des services, et plus généralement la possibilité de rester inaperçu. La protection de l'espace public est cruciale pour l'exercice des droits et libertés fondamentaux, en particulier le droit à la liberté d'expression. Si la reconnaissance faciale est largement déployée, par exemple sur des vidéos de surveillance ou des caméras portées par la police, elle peut redéfinir considérablement la nature de l'espace public[124]; son utilisation ne réussira pas le test de nécessité et proportionnalité. L'utilisation aveugle et non ciblée de la reconnaissance faciale conduisant à une surveillance de masse dans les espaces publics ne devrait jamais être autorisée.[125]
- **Droit de protester** : L'usage de la reconnaissance faciale dans les manifestations peut dissuader les individus d'y participer, et avoir des implications négatives évidentes sur le fonctionnement efficace de la démocratie participative[126]. Même si elle est appliquée aux violences policières lors de manifestations, elle peut encore avoir un impact sur des manifestants qui ne commettent pas de violences ou sur de simples passants. En d'autres termes, le déploiement de la reconnaissance faciale peut entraîner un effet paralysant où des individus modifient leur comportement et s'abstiennent d'exercer leur droit de manifester. Des personnes pourraient ainsi être dissuadées de rencontrer des individus ou des organisations, d'assister à des réunions particulières ou de participer à certaines manifestations. De nouveau, l'utilisation de la reconnaissance faciale en temps réel dans les espaces publics peut permettre de cibler des journalistes, engendrant un effet dissuasif sur la liberté d'expression.
- **Liberté de religion** : Les algorithmes de reconnaissance faciale peuvent également entraver la liberté de religion des individus[127]. Cela peut se produire, par exemple, si des personnes sont contraintes de se découvrir le visage dans des espaces publics contrairement à leurs convictions religieuses, et si elles s'exposent à des amendes ou d'autres conséquences négatives en cas de refus d'obtempérer.

Reconnaissance des émotions

Objectifs et utilisation des algorithmes de reconnaissance des émotions

Les algorithmes de reconnaissance des émotions visent à déduire l'état affectif intérieur d'un individu à partir de ses traits, notamment des mouvements musculaires du visage, du ton de la voix, des mouvements corporels et autres caractéristiques biométriques. Cette technologie utilise l'apprentissage automatique pour analyser les expressions faciales et d'autres données biométriques afin d'en déduire l'état émotionnel d'une personne. Ces technologies sont déployées par le secteur privé afin, entre autres, de cibler leur publicité, d'attirer l'attention des clients et d'influencer leurs choix. Elles semblent également séduire les gouvernements et les forces de l'ordre, qui aspirent à anticiper les activités criminelles, à éliminer les menaces terroristes et à contrôler les espaces publics et, de plus en plus, les espaces privés.[128]

Tout comme d'autres technologies biométriques, la reconnaissance des émotions implique une collecte massive invisible et non responsable de données personnelles sensibles qui permet le suivi, la surveillance, la catégorisation, la notation ou le profilage d'individus, souvent en temps réel. La reconnaissance des émotions est utilisée dans divers contextes, notamment par des patrouilles aux frontières ou des agents de police pour identifier visuellement les « comportements suspects » ou les « terroristes ».[129] Les États et les entreprises privées testent et déploient ces technologies de manière conséquente, souvent en collaborant les uns avec les autres.[130]

Efficacité des algorithmes de reconnaissance des émotions

La technologie de reconnaissance des émotions repose sur deux hypothèses fondamentales selon lesquelles il est possible de jauger les émotions intérieures d'une personne à partir de ses expressions externes, et ces émotions intérieures sont à la fois discrètes et uniformément exprimées à travers le monde. Cette idée, connue sous le nom de théorie des émotions de base (Basic Emotion Theory – BET), suggérait que les humains de toutes les cultures pouvaient discerner de manière fiable les états émotionnels intérieurs à partir des expressions faciales, censées être universelles.[131] La théorie des émotions de base a été extrêmement influente, inspirant même des émissions de télévision et des films populaires.[132] Toutefois, les scientifiques ont étudié, contesté et largement rejeté la validité de ces hypothèses et discrédité la revendication d'universalité de l'expression des émotions au fil du temps.[133]

Les technologies de reconnaissance des émotions visant à identifier, surveiller, tracer et catégoriser des individus dans une variété de secteurs sont donc fondamentalement problématiques non pas parce qu'elles fonctionnent, mais plutôt parce que les parties prenantes qui construisent et utilisent ces technologies *affirment* qu'elles fonctionnent.[134] Même ainsi, des études universitaires et des applications du monde réel

continuent d'être construites sur les hypothèses de base de l'universalité de l'expression émotionnelle, bien qu'elles soient enracinées dans des études scientifiques douteuses et un historique de pseudosciences discréditées et racistes.[135]

Défis posés par les technologies de reconnaissance des émotions en matière de droits humains

De nombreuses inquiétudes sur le déploiement et l'utilisation des technologies de reconnaissance des émotions sont similaires à celles déjà mentionnées pour les technologies biométriques et la reconnaissance faciale. Ces technologies sont également développées et déployées de manière invisible, opaque et sans entraves, sans mécanismes de contrôle ni consultations publiques. De plus, nous soulignons les préoccupations suivantes :

- Les technologies de reconnaissance des émotions reposent sur des fondements pseudo-scientifiques erronés et des hypothèses scientifiques longtemps discréditées. Comme indiqué précédemment, elles sont fondées sur des hypothèses selon lesquelles les expressions seraient universelles, qu'il serait possible de lire les états émotionnels dans les expressions faciales, et que de telles déductions seraient suffisamment fiables pour servir à prendre des décisions. Ces trois hypothèses ont été discréditées pendant des décennies par les scientifiques du monde entier, mais cela ne semble pas freiner l'expérimentation et la vente de ces technologies. Bien que la reconnaissance des émotions suscite de plus en plus de préoccupations techniques pour les développeurs privés, la plupart des critiques portent sur les problèmes techniques de l'industrie de la surveillance, au détriment des implications sur les droits de l'homme pour les personnes surveillées/espionnées ou les faux positifs.[136]

Défis posés par les technologies de reconnaissance des émotions en matière de liberté d'expression

En matière de liberté d'expression, les technologies de reconnaissance des émotions présentent des défis similaires à ceux de la reconnaissance faciale. La reconnaissance des émotions rajoute une couche de complication et d'arbitraire à une tendance déjà inquiétante, compte tenu de l'absence de base juridique et de garanties et de la nature extrêmement intrusive de ces technologies.

De plus, en prétendant savoir déduire les « vrais » états intérieurs d'un individu et en prenant des décisions basées sur ces déductions, le déploiement des technologies de reconnaissance des émotions conforte de manière conséquente des hypothèses arbitraires et unilatérales sur les individus, qui passent pour des vérités fondamentales lourdes de conséquences. Cela a deux implications importantes. Premièrement, cela

ouvre la voie à d'importants effets paralysants sur le droit à la liberté d'expression – le fait non seulement d'être vu et identifié, mais aussi d'être jugé et catégorisé fonctionne comme un mécanisme d'intimidation et encourage les individus à se conformer aux « bonnes » formes d'expression de peur d'être perçus comme « suspects » ou « à risque », selon le cas utilisé. Deuxièmement, étant donné le large éventail d'applications actuelles, cela peut normaliser la surveillance de masse dans la vie quotidienne d'un individu, en particulier dans les espaces civiques. Rappelons surtout que la liberté d'expression comprend le droit de ne pas parler ou de ne pas s'exprimer.[137]

La nature même de ces technologies est également en contradiction avec la notion de préservation de la dignité humaine, et cela constitue une méthode totalement inutile pour atteindre les prétendus objectifs de protection de la sécurité nationale, de l'ordre public et autres. Alors que les normes internationales des droits humains considèrent la protection de la sécurité nationale et de l'ordre public comme des motifs légitimes de restriction des droits humains, y compris de la liberté d'expression et de la vie privée, ces situations ne donnent pas aux États carte blanche pour acquérir et utiliser arbitrairement des technologies qui ont un impact sur les droits humains, et elles ne permettent pas non plus aux États de violer des droits sans fournir des justifications étroitement adaptées et des raisons valables et spécifiques de le faire.

