

10 septembre 2025 POL 30/0290/2025

# Synthèse de plaidoyer pour la défense des droits des réfugié·e·s, des personnes en quête d'asile et des migrant·e·s à l'ère numérique

*Illustration d'Eliana Rodgers :  
A Dream Deterred [« un rêve  
avorté »].  
À un passage frontalier, la  
surveillance de masse  
évoque l'incertitude de l'avenir  
pour un migrant. Des militant·e·s  
sont à la tâche  
pour faire front à ces murs et ces  
dispositifs de surveillance.*

*Illustration de couverture du  
document d'Amnesty International  
Introduction à la défense des  
droits des réfugié·e·s et des  
migrant·e·s à l'ère numérique,  
2024 (index AI :  
POL 40/7654/2024)*



## Sommaire

Introduction.....	3
À propos de ce document.....	3
Glossaire .....	4
L'utilisation des technologies numériques dans le contexte des migrations et de l'asile.....	9
Cadre et principes directeurs.....	10
Recommandations .....	12
Recommandations aux États.....	12
Interdictions totales .....	12
Avant le déploiement.....	13
Pendant le déploiement .....	16
Recommandations aux entreprises .....	17
Recommandations aux organisations internationales (notamment les agences des Nations unies).....	18
Recommandations aux autres prestataires de services .....	21
Contact .....	22
Ressources .....	22

## Introduction

Amnesty International est un mouvement mondial réunissant plus de 10 millions de personnes qui agissent pour que les droits fondamentaux de chacun et chacune soient respectés. Notre vision est celle d'un monde dans lequel les dirigeants et dirigeantes tiennent leurs promesses, respectent le droit international et sont tenus de rendre des comptes. Essentiellement financée par ses membres et des dons individuels, Amnesty International est indépendante de tout gouvernement, de toute tendance politique, de toute puissance économique et de tout groupement religieux. Nous avons la conviction qu'agir avec solidarité et compassion aux côtés de personnes du monde entier peut rendre nos sociétés meilleures.

**#ProtectNotSurveil** est une coalition basée en Europe qui réunit des militant·e·s, des organisations ainsi que des chercheurs et chercheuses et d'autres personnes qui mènent des activités afin que les politiques migratoires et relatives au numérique protègent les personnes en déplacement des dérives dangereuses des systèmes d'IA. Notre mission consiste à remettre en question l'usage des technologies numériques à différents niveaux des politiques de l'Union européenne (UE) et à défendre la possibilité pour toutes les personnes de se déplacer, de se mettre en sécurité et de trouver des opportunités sans risquer de subir des préjudices, d'être surveillées ou d'être victimes de discriminations. Notre travail de plaidoyer a pour but de demander des comptes à l'UE, aux États membres et aux entreprises privées qui tirent profit de violations des droits humains aux frontières et à l'intérieur de l'UE. Pour cela, nous créons des liens entre des organisations et mouvements de défense des droits numériques, des droits des migrant·e·s et de la justice raciale pour contester les approches technosolutionnistes des politiques migratoires.

## À propos de ce document

Ce document est conçu comme une ressource de plaidoyer à l'attention des militant·e·s, défenseur·e·s, acteurs de la société civile, migrant·e·s et réfugié·e·s impactés par les technologies numériques et la surveillance dans des situations de migration et de demande d'asile. Il fournit des principes et un cadre des droits humains au travers desquels il est possible d'analyser l'impact des technologies existantes et émergentes sur les réfugié·e·s, les personnes en quête d'asile et les migrant·e·s, et d'étudier notamment les effets discriminatoires et intersectionnels de ces technologies. Il comporte également des recommandations de plaidoyer pouvant être extraites du document et transmises directement aux principales parties concernées qui développent et/ou déploient des technologies numériques et de surveillance, à savoir des États, des entreprises, des organisations intergouvernementales et des prestataires de services.