Les États et les entreprises font également preuve d'un manque criant de transparence dans la conception, le développement et le déploiement des technologies de reconnaissance des émotions. Si les start-ups et les entreprises technologiques bien établies sont incitées à développer des applications, les justifications fournies par les autorités pour acheter et favoriser ces produits, les informations sur les mécanismes de surveillance, les garanties pendant les projets pilotes et les considérations relatives à la protection des données sont à peine disponibles dans le domaine public, voire pas du tout. Considérant les multiples menaces que constituent les technologies de reconnaissance des émotions pour les droits humains, les États qui les utilisent et les achètent sont dans l'obligation de garantir une responsabilité, une sécurité juridique et une transparence procédurale et juridique adéquates concernant leur acquisition et leur déploiement.[138] Les entreprises sont également soumises à des obligations de transparence en vertu des Principes directeurs relatifs aux entreprises et aux droits de l'homme, qui les contraignent à mettre en place des processus pour remédier à tout impact négatif sur les droits humains résultant de leurs activités ou auquel elles contribuent.[139]

Recommandations d'ARTICLE 19

Sur la base des éléments précédents, ARTICLE 19 propose aux parties prenantes d'adopter une approche des technologies biométriques fondée sur les droits humains et de se conformer aux recommandations ci-dessous.

Il est important de souligner que tant que ces recommandations ne sont pas mises en place, **les États et les acteurs privés devraient imposer un moratoire sur le développement et le déploiement de toutes ces technologies.**

Recommandation 1 : La surveillance biométrique de masse devrait être interdite

Les États devraient interdire l'utilisation de technologies biométriques pour le traitement indiscriminé et non ciblé de données biométriques dans les espaces publics et accessibles au public, à la fois hors ligne et en ligne. Les États devraient également suspendre tout financement pour des programmes et systèmes de traitement biométrique susceptibles de contribuer à la surveillance de masse dans les espaces publics.

Recommandation 2 : La conception, le développement et l'utilisation de technologies de reconnaissance des émotions devraient être interdits

Les technologies de reconnaissance des émotions sont fondamentalement déficientes et basées sur des méthodes discriminatoires contestées par les chercheurs exerçant dans les domaines de l'informatique affective et de la psychologie. Elles ne peuvent jamais satisfaire aux critères étroitement définis de nécessité, proportionnalité et légalité, et légitimité. De ce fait, leur développement, leur vente, leur transfert et leur utilisation devraient être interdits.

Les États devraient également établir des normes internationales interdisant la création, la conception, le développement, le déploiement, la vente, l'exportation et l'importation de ces technologies en reconnaissance de leur incompatibilité fondamentale avec les droits humains.

Recommandation 3 :
La conception, le développement et l'utilisation de technologies biométriques devraient respecter les principes de légitimité, proportionnalité et nécessité

Les États ainsi que les acteurs privés devraient effectuer une évaluation adéquate au cas par cas de la légitimité de l'utilisation à certaines fins des technologies biométriques. La simple disponibilité d'une technologie ne deviendra jamais une raison suffisante pour justifier son déploiement et son utilisation. La conception, le développement et le déploiement de ces technologies devraient être limités à des fins légales conformes aux normes des droits humains et qui ne portent pas atteinte à la dignité humaine.

Pour les technologies invasives comme **la reconnaissance faciale,** le point de départ de l'évaluation est de reconnaître que cette technologie n'est jamais inoffensive en raison de son caractère intrinsèquement invasif. De ce fait, les États devraient considérer l'interdiction du déploiement de la reconnaissance faciale comme la norme, et la possibilité de l'utiliser comme une exception qui doit être justifiée et liée à un objectif spécifique.

Lorsqu'un objectif légitime justifie l'utilisation de la biométrie, son développement et son déploiement doivent répondre à un test étroitement défini de nécessité et proportionnalité : la technologie doit être absolument nécessaire pour correspondre à la portée et il ne devrait y avoir aucun autre moyen moins invasif de le faire.

Les États devraient éviter une utilisation généralisée des technologies biométriques, et en particulier de la reconnaissance faciale, dans l'espace public, car elle prive ce dernier de son rôle fondamental de catalyseur des droits des individus à s'exprimer et à participer à la vie sociale. Il est de la plus haute importance que les États résistent à la normalisation de la surveillance, qu'ils préservent le rôle de l'espace public pour la démocratie, et qu'ils garantissent ainsi le droit des individus à rester anonymes, de manifester et à s'exprimer dans un tel espace.

Les États devraient empêcher que les technologies biométriques soient utilisées pour cibler les individus ou les catégories d'individus qui jouent un rôle important dans la promotion des valeurs démocratiques, par exemple les journalistes et les activistes.

Recommandation 4 :
Les États devraient élaborer un cadre législatif adéquat pour la conception, le développement et l'utilisation des technologies biométriques

Pour les utilisations légitimes et conformes au test de nécessité et de proportionnalité, les États devraient élaborer un **cadre législatif** adéquat pour le développement et le déploiement des technologies biométriques, qui comprend, au minimum :

- Des règles sur la collecte, le stockage et la détention qui protègent de manière adéquate les données biométriques des individus et offrent des garanties suffisantes contre les atteintes à la sécurité ;
- Des exigences relatives à la qualité des données utilisées pour alimenter et entraîner les technologies ; la mise en œuvre obligatoire d'audits internes, de tests d'exactitude et de préjugés raciaux ;
- L'obligation de réaliser des analyses d'impact ex ante sur la protection des données et des analyses d'impact sur les droits humains, sous réserve d'un examen continu ;
- L'obligation, tant pour les développeurs que pour les utilisateurs, de prévenir et de minimiser les risques. Cette obligation devrait être adaptée au niveau de risque identifié ;
- Un code de pratique contraignant à l'usage des organismes de maintien de la loi ;
- Des dispositions spécifiques pour éviter le double usage ou le « dévoiement de la mission » dans l'utilisation de la technologie biométrique par des acteurs publics et privés.
- Par ailleurs, les États devraient respecter des lignes rouges dans le cadre de leur boîte à outils réglementaire en matière de biométrie.

Recommandation 5 :
La conception, le développement et l'utilisation de technologies biométriques devraient être transparents et faire l'objet d'un débat ouvert et public

Alors que les technologies biométriques ciblent de plus en plus un grand nombre de processus sociétaux critiques et de valeurs démocratiques, leur conception, leur déploiement et leur développement devraient avoir lieu après un débat public et ouvert. Il est essentiel que les coalitions de la société civile et les réseaux d'expertise puissent s'exprimer de manière appropriée dans le débat. Cela permettra d'éviter que les droits et libertés des individus succombent aux intérêts économiques de l'industrie et que les États recourent à des préoccupations de sécurité vagues et excessives pour normaliser la surveillance de masse.

Recommandation 6 :
Des exigences de transparence pour ce secteur devraient être imposées et intégralement mises en œuvre

Les États devraient divulguer publiquement toutes les activités existantes et prévues et tous les déploiements de technologies biométriques. Il faudrait également imposer une obligation spécifique de prévoir des consultations publiques sur des questions telles que les incidences de l'achat de ces technologies sur les droits humains et sur la question de savoir si les technologies en cause atteindront efficacement leurs objectifs.

Les États devraient garantir le plus haut niveau de transparence et de contrôle public sur les processus de passation des marchés publics pour l'acquisition, le développement et le déploiement de technologies biométriques. La transparence devrait inclure des critères d'évaluation des offres, les conditions des partenariats public-privé, le contenu des marchés publics, et des rapports publics réguliers sur les approbations, les acquisitions et l'utilisation.

Les États devraient garantir un droit d'accès à l'information relative à la conception, au développement et au déploiement de technologies biométriques conforme aux normes internationales. Les États devraient considérer les informations sur les technologies biométriques comme des « informations publiques » dans le cadre des lois sur le droit à l'information et publier ces informations de manière proactive et les diffuser par le biais de demandes d'accès à l'information.

Les États et les acteurs privés devraient publier régulièrement leurs analyses d'impact sur la protection des données et sur les droits humains et leurs rapports d'analyse des risques, ainsi que la description des mesures prises pour atténuer les risques et protéger les droits humains des individus. La publication ne doit pas être un exercice de cases à cocher ; cela devrait être plutôt fait d'une manière qui permette et facilite le retour d'information, le dialogue et les retours en arrière.

Recommandation 7 :
La redevabilité et l'accès à des recours devraient être garantis

Les cadres législatifs du développement et du déploiement des technologies biométriques devraient prévoir des structures de responsabilité claires et des mesures de contrôle indépendant. Les États devraient conditionner la participation du secteur privé aux technologies biométriques utilisées à des fins de surveillance – de la recherche et développement à la commercialisation, à la vente, au transfert et à la maintenance – à une diligence raisonnable en matière de droits humains et à un bilan de conformité avec les normes des droits de l'homme.

Le cadre législatif devrait également garantir l'accès à des recours efficaces pour les individus dont les droits sont violés par l'utilisation de technologies biométriques.

Recommandation 8 :
Le secteur privé devrait concevoir, développer et déployer des systèmes biométriques conformément aux normes relatives aux droits de l'homme

Les entreprises engagées dans la conception, le développement, la vente, le déploiement et la mise en œuvre de technologies biométriques devraient :

- Garantir la **protection et le respect des normes des droits humains.** Pour ce faire, elles doivent adopter une approche centrée sur les hommes et les femmes et réaliser une analyse d'impact sur les droits humains ex ante ;
- Mettre en place des procédures **d'évaluation des risques adéquates et continues** afin d'identifier les risques pour les droits et libertés des individus – et en particulier leur droit à la vie privée et à la liberté d'expression – découlant de l'utilisation de technologies biométriques, et adopter une approche de minimisation des risques.
- Fournir **des recours efficaces** en cas de violation des droits humains des individus.

Notes

1 Voir, par exemple, Conseil de l'Europe, Direction générale Droits de l'homme et État de droit, Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, janvier 2014, p. 44. Les technologies biométriques de seconde génération comprennent également la reconnaissance du visage ou de l'iris à distance, l'anthropométrie (mesure de la morphologie corporelle), ou la physiométrie (mesure des fonctions corporelles, par ex. la fréquence cardiaque, la pression artérielle, et d'autres états physiques).

2 Voir, par ex., S. Hood, Biometric Marketing: What Is Biometric Technology and How Can Marketers Use It?, Hitsearch, 15 octobre 2018.

3 C.f. par ex., Cour suprême de l'Illinois, Rosenbach v. Six Flags Entertainment Corporation, 2019 IL 123186.

4 Voir, par ex., Panel d'experts à la demande de la Commission européenne, Éthique et protection des données, 14 novembre 2018.

5 Voir, par ex., Contrôleur européen de la protection des données, Avis 4/2015, Vers une nouvelle éthique numérique : données, dignité et technologie , 11 septembre 2015.

6 Voir, par ex., Centre pour l'éthique des données et l'innovation, Interim report: Review into bias in algorithmic decision-making, juillet 2019.

7 C.f par exemple, le Haut-Commissariat aux droits de l'homme des Nations Unies, Recommandations pratiques pour la création et le maintien d'un environnement sûr et favorable à la société civile, en se fondant sur les bonnes pratiques et les enseignements tirés, A/HRC/32/20, 11 avril 2016.

8 En Chine, par exemple, l'État utilise une application pour contrôler l'accès des personnes aux espaces publics, en envoyant leurs données personnelles à la police, voir New York Times, In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, 1er mars 2020. Au Royaume-Uni, le gouvernement a projeté de rajouter des fonctions de reconnaissance faciale à l'application de traçage des contacts sponsorisée par la NHS, annonçant également que cela pourrait servir à l'émission de passeports d'immunité, voir, par ex. The Telegraph, NHS app adds face-scanning sign ups in step towards immunity certificates, 19 mai 2020. Au Liechtenstein, une partie de la population porte maintenant un bracelet électronique pour surveiller la température de la peau, le rythme de la respiration et d'autres données biométriques. Le gouvernement projette de déployer le bracelet électronique dans tout le pays d'ici à l'automne, voir par ex. L. Cendrowicz, Coronavirus Testing: Liechtenstein tracks virus with pioneering biometric bracelets, iNews.co.uk, 16 avril 2020.

9 Voir, par ex., New Statesman, Facial verification tech in NHS app could pave way for immunity passports, 20 mai 2020.

10 Actuellement, l'utilisation de ces casques de surveillance est confirmée en Chine, à Dubai et en Italie ; voir Business Insider, Police in China, Dubai, and Italy are using these surveillance helmets to scan people for COVID-19 fever as they walk past and it may be our future normal, 17 mai 2020.

11 Pour élargir le débat sur ce sujet, voir V. Marda, Papering over the crack: on privacy versus health, in Data Justice and Covid-19: Global Perspectives, 2020.

12 Voir Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des

données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, Article 3 (13); Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (RGPD), Article 4(14); Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le Règlement (CE) No 45/2001 et la Décision n° 1247/2002/CE, Article 3(18).

13 Voir le Groupe de travail Article 29 sur la protection des données, Avis 3/2012 sur l'évolution des technologies biométriques.

14 Voir D. Hambling, The Pentagon has a laser that can identify people from a distance-by their heartbeat, MIT Technology Review, 27 juin 2019.

15 Voir E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context, Springer Netherlands, 2019.

16 Voir Groupe de travail Article 29, Avis 02/2012 sur la reconnaissance faciale dans les services en ligne et mobiles, 00727/12/EN, WP 192, Bruxelles, 22 mars 2012, p. 2.

17 ARTICLE 19, Emotional Entanglement: Freedom of Expression Implications of China's Emotion Recognition Market, 2020.

18 Voir Association for Psychological Science, Corrigendum: Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, 2016; ou L. Feldman Barrett et al., Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, Psychological Science in the Public Interest. Volume 20, Issue 1, 2019.

19 Voir A. Korte, Facial recognition technology cannot read emotions, scientists say, American Association for the Advancement of Science, 16 février 2020; ou S. Porter, Secrets and Lies: Involuntary Leakage in Deceptive Facial Expressions as a Function of Emotional Intensity, Journal of Nonverbal Behavior, 36(1):23-37, mars 2012.