Amnesty International a préparé ce document avec le soutien d'AlgorithmWatch, du Border Violence Monitoring Network (BVMN), d'EuroMed Droits et de Privacy International, en s'appuyant sur les recommandations politiques et juridiques élaborées par la coalition #ProtectNotSurveil en matière de technologies s'appliquant dans le contexte de la migration, de l'asile et de la surveillance aux frontières, dont le développement et l'utilisation de l'intelligence artificielle dans ces domaines. Le document se veut évolutif et sera régulièrement mis à jour en fonction des

changements clés observés<sup>1</sup>. Les recommandations ne sont pas exhaustives. Elles servent simplement de point de départ au travail de plaidoyer national et international. En fin de document, une section « Ressources » présente une liste de publications d’Amnesty International et d’organisations partenaires, dans lesquelles ces recommandations ont été puisées.

## Glossaire

Intelligence artificielle (IA)	Toute technique ou tout système permettant aux ordinateurs d’imiter des comportements humains. Des discussions sont en cours sur ce qui constitue un système d’IA, qui est généralement défini comme « un système automatisé qui, pour des objectifs explicites ou implicites, déduit, à partir d’entrées reçues, comment générer des résultats en sortie tels que des prévisions, des contenus, des recommandations ou des décisions qui peuvent influencer sur des environnements physiques ou virtuels. Différents systèmes d’IA présentent des degrés variables d’autonomie et d’adaptabilité après déploiement <sup>2</sup> . »
Systèmes algorithmiques de prise de décision	Système algorithmique utilisé à l’appui de diverses étapes du processus décisionnel.
Prise de décision automatisée	Système algorithmique de prise de décision n’incluant aucune intervention humaine. Seul le système intervient dans le processus de décision.
Technologies (de surveillance) biométriques	Technologies (de surveillance) utilisées pour reconnaître des caractéristiques du corps humain à partir d’éléments biologiques uniques tels que les empreintes digitales, les iris et rétines des yeux, la voix, les traits du visage et la taille des mains. Cela inclut, par exemple, les technologies qui catégorisent les personnes en fonction de leurs caractéristiques biométriques, les technologies de reconnaissance faciale utilisées pour identifier des personnes et les technologies de « détection des émotions ».
Développeurs	Essentiellement des entreprises et des organisations internationales qui investissent des

<sup>1</sup> Le document sera révisé tous les 12 mois et lorsque nous recevrons des retours ad hoc nécessitant de mettre à jour les recommandations. Vous pouvez envoyer vos commentaires à l’adresse suivante : [charlotte.phillips@amnesty.org](mailto:charlotte.phillips@amnesty.org).

<sup>2</sup> Voir la présentation des Principes de l’OCDE sur l’IA, <https://oecd.ai/fr/ai-principles>

	ressources dans la conception d'outils d'IA, dans le but de proposer à d'autres parties d'utiliser ces outils ou de s'en servir elles-mêmes.
Acteurs déployant les technologies	Acteurs qui appliquent un outil d'IA pour atteindre les objectifs finaux pour lesquels il est destiné. Il peut s'agir d'acteurs publics ou privés. Une entité unique, comme une entreprise ou un organisme public, peut à la fois développer et déployer l'outil si elle dispose des ressources nécessaires en interne pour concevoir des outils d'IA.
Reconnaissance faciale	Terme général qui recouvre une série d'applications chargées d'effectuer une tâche spécifique, à savoir identifier une personne ou confirmer son identité à partir d'un visage humain. La reconnaissance faciale appartient à la catégorie plus large des technologies biométriques qui sont déployées à des fins multiples par les États et les entités commerciales.
Majorité mondiale	Terme faisant référence aux personnes racisées, appartenant notamment aux populations autochtones, aux populations d'origines asiatique, africaine ou latino-américaine, qui, réunies, représentent la majeure partie de la population mondiale. Ce terme est utilisé pour contester l'usage de termes tels que « minorités », dont le caractère marginalisant est souvent souligné, et pour faire valoir la solidarité et la capacité d'action collective des personnes subissant le racisme systémique et les injustices raciales historiques <sup>3</sup> .
Évaluation de l'impact sur les droits humains	Processus de mesure de l'impact en matière de droits humains, consistant notamment à identifier les risques encourus tout au long du cycle de vie de l'IA. Cela doit inclure une évaluation de la pertinence de recourir à une solution reposant sur l'IA dans une situation spécifique, en déterminant qui sont les groupes affectés et