20 Voir A. M'charek, Tentacular Faces: Race and the Return of the Phenotype in Forensic Identification, American Anthropologist, 6 mai 2020.

21 Voir R. Wevers, Unmasking biometrics' biases: Facing gender, race, class and ability in biometric data collection, Tijdschrift voor Mediageschiedenis 21.2 (2018): 89-105, TMG Journal for Media History.

22 Pour un aperçu, voir S. Fussel, An Algorithm That 'Predicts' Criminality Based on a Face Sparks a Furor, Wired, 24 juin 2020; K. Amjad & A.A. Malik, A Technique and Architectural Design for Criminal Detection based on Lombroso Theory Using Deep Learning, LGURJCSIT Vol. 4 No 3 (2020).

23 Voir INTERPOL, Biometrics for Frontline Policing; ou The Brussels Times, The Brussels Airport to be equipped with facial recognition cameras, 9 juillet 2019.

24 Voir Aadhaar, le système d'identification de la population en Inde, le système d'identification national d'Afrique du Sud, PYMNTs; ou Deep Dive: Digital ID Developments From Around The World, 27 février 2019.

25 C.f. Metropolitan Police et NPL, Metropolitan Police Service Live Facial Recognition Trials, février 2020.

26 Voir V. Marda & S. Narayan, Data in New Delhi's predictive policing system, 2020; ou A. Daly, Algorithmic oppression with Chinese characteristics: AI against Xinjiang's Uyghurs, 2019.

27 Le déploiement croissant de la biométrie par l'État pour la prestation de services publics, et les risques de cette approche, ont été signalés par le Rapporteur spécial des Nations Unies sur l'extrême pauvreté et les droits de l'homme dans son rapport 2019 à l'Assemblée générale, voir Rapporteure spéciale des Nations Unies sur l'extrême pauvreté, les technologies numériques, la protection sociale et les droits de l'homme, A/74/493, octobre 2019.

28 Voir les systèmes d'identification biométrique de Thales dans les listes électorales ; selon leur site Internet, les pays comprennent la République démocratique du Congo, le Gabon, Oman, le Burkina Faso, le Bénin, les Philippines et la Suède.

29 C.f. Cour suprême de l'Illinois, Rosenbach v.Six Flags Entertainment Corporation, 2019 IL 123186.

30 Des remarques similaires sont faites par le Rapporteur spécial sur l'extrême pauvreté, op.cit.

31 Par son adoption dans une résolution de l'Assemblée générale des Nations Unies, la DUDH n'est pas strictement contraignante. Cependant, nombre de ses dispositions sont considérées comme ayant acquis une force juridique en tant que droit international coutumier depuis son adoption en 1948; voir *Filartiga* c. *Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).

32 Assemblée générale des Nations Unies, Pacte international relatif aux droits civils et politiques, 16 décembre 1966, Recueil des traités des Nations Unies, vol. 999, p. 171.

33 Article 10 de la Convention européenne sur les droits de l'homme (Convention européenne), 4 septembre 1950; Article 9 de la Charte africaine des droits de l'homme et des peuples (Charte de Banjul, Charte africaine), 27 juin 1981; Article 13 de la Convention américaine des droits de l'homme (Convention américaine), 22 novembre 1969 ; et Article 11 de la Charte des droits fondamentaux de l'UE (Charte UE).

34 CDH, *Belichkin* c. *Biélorussie*, Comm. n° 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

35 CDH, Observation générale n° 34, Article 19: Liberté d'opinion et d'expression, CCPR/C/GC/34, par. 18.

36 Ibid., par. 19. La même formulation apparaît dans les conventions régionales des droits de l'homme, notamment l'Article 13 de la Convention américaine, l'Article 9 de la Charte africaine, l'Article 10 de la Convention européenne, et l'Article 23 de la Déclaration des droits de l'homme de l'ASEAN.

37 Convention internationale sur l'élimination de toutes les formes de discrimination raciale, 21 décembre 1965, Recueil des traités des Nations Unies, vol. 660, p. 195.

38 Article 11 de la Convention européenne, Article 12 de la Charte de l'UE, Article 15 de la Convention américaine et Article 11 de la Charte africaine.

39 Comité DH, Observation générale n° 37, Article 21: Droit de réunion pacifique, CCPR/C/GC/37, 27 juillet 2020, par. 36.

40 Article 11 de la Convention américaine ; et Article 8 de la Convention européenne.

41 C.f. Comité DH, Observation générale n° 16 : Article 17 (Droit à la vie privée), Droit au respect de la vie privée, la famille, le domicile et la correspondance, et protection de l'honneur et la réputation, 8 avril 1988, par. 3; Principes internationaux pour le respect des droits humains dans la surveillance des communications (Principes de nécessité et de proportionnalité), Principe 1.

42 C.f. ARTICLE 19, The Global Principles on Protection of Freedom of Expression and Privacy, 2017.

43 Observation générale n° 16, op.cit., par. 10.

44 Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, Rés. 45/95 AG, 14 décembre 1990.

45 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ETS n°108.

46 En vertu de l'Article 1 de la Charte de l'UE, la dignité humaine est le fondement de tous les droits fondamentaux qui y sont garantis. Par conséquent, les données biométriques devraient être collectées et traitées de manière à protéger la dignité humaine de manière adéquate ; c.f. aussi CJEU, C-377/98, Pays-Bas c. Parlement européen et Conseil, 9 octobre 2001, par. 70-77. En outre, conformément à l'Article 52 (1) de la Charte de l'UE, toute limitation des droits fondamentaux doit : (i) être prévue par la loi. Cette obligation exige une base juridique appropriée répondant à l'exigence qualitative : la règle doit être publique, précise et prévisible ; (ii) répondre véritablement aux objectifs d'intérêt général reconnus par l'Union ou à la nécessité de protéger les droits et libertés d'autrui ; (iii) respecter l'essence du droit ; (iv) être nécessaire et proportionnelle. Le Contrôleur européen de la protection des données (CEPD) fournit des orientations strictes sur la démonstration de la nécessité et la proportionnalité. L'Agence des droits fondamentaux de l'Union européenne (FRA) considère que l'utilisation de la reconnaissance faciale peut porter atteinte à la dignité humaine en contraignant les personnes à éviter des lieux ou événements importants ; par des moyens excessivement puissants/ coercitifs de collecte de données ; et par un « comportement inapproprié de la police », voir FRA, Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le maintien de l'ordre, Vienne, 2020, p. 20.

47 Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel, 2014. ARTICLE 19 estime que les sanctions pénales et les réglementations fondées sur le contenu présentes dans la Convention ne satisfont pas aux normes de restrictions autorisées de la liberté d'expression en vertu d'autres instruments contraignants des droits humains.

48 OEA, Principes relatifs à la protection de la vie privée et des données à caractère personnel aux Amériques, 2015, actuellement en cours de révision. Les révisions comprennent notamment des références spécifiques aux données biométriques.

49 CDH, Observation générale n° 16 (Article 17 PIDCP), 8 avril 1988, par. 10, dans laquelle le Comité des droits de l'homme a noté que le droit était nécessaire pour garantir le respect du droit à la vie privée.

50 Ibid.

51 *C.f. Cour européenne, Gaskin c. Royaume-Uni*, 7 juillet 1989, Series A no. 160, par. 49; M.G. c. *Royaume-Uni*, Req. n° 39393/98, 24 septembre 2002, par. 27; *Odièvre c.* France [GC], Req. n° 42326/98, ECHR 2003III), par. 41-47; *Guerra et autres c. Italie*, Req. n° 14967/89, 19 février 1998.