<sup>3</sup> Voir R. M. Campbell-Stephens, 2020, "Global Majority: we need to talk about labels such as 'BAME'", <https://www.linkedin.com/pulse/global-majority-we-need-talk-labels-bame-campbell-stephens-mbe/> ; R. M. Campbell-Stephens, 2021, "Introduction: Global Majority Decolonising Narratives", *Educational Leadership and the Global Majority*, Palgrave Macmillan, Cham, [https://doi.org/10.1007/978-3-030-88282-2\\_1](https://doi.org/10.1007/978-3-030-88282-2_1)

	<p>quelles sont les conséquences à prévoir, et en cherchant à savoir si les populations concernées ont été consultées et quelles sont les solutions proposées pour atténuer les préjudices.</p>
Intersectionnalité	<p>Permet d'examiner comment les différentes formes de discrimination peuvent se superposer et s'influencer mutuellement, de telle sorte qu'elles créent une situation unique et complexe d'oppression pour une personne. Elle explique comment les différents types de discrimination vécus par une personne appartenant à un groupe particulier au sein de la société et subissant une oppression fondée sur le genre, l'orientation sexuelle, la race, la classe sociale, la caste, le handicap, la situation au regard de la législation sur l'immigration, la religion, l'appartenance ethnique, l'identité autochtone, l'âge ou tout autre motif, peuvent s'associer pour engendrer une forme d'oppression qui diffère d'une personne à l'autre. Le concept va donc plus loin que la simple reconnaissance de l'existence de différentes formes d'oppression et prend en compte la façon dont, ensemble, elles génèrent une forme de discrimination particulière. Par exemple, si une personne demandeuse d'asile noire ou musulmane est plus susceptible d'être détenue pour des raisons liées au statut migratoire, la discrimination et les violations des droits fondamentaux de cette personne sont dues à une combinaison de facteurs, dont sa race réelle ou supposée, son origine nationale, son statut migratoire ou sa citoyenneté.</p>
Obligation de « non-refoulement »	<p>Obligation des États au regard du droit de ne pas renvoyer ni transférer quiconque dans un territoire où il est avéré que cette personne risquerait de subir des persécutions ou d'être victime d'autres graves atteintes aux droits humains.</p>
Profilage	<p>Traitement automatisé de données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, tels que le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, le comportement, la</p>

	localisation ou les déplacements de cette personne <sup>4</sup> .
Discrimination raciale	La Convention internationale sur l'élimination de toutes les formes de discrimination raciale définit la discrimination raciale comme étant « toute distinction, exclusion, restriction ou préférence fondée sur la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, qui a pour but ou pour effet de détruire ou de compromettre la reconnaissance, la jouissance ou l'exercice, dans des conditions d'égalité, des droits de l'homme et des libertés fondamentales dans les domaines politique, économique, social et culturel ou dans tout autre domaine de la vie publique <sup>5</sup> ».
Identification biométrique à distance	Systèmes utilisés pour identifier des personnes à distance en recherchant leurs attributs biométriques dans une base de données. La technologie de reconnaissance faciale (cf. définition dans ce glossaire) est l'exemple le plus connu de ce type de dispositif, et les deux expressions sont parfois utilisées de manière interchangeable. L'identification biométrique à distance peut être réalisée en temps réel, en traitant les informations collectées de manière instantanée ou quasi instantanée (systèmes d'identification biométrique à distance en temps réel) ou <i>a posteriori</i> si l'analyse des images enregistrées est effectuée ultérieurement.
Outils d'évaluation du risque	Traitement de données partiellement ou entièrement automatisé à des fins d'évaluation statistique et/ou de modélisation prédictive en vue d'évaluer le risque de survenance d'un événement, au niveau individuel ou d'un groupe, ou en relation avec un événement ou un scénario particulier.

<sup>4</sup> Voir l'article 4.4 du 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), <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

<sup>5</sup> Article premier, Nations unies, 1965, Convention internationale sur l'élimination de toutes les formes de discrimination raciale, [en ligne] HCDH, <https://www.ohchr.org/fr/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial>

<p>Notation sociale</p>	<p>Recours à l'intelligence artificielle et à d'autres systèmes algorithmiques de prise de décision pour évaluer et catégoriser les personnes dans le but de prendre certaines décisions les concernant. Ce système d'évaluation ou de classification est généralement prédictif. Il peut, par exemple, être programmé pour déduire la probabilité qu'un-e demandeur-se d'emploi trouve du travail ou qu'un-e client-e rembourse un prêt. Le système se fonde sur un vaste éventail d'informations, telles que l'identité de la personne (dont son âge, son genre, sa race et son appartenance ethnique), ses comportements passés (parcours professionnel ou casier judiciaire, par exemple) ou sa situation socioéconomique (revenus ou niveau d'études, par exemple<sup>6</sup>).</p>
<p>Racisme systémique</p>	<p>Le Comité consultatif du Conseil des droits de l'homme des Nations unies souligne que le racisme constitue un problème systémique qui</p> <p>« repose sur un ensemble de lois, de politiques, de pratiques, de comportements, de stéréotypes et de biais interdépendants ou étroitement liés. Il se maintient grâce à un large éventail d'acteurs, parmi lesquels figurent les institutions publiques, le secteur privé et, plus largement, les structures sociales. Il entraîne non seulement une discrimination expresse, directe, <i>de jure</i> ou intentionnelle, mais aussi une discrimination, une distinction, une exclusion, une restriction ou une préférence masquée, indirecte, <i>de facto</i> ou involontaire fondée sur la race, la couleur de peau, l'ascendance ou l'origine nationale ou ethnique. Il prend souvent ses racines dans l'héritage de l'esclavage, du commerce des Africains réduits en esclavage et du colonialisme, et détermine le plus souvent les possibilités et la situation des individus au fil des générations<sup>7</sup>. »</p>

<sup>6</sup> Définition adaptée de Human Rights Watch, *Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net*, [https://www.hrw.org/sites/default/files/media\\_2021/11/202111hrw\\_eu\\_ai\\_regulation\\_qa\\_0.pdf](https://www.hrw.org/sites/default/files/media_2021/11/202111hrw_eu_ai_regulation_qa_0.pdf)

<sup>7</sup> Comité consultatif du Conseil des droits de l'homme, 8 août 2023, Éliminer le racisme systémique pour faire progresser la justice et l'égalité raciales, doc. ONU A/HRC/54/70, § 7, <https://docs.un.org/fr/A/HRC/54/70>

# L'utilisation des technologies numériques dans le contexte des migrations et de l'asile

Les technologies numériques, qui vont de la surveillance électronique, des satellites et des drones à la reconnaissance faciale, aux « détecteurs de mensonges » et à la reconnaissance de l'iris, sont devenus des outils omniprésents, à haut risque et souvent expérimentaux, utilisés pour orienter et appliquer les politiques des États et des organisations régionales en matière de migration et d'asile.

Les technologies numériques peuvent, directement et indirectement, causer et accroître de façon exponentielle diverses violations graves des droits humains. Lorsque des États défendent activement des objectifs contraires à leurs obligations en matière de droits humains envers les réfugié.e.s et les migrant.e.s, ces technologies risquent d'exacerber les atteintes aux droits humains et de causer beaucoup de souffrance. Les technologies utilisées pour mettre en œuvre les politiques en matière d'asile et de migration peuvent également poser problème en soi, car les systèmes sont exposés à des biais et des erreurs, et se fondent souvent sur la collecte d'informations, leur stockage et leur utilisation de façon excessive, qui mettent en péril le droit à la vie privée, la non-discrimination et d'autres droits fondamentaux.