52 RGPD, op.cit.

53 FRA, Opinions Biometrics, 2019.

54 Voir le Biometric Information Privacy Act de l'État de l'Illinois reconnaissant qu'une « écrasante majorité des membres du public sont las de l'utilisation de la biométrie lorsque ces informations sont liées aux finances et autres informations personnelles » ; Illinois Compiled Statutes 740 ILCS 14/1 Biometric Information Privacy Act, Sec 5 (d).

55 Rapporteur spécial sur la liberté d'expression, Rapport sur le chiffrement, l'anonymat et le cadre des droits de l'homme, A/HRC/29/32, 22 mai 2015.

56 Convention européenne, *op. cit.*, Article 14; Charte UE, *op. cit.*, Article 21; Charte africaine, *op. cit.*, Articles 2 et 3; Convention américaine, *op. cit.*, Article 24.

57 PIDCP, Article 26.

58 CDH, Résolution sur le droit à la vie privée à l'ère du numérique, UN Doc. A/HRC/RES/34/7, 23 mars 2017, par. 2.

59 Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981, ETS 108.

60 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (règlement général sur la protection des données), Article 9.

61 Réseau ibéro-américain de protection des données (RIPD), Data Protection Standards of the Ibero-American States, Articles 2.1(d) et 29.4.

62 Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, cit. Article 10.4(d).

63 Haut-Commissariat des Nations Unies aux droits de l'homme, Le droit à la vie privée à l'ère du numérique, A/HRC/39/29, 3 août 2018, par. 14.

64 Ibid., par. 61 c).

65 Rapport du Rapporteur spécial sur les droits à la liberté de réunion pacifique et à la liberté d'association, A/HRC/41/41 17 mai 2019, par. 57.

66 Biometric Update, Biometric Update, UN privacy rapporteur criticizes accuracy and proportionality of Wales police use of facial recognition, 3 juillet 2018.

67 HCDH, UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools, 25 juin 2019.

68 Cour européenne, S. et *Marper c. Royaume-Uni* [GC], App. Nos. 30562/04 et 30566/04, 4 décembre 2008, par. 112 et 125.

69 Conseil de sécurité des Nations Unies, Résolution 2396 (2017).

70 2018 Addendum to the 2015 Madrid Guiding Principles, Annexe à la lettre datée du 28 décembre 2018 du Président du Comité du Conseil de sécurité créé par la Résolution 1373 (2001) relative à la lutte contre le terrorisme adressée au Président du Conseil de sécurité.

71 UN Compendium des Nations Unies sur les pratiques recommandées pour l'usage et le partage responsables de la biométrie pour la lutte contre le terrorisme, Compilé par DECT et UNOCT, 18 juin 2018.

72 Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies (Principes de Ruggie), A/HRC/17/31, 21 mars 2011, Annexe. Le Conseil des droits de l'homme a adopté les principes directeurs dans sa Résolution 17/4, A/HRC/RES/17/14, 16 juin 2011.

73 Les Principes directeurs relatifs aux entreprises et aux droits de l'homme – mise en œuvre du cadre de référence « protéger, respecter et réparer des Nations Unies », élaborés par le Représentant spécial du Secrétaire général chargé de la question des droits de l'homme et des sociétés transnationales et autres entreprises. John Ruggie, 7 avril 2008, A/HRC/8/5A/ HRC/17/31. Le Conseil des droits de l'homme a approuvé les Principes directeurs dans sa Résolution 17/4 du 16 juin 2011.

74 Ibid., Principe 15.

75 Certaines entreprises sont allées encore plus loin et onT commencé à développer leurs propres conseils en faisant pression sur les législateurs pour les promulguer ; voir Vox, Jeff Bezos says Amazon is writing its own facial recognition laws to pitch to lawmakers, 26 septembre 2019.

76 Rapporteur spécial sur la liberté d'expression, Rapport au Conseil des droits de l'homme sur la liberté d'expression, États et secteur privé à l'ère du numérique, 2013, A/HRC/32/38, 11 mai 2016.

77 Google, Artificial Intelligence at Google: Our Principles.

78 Le Système européen de comparaison des empreintes digitales des demandeurs d'asile (EURODAC), base de données biométriques à l'échelle européenne, a pour objet de stocker les empreintes digitales de toutes les personnes qui franchissent une frontière européenne. Cependant, des inquiétudes ont été exprimées sur le fait que les informations contenues dans la base de données seraient mises à disposition des forces de l'ordre et d'Europol dans le cadre de leurs enquêtes sur le terrorisme. La réaffectation de la base de données à des fins de lutte contre le terrorisme et non d'immigration renforce les stéréotypes et stigmatise une population déjà vulnérable : les demandeurs d'asile, qui fuient déjà les persécutions, sont immédiatement associés à des actes de terrorisme, voir Statewatch and PICUM, Data protection, Immigration Enforcement and fundamental Rights: What's the EU's Regulations on Interoperability Mean for People with Irregular Status.

79 S. *et Marper c. le Royaume-Uni, op.cit.*, par. 103.

80 L'exemple de la collecte de métadonnées en masse à l'échelle de l'UE montre comment les États recueillent des informations à des fins particulières (par ex. la recherche de terroristes) mais élargissent avec le temps la portée à des crimes non violents tels que les cambriolages.

81 CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019, p. 6.

82 Ada Lovelace Institute et DataKind UK, Examining the Black Box: Tools for Assessing Algorithmic Systems, 29 avril 2020.

83 Par exemple, la société britannique Sthaler a développé un système biométrique pour l'authentification et la sécurité des clients pour usage dans les festivals de musique. Le système est actuellement déployé à d'autres fins également ; voir From Sthaler to FinGo.

84 German Data Ethics Commission, Opinion, octobre 2019.

85 Tribunal administratif de Marseille, 27 février 2020, req. n° 1901249.

86 Lorsqu'elle est accompagnée de garanties juridiques et procédurales appropriées, l'interception ciblée des communications d'un individu est un acte légitime d'un gouvernement démocratique, qui peut être nécessaire pour prévenir des crimes et des désordres et protéger la sécurité nationale. La surveillance ciblée ne peut être justifiée que si elle est prescrite par la loi, nécessaire pour atteindre un but légitime et proprotionnée au but poursuivi; voir Cour européenne, Klass et autres c. Allemagne, Req. n° 5029/71, 6 septembre 1978. La Cour européenne a utilisé le concept d'attente raisonnable en matière

de vie privée – mesure dans laquelle des personnes peuvent espérer protéger leur vie privée dans des espaces publics sans faire l'objet d'une surveillance – comme un des facteurs permettant de décider s'il y a violation du respect de la vie privée en vertu de la Convention européenne, *Copland c. Royaume-Uni*, Requête n° 62617/00, 3 juillet 2007, par. 42. Dans la même veine, le Comité européen de la protection des données (CEPD), dans ses lignes directrices sur le traitement de données personnelles par des dispositifs vidéo, stipule que les individus « peuvent également s'attendre à ne pas être surveillés dans les zones accessibles au public, en particulier si ces zones sont généralement utilisées pour des activités de récupération, de régénération et de loisirs, ainsi que dans les lieux où les personnes séjournent et/ou communiquent, tels que les salons, les tables des restaurants, les parcs, les cinémas et les salles de fitness. Dans ces cas, les intérêts ou les droits et libertés de la personne concernée prévalent souvent sur les intérêts légitimes du responsable du traitement »; Voir EDPB, Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo, Version 2.0, 29 janvier 2020.