Les technologies numériques renforcent des régimes discriminatoires aux frontières, selon la race, l'appartenance ethnique, l'origine nationale et le statut de citoyenneté. Le racisme et la discrimination intrinsèques sont profondément enracinés dans les systèmes de gestion de la migration et de l'asile. Ces technologies risquent de perpétuer et d'occulter les préjugés raciaux et la discrimination qui trouvent leur origine dans des pratiques historiques et coloniales d'exclusion fondée sur la race, sous couvert de neutralité et d'objectivité, notamment sur le plan religieux. Leur usage peut produire des effets disproportionnés sur les groupes racisés et créer différentes formes de discrimination, perpétuant le racisme systémique, la discrimination, l'oppression et la violence.

Ces dernières années, les règles de protection des données et de la vie privée, de transparence et d'obligation des pouvoirs publics de rendre des comptes, ainsi que d'autres obligations réglementaires tendent à ne pas s'appliquer aux technologies utilisées pour la gestion des migrations et des frontières<sup>8</sup>. Cela s'observe dans le cadre d'une tendance plus globale à l'adoption de mesures punitives en ce qui concerne la gestion des frontières et des migrations<sup>9</sup> et à l'amalgame des politiques de sécurité nationale, des politiques de maintien de l'ordre et des politiques migratoires<sup>10</sup>.

---

<sup>8</sup> Voir, par exemple, #ProtectNotSurveil, 2024, *Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move*, <https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/>

<sup>9</sup> Equinox Initiative for Racial Justice et la coalition #ProtectNotSurveil, 2025, *EU: Stop criminalising migration in the Facilitator's Package law*, <https://www.equinox-eu.com/eu-stop-criminalising-migration-in-the-facilitators-package-law/>

<sup>10</sup> Voir, par exemple, *The New York Times*, 2025, "Trump Calls for 20,000 Extra Officers to Help with Deportation Efforts", <https://www.nytimes.com/2025/05/10/us/politics/dhs-deportation-extra-officers.html>

Il est plus urgent que jamais d'appeler les États, les entreprises et les autres parties concernées à veiller à ce que le développement et l'utilisation de technologies respectent et protègent les droits fondamentaux de toutes les personnes, dont les réfugié·e·s, les personnes demandeuses d'asile et les migrant·e·s, sans discrimination. La transparence est une forme de garantie et peut constituer un premier pas important vers l'exercice des droits, la justice et l'obligation de rendre des comptes, mais elle ne peut à elle seule protéger les droits et doit être accompagnée d'autres garanties. Les technologies qui sont délibérément incompatibles avec le droit international relatif aux droits humains et qui donnent lieu à des préjudices inévitables, sans atténuation possible, doivent être interdites.

## Cadre et principes directeurs

Les États ont des devoirs et des obligations contraignantes en vertu du droit international relatif aux droits humains, qui les obligent à respecter, protéger et concrétiser les droits humains de toutes les personnes. Les organisations internationales, les entreprises et les autres acteurs non étatiques doivent aussi respecter les droits humains.

Pour adopter une approche centrée sur les droits humains dans ce domaine thématique, il peut être utile de garder à l'esprit certains cadres et principes généraux qui doivent être appliqués à toutes les technologies potentielles dans le domaine de l'asile et des migrations (et de manière plus globale). Citons notamment :



**Les technologies ne sont pas neutres.** Les incitations financières et autres, les systèmes de pouvoir et d'oppression structurels, le racisme systémique, la discrimination, les inégalités systémiques et les environnements politiques s'intègrent dans les technologies et l'utilisation de ces technologies les perpétue. Dans de nombreux cas, les technologies servent à concrétiser des politiques structurelles, dont les objectifs ou les pratiques peuvent s'avérer xénophobes ou discriminatoires.