87 Voir P. Fussey & D. Murray, Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, Human Rights Centre, juillet 2019, p. 36 et fn. 87. Voir également, the International Justice and Public Safety Network, Privacy Impact Assessment: Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field, 30 juin 2011, Document p. 016632; qui stipule que l'utilisation de la reconnaissance faciale à des fins de surveillance a le potentiel de rendre les gens extrêmement mal à l'aide, de les amener à modifier leur comportement et de conduire à l'autocensure et à l'inhibition. Voir également le Rapport du Haut-Commissariat aux droits de l'homme, Impact des nouvelles technologies sur la promotion et la protection des droits humains dans le contexte des rassemblements, y compris des manifestations pacifiques, A/HRC/44/24, p. 34.

88 C.f. Cour européenne, Szabó et Vissy c. Hongrie, Req. n° 37138/14, 12 janvier 2016, par. 38. Voir également Human Rights Watch & Pen International, With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy, juillet 2014; et CNIL, rapport 2019, *op.cit.* (la CNIL a noté que la surveillance constante et la reconnaissance faciale dans les espaces publics peuvent donner l'impression que des attitudes et des comportements apparemment normaux semblent suspects, tel que le port de lunettes de soleil, le port d'une cagoule ou le regard fixé au sol ou sur un téléphone).

89 Voir rapport FRA 2020, *op.cit.*, p. 20; ou London Policing Ethics Panel, Final Report on Live Facial Recognition, mai 2019.

90 Surveillance et droits de l'homme, *op. cit.*, p. 26.

91 Voir l'Indian Express, Delhi Police film protests, run its images through face recognition software to screen crowd, 28 décembre 2019; India Today, Amit Shah on Delhi riots probe: 1100 people identified using face recognition tech, 300 came from UP, 11 mars 2020.

92 Surveillance et droits de l'homme, op.cit., p. 15.

93 Voir le Comité sur les normes de la vie publique (Committee on Standards in Public Life, Artificial Intelligence and Public Standards, Section 4.7: analyse d'impact, février 2020. Le Comité a noté qu'une responsabilité appropriée dépend de la reconnaissance par les organes publics des risques de leurs systèmes IA, afin que les autorités puissent être évaluées par rapport aux mesures d'atténuation qu'elles prennent.

94 En décembre 2020, la Cour d'appel des États-Unis pour le neuvième circuit a accueilli favorablement les arguments du demandeur selon lesquels les demandes d'informations sollicitant l'accès à des données agrégées sont essentielles pour préserver l'intérêt du public à comprendre la manière dont le gouvernement utilise les données biométriques et autres données personnelles recueillies sans divulguer les données sous-jacentes, souvent privées ou intrusives ; voir US Court of Appeals for the Ninth Circuit, The Center for Investigative Reporting v. United States Department of Justice, n°18-17356D.C. n° 3:17-cv-06557-JSC, 3 décembre 2020. Voir également EPIC v. FBI- Next Generation Identification; et US Government Accountability Office, Face Recognition Technology Report and Recommendations, mai 2016.

95 Par exemple, au Royaume-Uni, le Bureau du Commissaire à la conservation et à l'utilisation du matériel biométrique, chargé d'assurer un contrôle indépendant du régime établi par la loi sur la protection des libertés de 2012 (Protection of Freedoms Act) et de régir la conservation et l'utilisation par la police, en Angleterre et au pays de Galles, d'échantillons d'ADN, de profils et empreintes digitales, n'est pas couvert par la loi sur la liberté d'information. Ainsi, le Bureau britannique n'a aucune obligation juridique de répondre à des demandes d'accès à l'information. Pour de plus amples informations sur le mandat et les pouvoirs du Commissaire à la biométrie, voir la page du Bureau du Commissaire à la biométrie sur le site Internet du gouvernement britannique.

96 Les demandes d'accès à l'information ont permis aux particuliers d'obtenir des informations cruciales sur la technologie de reconnaissance faciale telles que le taux d'erreur, les accords de licence entre des organismes publics et des entreprises privées, ou la diffusion de données biométriques entre agences à des fins très diverses ; voir l'expérience de l'EPIC aux États-Unis dans la contestation de l'utilisation de technologies biométriques par divers organismes publics : EPIC FOIA: DHS Biometric Program. Les demandes d'accès à l'information ont aussi révélé l'incapacité des organismes publics à mener une vérification de la confidentialité de l'utilisation de la reconnaissance faciale par l'agence ou à tester adéquatement l'exactitude de la technologie ; voir. U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI should better ensure privacy and accuracy, 2016.

97 C.f. UK Biometrics and Forensics Ethics Group Principles, décembre 2020.

98 En effet, 1:1 les systèmes de vérification suscitent des inquiétudes aussi ; voir Kak A., The State of Play and Open Questions for the Future, in Regulating Biometrics: Global Approaches and Urgent Questions, septembre 2020.

99 Voir FRA, rapport 2020, *op.cit*.

100 Voir Planet Biometrics, Met begins operational use of Live Facial Recognition (LFR), 24 janvier 2020; EDRigram, Serbia: Unlawful facial recognition video surveillance in Belgrade, 4 décembre 2019; Human Rights Watch, Facial Recognition Deal in Kyrgyzstan Poses Risks to Rights, 15 novembre 2019; ou The Times of India, From protest to chai, facial recognition is creeping up on us, 5 janvier 2020; The Ken, Watch this space: New Bill could unleash facial recognition free for all, 11 février 2020.

101 Par exemple, au Brésil, les systèmes de reconnaissance faciale sont utilisés depuis au moins 2011, et leur usage à des fins de sécurité a été largement étendu en 2019, principalement pendant le Carnaval, grâce à des partenariats avec des acteurs privés. Aujourd'hui, plus de 40 villes brésiliennes ont adopté la technologie. Voir, par exemple, Le Monde Diplomatique, Brésil, La reconnaissance faciale : la banalisation de la technologie controversée (en portugais), 22 avril 2020. Pour un aperçu de l'utilisation des technologies de reconnaissance faciale au Brésil, voir Instituto Igarape, Infografic of Facial Recognition in Brazil (en portugais).

102 Voir The Guardian, Facial recognition… coming to a supermarket near you, 4 août 2019; Big Brother Watch, Co-op Facial Recognition Supermarkets Revealed, 14 janvier 2021.

103 Voir Institut brésilien de protection des consommateurs (Instituto Brasileiro de Defensa do Consumidor, IDEC), qui veut savoir comment Hering utilise les données sur la reconnaissance faciale des clients (ien portugais), 6 mars 2019.

104 Voir IDEC, IDEC asks for clarification on facial data collection in Carefour store (en portugais), 23 avril 2019.

105 Voir IDEC, Justice prevents use of camera that collects facial data in subway in SP (en portugais), 18 septembre 2018.

106 Voir The Telegraph, Uber faces racism claim over facial recognition software, 23 avril 2019.

107 Par exemple, Huawei place la reconnaissance faciale au cœur de son projet 'Safe City', que la société tente de développer dans de nombreuses villes du monde entier, et plus particulièrement dans les régions africaines et asiatiques ; voir CSIS, Watching Huawei's "Safe Cities," 4 novembre 2019.

108 Par exemple, en 2019, San Francisco a interdit l'usage de la reconnaissance faciale par les forces de l'ordre ; voir EFF, Stop Secret Surveillance Ordinance (05/06/2019) (pour l'ordre d'interdiction) et The Guardian, San Francisco was right to ban facial recognition. Surveillance is a real danger, 30 mai 2019. Portland discute actuellement d'une interdiction englobant son utilisation par des acteurs à la fois publics et privés ; voir Fast Company, Portland plans to propose the strictest facial recognition ban in the country, 12 février, 2019. Au Royaume-Uni, la police écossaise a révélé qu'elle ne déploierait pas encore la technologie de reconnaissance faciale car elle n'était pas « apte à être utilisée » en raison, entre autres, de problèmes liés aux droits de l'homme et à la protection de la vie privée. Les plans de déploiement initialement prévus pour 2026 ont été suspendus afin de permettre la tenue d'une consultation plus large sur l'impact du logiciel ; voir BBC, Facial recognition: 'No justification' for Police Scotland to use technology, 11 février 2020.

109 Par exemple, l'entreprise IBM, dans une lettre au Congrès américain sur la réforme de la justice raciale, a annoncé qu'elle cesserait la vente de logiciels de reconnaisance faciale « à usage général »; voir IBM CEO's Letter to Congress on Racial Justice Reform, 8 juin 2020. Amazon a annoncé un moratoire d'un an sur l'usage par la police de sa technologie Rekognition, voir Amazon, We are implementing a one-year moratorium on police use of Rekognition, 10 juin 2020. Microsoft a promis de ne pas vendre aux forces de l'ordre ses technologies de reconnaissance faciale ; voir e.g. The Washington Post, Microsoft won't sell police its facial recognition technology, following similar moves from Amazon and IBM, 11 juin 2020.

110 Voir New York Times, The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?, 28 mars 2019.

111 Par exemple, à Moscou, l'administration utilise la reconnaissance faciale pour vérifier que les personnes en quarantaine pour cause de coronavirus restent bien chez elles ou à leur hôtel ; voir Reuters, Moscow deploys facial recognition technology for coronavirus quarantine, 21 février 2020. Des entreprises chinoises déploient une technologie de RF qui peut détecter les températures élevées dans une foule ou signaler les citoyens qui ne portent pas de masque facial; voir The Guardian, 'The New Normal': China's excessive coronavirus public monitoring could be here to stay, 9 mars 2020. Le Royaume-Uni considère la RF comme un instrument de la mise en place d'un système de passeport d'immunité.

112 Voir Facewatch, Facewatch launches facemask, 11 mai 2020.

113 Fait inquiétant, la Commission européenne semble approuver cette approche et a récemment décerné son « sceau d'excellence » à la technologie Aware, développée par la société espagnole Herta Security, qui fournit des analyses vidéo avancées, dont la reconnaissance faciale en temps réel et l'analyse de comportement de la foule, pour usage dans la lutte contre une autre épidémie potentielle de coronavirus. Voir Euractiv, Crowd monitoring facial recognition tech awarded seal of excellence, 19 juin 2020.

114 Début 2019, le ministre de l'Intérieur et le directeur de la police de Serbie ont annoncé l'installation de 1000 caméras dans 800 lieux à Belgrade. Le public a été informé que ces caméras de surveillance disposeront d'un logiciel de reconnaissance faciale et de plaques d'immatriculation. Trois organisations de la société civile ont publié une analyse détaillée de la DPIA du ministère de l'Intérieur sur l'utilisation de la vidéosurveillance intelligente, concluant qu'elle ne remplissait pas les conditions formelles ou matérielles requises par la loi sur la protection des données à caractère personnel en Serbie. L'autorité serbe de protection des données a confirmé les conclusions. Pour plus d'information, voir EDRigram, Serbia: Unlawful facial recognition video surveillance in Belgrade, 4 décembre 2019.

115 En février 2020, Facebook a réglé un recours collectif dans l'Illinois où des utilisateurs ont affirmé que le système de marquage de photos du site de l'entreprise utilisait la reconnaissance faciale pour analyser leurs photos et créer et stocker des « modèles de visage » sans informer les utilisateurs ni demander leur consentement à compter de juin 2011; voir New York Times Facebook to Pay $550 Million to Settle Face Recognition Suit, 29 janvier 2020. De même, l'application Clearview AI de reconnaissance faciale a été développée et largement commercialisée auprès des forces de l'ordre en s'appuyant sur une base de données de 3 milliards d'images illégalement extraites de Facebook, Google et YouTube. L'entreprise fait face actuellement à un procès intenté au nom de plusieurs citoyens de l'Illinois pour violation de la loi sur les informations biométriques de l'État. En mars 2020, le Procureur général du Vermont a lancé une action en justice contre la société, qualifiant ses pratiques commerciales « sans scrupules, contraires à l'éthique et à l'ordre public » ; voir Gizmodo, We Found Clearview AI's Shady Face Recognition App, 27 février 2020; ou Bureau du Procureur général du Vermont, Attorney General Donovan Sues Clearview AI for Violations of Consumer Protection Act and Data Broker Law, 10 mars 2020.

116 Voir OneZero, Why you can't really consent to Facebook's Facial Recognition, 30 septembre 2019 ; E. Selinger & W. Hartzog, The Inconsentability of Face Surveillance, 66 Loyola Law Review 101 (2019).

117 Voir J. Buolamwini & T. Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 2018. En outre, l'Institut national des normes et de la technologie (NIST) a récemment réalisé une étude pour évaluer la précision avec laquelle les outils logiciels de RF identifient des personnes de sexe, âge et race différents. Selon leurs conclusions, la réponse dépend de l'algorithme au cœur du système, de l'application qui l'utilise et des données qui l'alimentent. Cependant, une étude de la NIST a révélé que la majorité des algorithmes de reconnaissance faciale présentent des différentiels démographiques. Un différentiel signifie que la capacité d'un algorithme à faire correspondre deux images de la même personne varie d'un groupe démographique à l'autre. Les femmes afro-américaines constituaient le groupe démographique indiquant le plus grand nombre de faux positifs ; plus généralement, les groupes démographiques asiatiques, afro-américains et autochtones sont les plus sujets à engendrer des résultats inexacts ; voir NISTIT, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 8280.

118 Voir ACLU, Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots, 26 juillet 2018 (qui a documenté le fait que le système RF développé par Amazon a reconnu à tort que 28 membres du Congrès américain, sur 535 testés, ont commis des crimes et parmi eux un nombre disproportionnellement élevé de noirs); University of Essex, Human Rights Centre, Independent Report on the London Metropolitan Police Service's Trial of Live Recognition Technology, juillet 2019 (qui a constaté que les correspondances à 80% étaient fausses dans six essais en direct par la police métropolitaine du Royaume-Uni dans les régions londoniennes de Soho, Romford et Stratford); Stark, Face Recognition is the Plutonium of AI, 17 avril 2019 (qui a alerté sur le fait que les préjugés raciaux sont une caractéristique, et non un bug, des technologies de RF).

119 Ibid. ACLU. De plus, au moins trois cas d'hommes noirs arrêtés aux États-Unis à tort en raison d'une mauvaise reconnaissance faciale ont été signalés. Voir NBCNews, Man wrongfully arrested due to facial recognition software talks about 'humiliating' experience, 26 juin 2020; The New York Times, Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match, 29 décembre 2020; The New York Times, Wrongfully Accused by an Algorithm, 24 juin 2020.

120 C.f. Interpol, Facial Recognition.

121 Voir le Bureau du Commissaire britannique à l'information, ICO investigation into how the police use facial recognition technology in public places, 31 octobre 2019.