**Il faut se méfier/adopter une approche critique du « technosolutionnisme »**, l'idée selon laquelle les technologies peuvent résoudre des problèmes politiques, économiques et sociaux complexes. Au lieu de partir du principe que le développement et le déploiement de technologies sont nécessaires ou inévitables, et d'imaginer des procédures pour en gérer les risques, il est important de s'interroger dès les débuts du processus, puis de manière régulière, sur la nécessité ou l'intérêt fondamental de technologies spécifiques et sur leurs capacités réelles à résoudre les problèmes systémiques sans aggraver ou créer involontairement d'autres problèmes.



**Toutes les technologies doivent respecter, protéger et promouvoir les droits humains (directement et indirectement)**, dont la non-discrimination, le droit à la vie privée, le droit à la vie, le droit de solliciter l'asile, le droit à la liberté et le principe de « non-

refoulement », entre autres. Cela est également valable lorsque les technologies sont exportées vers d'autres territoires.



**L'intersectionnalité est clé.** Les États et les entreprises doivent évaluer les risques directs et indirects, ainsi que les effets de la conception des technologies et de leur utilisation. L'évaluation, qui adoptera un angle intersectionnel, doit être réalisée à un stade précoce, durant la phase qui précède le déploiement, puis de manière régulière. Cela signifie que les États, les entreprises et les autres acteurs doivent examiner comment les différentes formes de discrimination peuvent se superposer et s'influencer mutuellement à tout moment, de telle sorte qu'elles créent une situation unique et complexe d'oppression pour une personne ou des groupes en lien avec les technologies.



Les mesures mises en place pour réglementer les technologies doivent être **contraignantes et applicables**. C'est fondamental, car il existe déjà de nombreux principes, codes de conduite et codes éthiques non contraignants qui, souvent, ne garantissent pas une protection adéquate.



La liberté d'information est une composante essentielle du droit à la liberté d'expression<sup>11</sup>. Les États, les entreprises et les autres acteurs doivent garantir **la transparence, l'obligation de rendre des comptes et l'accessibilité** de l'information, notamment pour la mettre à la disposition du public et la soumettre à son examen et pour que les diverses parties prenantes, dont les détenteurs et détentrices de droits concernés, puissent participer à l'élaboration des politiques. Il convient notamment d'assurer la transparence en ce qui concerne les rôles et les responsabilités des acteurs qui participent au développement, à l'achat et au déploiement des technologies. La transparence est essentielle, mais elle ne représente qu'une première étape qui ne suffit pas en soi.



Les États, les entreprises et les autres acteurs doivent garantir la **participation concrète des populations concernées** et placer leurs besoins et priorités au cœur des discussions autour des politiques. Il convient par ailleurs d'engager des ressources pour permettre la participation égalitaire de militant·e·s et organisations représentatifs, de garantir des conditions égales pour l'ensemble des parties prenantes et détenteurs·trices de droits, et de prendre davantage en compte l'expertise empirique. Il est capital de mettre en avant les voix et priorités des populations concernées et des acteurs·trices de la société civile appartenant à la majorité mondiale.

<sup>11</sup> Comité des droits de l'homme des Nations unies, 12 septembre 2011, Observation générale n° 34, Pacte international relatif aux droits civils et politiques, CCPR/C/GC/34, § 18-19, <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

# Recommandations

## Recommandations aux États

### Interdictions totales

***Les États ne doivent en aucun cas autoriser le développement, la production, la vente, l'utilisation, l'exportation et l'importation de technologies qui, par définition, violent les droits humains, causent des dommages irréparables et irréversibles, et/ou présentent des risques inacceptables.*** Dans ces cas, les États doivent promulguer des interdictions totales. Parmi les technologies que les États doivent interdire se trouvent :

- Les systèmes automatisés d'évaluation du risque, de notation et de profilage dans le contexte de la gestion des migrations, de l'asile et du contrôle aux frontières (y compris les systèmes de détection des fraudes). Utilisés pour déterminer si les personnes en situation de déplacement présentent un « risque » de commettre des activités illégales ou d'être une menace pour la sécurité, ces systèmes, qui jugent d'avance des personnes en fonction de facteurs qu'ils ne maîtrisent pas ou de déductions discriminatoires reposant sur des caractéristiques personnelles, sont par nature discriminatoires. Ils violent les droits à l'égalité et à la non-discrimination, à la vie privée et à la protection des données, ainsi que la présomption d'innocence. En outre, ils peuvent porter atteinte au droit de travailler, à la liberté (détention illégale, par exemple), au droit à un procès équitable, à la protection sociale ou à la santé. Le profilage automatisé doit être interdit étant donné le risque particulièrement élevé de discrimination dans ce contexte.
- Les technologies de traitement ou de déduction des caractéristiques personnelles sensibles ou d'éléments en tenant lieu, comme la race, l'affiliation politique, les croyances, la génétique, la santé et les données biométriques, à des fins de notation des risques présentés par des personnes<sup>12</sup>. Cela inclut l'utilisation de données relatives à la citoyenneté, aux « liens avec l'étranger » et à la nationalité. Autres exemples : l'utilisation de données relatives au code postal d'une personne pour déduire sa situation socioéconomique ou de données liées à son régime alimentaire pour parvenir à des conclusions sur sa religion ou son état de santé.
- Les technologies prédictives qui déterminent un risque de « migration irrégulière ». Ces systèmes peuvent être utilisés pour mettre en place des mesures préventives afin de juguler un mouvement, notamment dans des pays tiers faisant office de gardiens. Ils risquent de donner lieu à des politiques de contrôle aux frontières punitives et abusives reposant sur des stéréotypes et des préjugés raciaux, d'empêcher des personnes de demander l'asile, de les exposer à un risque de « refoulement » et de menacer leur droit à la vie, à la liberté et à la sécurité.
- Les outils de reconnaissance des émotions reposant sur l'IA, comme les « détecteurs de mensonges » et les analyses comportementales opérés par des IA. Les systèmes tels que

<sup>12</sup> Lighthouse Reports, 2023, *Whistleblower reveals Netherlands' use of secret and potentially illegal algorithm to score visa applicants*, Ethnic Profiling, <https://www.lighthousereports.com/investigation/ethnic-profiling/>

les « détecteurs de mensonges » reposant sur l'IA sont des technologies pseudo-scientifiques censées déduire les émotions en fonction de données biométriques. Les analyses comportementales sont quant à elles utilisées pour repérer des personnes « suspectes » en se fondant sur leur apparence ou sur d'autres caractéristiques personnelles qui ne sont pas pertinentes. Le recours à ces systèmes renforce les suspicions à l'égard des personnes racisées en quête d'asile et des migrant·e-s, et émet des suppositions discriminatoires reposant sur des stéréotypes et des préjugés raciaux et religieux, qui menacent les droits à la non-discrimination, à la vie privée, à la liberté et à un procès équitable<sup>13</sup>. Derrière ces technologies apparaissent en filigrane des notions validistes de « normalité » comportementale, cognitive ou physique visant à « traiter », « soigner » et au fond éradiquer le handicap et la neurodiversité.

- Les technologies d'identification biométrique à distance, a posteriori et en temps réel, telles que la reconnaissance faciale. Ces technologies facilitent la surveillance de masse discriminatoire dans tous les contextes, dont la gestion des migrations et des frontières. Elles peuvent être utilisées de manière dissuasive aux frontières ou dans le cadre d'un système plus vaste d'interdiction, empêchant des personnes de demander l'asile et compromettant les obligations des États en vertu du droit international, en particulier l'obligation de « non-refoulement ».
- La collecte, le traitement, la fusion et l'exploitation à grande échelle des données personnelles, dont le partage des données collectées entre les responsables de la sécurité nationale, du maintien de l'ordre, de la protection sociale et des migrations. Ces pratiques compromettent les principes établis de protection des données et le droit à la vie privée. Le partage de données personnelles avec des pays tiers via des organismes supranationaux d'application des lois, sous prétexte d'assurer la sécurité nationale, doit également être interdit si les données ne sont ni nécessaires, ni proportionnées, ou si cela risque d'engendrer des violations des droits humains.