122 Voir ARTICLE 19, Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence, avril 2019; ARTICLE 19 et Privacy International, Privacy and freedom of expression in the age of artificial intelligence, avril 2018.

123 En 2019, la CNIL a condamné l'utilisation d'algorithmes de reconnaissance faciale pour faciliter et contrôler l'accès des enfants à l'école au motif que le même objectif pouvait être atteint par des moyens moins invasifs pour les droits fondamentaux des enfants ; voir CNIL, op.cit. Plusieurs ONG ont également dénoncé la mise en œuvre de cette technologie de reconnaissance faciale dans les écoles ; voir La Quadrature du Net, La Ligue des droits de l'homme, la CGT Educ'Action des Alpes-Maritimes et la Fédération des conseils de parents des écoles publiques dans les Alpes-Maritimes, Reconnaissance faciale dans les lycées : un recours pour bloquer la surveillance biométrique, 19 février 2019. Voir aussi Tribunal administratif de Marseille, 9e ch., arrêt du 27 février 2020. Par ailleurs, le magistrat français impliqué dans une affaire pertinente à Marseille a déclaré lors de l'audience que la région avait utilisé « un marteau-piqueur pour frapper une fourmi », une illustration parfaite du manque de proportionnalité entre la mesure mise en œuvre (le système de RF) et l'objectif à atteindre (contrôle de l'accès des élèves). Dans le même ordre d'idées, des élèves de diverses écoles aux Etats-Unis ont protesté contre l'utilisation de la reconnaissance faciale et dans certains cas, cela a mené la direction de l'école à abandonner le plan de déploiement de la technologie. Voir The Guardian, Ban this technology': students protest US universities' use of facial recognition, 3 mars 2020.

124 Toutes les sociétés civiles dans le monde ont commencé à dénoncé l'impact de la surveillance RF sur l'anonymat et son effet dissuasif sur la liberté d'expression. Par exemple, en Australie, le directeur adjoint du Conseil de Nouvelle-Galles du Sud pour les libertés civiles, dans le cadre de l'enquête parlementaires de la Nouvelle-Galles du Sud sur le déploiement de systèmes de mise en correspondance d'images faciales, a déclaré que cela entraîne une réelle menace pour l'anonymat. Mais la dimension la plus préoccupante est l'effet paralysant de ces systèmes sur les libertés de discussion politique, le droit de manifester et le droit à la dissidence. « Nous pensons que ces

implications potentielles devraient nous préoccuper tous » ; voir The Guardian, Facial image matching system risks 'chilling effect' on freedoms, rights groups say', 7 novembre 2018.

125 Voir E. Denham, Commissaire à l'information, Blog: Live facial recognition technology – police forces need to slow down and justify its use.

126 À titre d'exemple, le ministère de l'Intérieur de l'Inde, en février 2020, a arrêté 1100 personnes qui ont participé à des manifestations pacifiques, en les identifiant grâce à la reconnaissance faciale. Voir India Today, Amit Shah on Delhi riots probe: 1100 people identified using face recognition tech, 300 came from UP, cit.

127 La liberté de religion est garantie par l'Article 18 de la DUDH et mis en application par les dispositions de l'Article 18 du PIDCP, ainsi que par d'autres instruments régionaux et nationaux.

128 Ibid.

129 Voir le programme SPOT de la US Transportation Security Authority ou le système IA iBorderCtrl de l'Europe (un système IA de pré-dépistage où des caméras scannent les visages de voyageurs afin de détecter leurs mensonges quand ils répondent aux agents de sécurité aux frontières, expérimenté en Hongrie, en Lettonie et en Grèce). Les critiques à l'encontre des ensembles de données, des faux positifs et du potentiel discriminatoire du système ont conduit à son retrait. Voir Government Accountability Office, Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities, 14 novembre 2013; Department of Homeland Security Office of Inspector General, TSA's Screening of Passengers by Observation Techniques, mai 2013; ACLU vs. TSA, 8 février 2017; Ars Technica, TSA's got 94 signs to ID terrorists, but they're unproven by science, 13 novembre 2013; The Intercept, Exclusive: TSA's Secret Behavior Checklist to Spot Terrorists, 27 mars 2015; Ars Technica, The premature quest for AI-powered facial recognition to simplify screening, 2 juin 2017; J. Sánchez-Monederoa & L. Dencik, The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl'; The Intercept, We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive, 26 juillet 2019.

130 Par exemple, le système chinois de reconnaissance des émotions Alpha Hawkeye est utilisé par les autorités à la gare ferroviaire de Yiwu pour appréhender des « criminels » ; l'entreprise publique Chang'an Automobiles commercialise des voitures équipées de détecteurs d'émotion et de fatigue ; Hikvision collabore avec le Hangzhou Educational Technology Centre (en charge de l'achat de technologie pour les écoles primaires et secondaire de la ville), sous la supervision du Bureau de l'Éducation de Hangzhou.

131 Voir P. Ekman, E. Richard Sorenson & W. V. Friesen, Pan-Cultural Elements in Facial Displays of Emotion, Science, 1969, Vol. 164, Issue 3875, pp. 86 – 88; P. Ekman, Universal Facial Expressions of Emotions, California Mental Health Research Digest, 8(4), 151-158, 1973; P. Ekman, Universals and Cultural Differences in Facial Expressions of Emotions, In Cole, J. (Ed.), Nebraska Symposium on Motivation (pp. 207-282), Lincoln, University of Nebraska Press, 1973.

132 Voir A. L. Hoffman & L. Stark, Hard Feelings - Inside Out, Silicon Valley, and Why Technologizing Emotion and Memory Is a Dangerous Idea, Los Angeles Review of Books, 11 septembre 2015.

133 Voir J. A. Russel, Is there universal recognition of emotion from facial expression? A review of the cross-cultural studies, Psychological Bulletin, 115(1), 102–141, 1994; L. Feldman Barrett et al, Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, Psychological Science in the Public Interest, Vol. 20, Issue 1, 2019; Oxford Scholarship Online, Coherence between Emotions and Facial Expressions, The Science of Facial Expression, 2017; The New York Times, What Faces Can't Tell Us, 28 février 2014.

134 Voir A. Daub, The Return of the Face, Longreads, octobre 2018.

135 Voir L. Safra, C. Chevallier, J. Grezes & N. Baumard, Tracking historical changes in trustworthiness using machine learning analyses of facial cues in paintings, Nature Communications, 11, 4728, 2020; or Coalition for Critical Technology, Abolish the #TechToPrisonTimeline, Medium, 23 juin 2020.

136 Voir C. Cun, C. Zhengdong & S. Beibei, Grasp the Truth in an Instant: Application of Micro-expressions Psychology in Customs Inspection of Passengers (in Chinese), Journal of Customs and Trade, 2018(03), pp. 31, 33.

137 C.f. Observation générale n° 34, op.cit., stipulant que « toute forme de tentative de coercition visant à obtenir de quelqu'un qu'il ait ou qu'il n'ait pas une opinion est interdite. La liberté d'exprimer ses opinions comporte nécessairement la liberté de ne pas exprimer ses opinions », par. 10.

138 Rapport du Haut-Commissariat aux droits de l'homme, Impact des nouvelles technologies sur la promotion et la protection des droits humains dans le contexte des rassemblements, y compris des manifestations pacifiques, 24 juin 2020, par. 40.

139 Principes directeurs relatifs aux entreprises et aux droits de l'homme, op.cit., p. 15.

www.article19.org