## Avant le déploiement

Outre les interdictions évidentes des technologies incompatibles avec les droits humains, **les États doivent, avant le déploiement de tout système technologique :**

- Évaluer et démontrer la légalité, la nécessité et la proportionnalité d'une nouvelle technologie numérique, ainsi que sa valeur et son impact. Toute technologie adoptée doit être conforme
  - au cadre et aux principes internationaux de défense des droits humains, dont l'interdiction de la discrimination, et
  - aux normes de protection des données, notamment les principes de légalité, d'équité, de transparence, de limitation des finalités, de minimisation des données,

<sup>13</sup> Déclaration de la société civile, 2022, *The EU AI Act must protect people on the move*, [https://edri.org/wp-content/uploads/2022/12/Joint-Statement\\_The-EU-AI-Act-must-protect-people-on-the-move\\_December-2022.docx.pdf](https://edri.org/wp-content/uploads/2022/12/Joint-Statement_The-EU-AI-Act-must-protect-people-on-the-move_December-2022.docx.pdf)

d'exactitude, de limite de stockage, d'intégrité, de confidentialité (sécurité) et d'obligation de rendre des comptes<sup>14</sup>.

- S'abstenir de promulguer des lois qui contribuent à la discrimination numérique (et non numérique) en renforçant les systèmes existants d'oppression et de marginalisation.
- Adopter des cadres de gouvernance contraignants, applicables et respectueux des droits, qui portent sur le développement et le déploiement de technologies numériques, dans le but de protéger et de promouvoir les droits de toutes les personnes, dont les migrant·e·s, les réfugié·e·s et les personnes demandeuses d'asile. De tels cadres juridiques doivent notamment être exempts de dérogations généralisées accordées pour des motifs de sécurité nationale ou d'autres motifs similaires, car ces dérogations ne sont ni nécessaires ni proportionnées et peuvent avoir des effets discriminatoires.
- Promulguer ou modifier des lois, politiques et normes établies de sorte que le recours aux systèmes de décision automatisée dans les domaines des migrations et de l'asile et dans des domaines connexes ne perpétue pas les discriminations liées aux revenus, à la race, à l'appartenance ethnique, à la religion, à la situation au regard de la législation relative à l'immigration ou à d'autres caractéristiques, et que le déploiement du système respecte les normes internationales pertinentes en matière de droits humains.
- Imposer une obligation stricte de rendre des comptes et des obligations de transparence publique à tous les organes publics qui déploient des technologies numériques, dont les autorités chargées de la sécurité nationale, du maintien de l'ordre, des migrations et du contrôle des frontières. Parmi ces obligations figurent notamment les points suivants :
  - Établir une base de données publiquement accessible comportant des informations sur leurs technologies numériques et les collaborations avec des développeurs privés de technologies, le cas échéant, en précisant notamment comment et où les technologies seront/sont utilisées.
  - Conformément à l'obligation qui leur incombe de garantir l'égalité et de prévenir la discrimination raciale, collecter et divulguer des informations et données ventilées officielles sur les effets discriminatoires.
  - Établir un processus d'évaluation du risque en matière de droits humains et mener de manière systématique des évaluations de l'impact sur les droits humains et sur la protection des données pour identifier et atténuer les risques en matière de droits fondamentaux encourus par les personnes soumises aux technologies et politiques numériques de gouvernance aux frontières, dont les conséquences discriminatoires. Des ressources humaines et financières suffisantes doivent être allouées à la réalisation de ces évaluations, et une expertise en matière de droits humains est requise. Les évaluations doivent comporter des données ventilées sur la race, l'appartenance ethnique, le genre et d'autres motifs de discrimination, et être menées en consultation avec les parties concernées, dont les personnes affectées

<sup>14</sup> Data Protection Commission, *Principles of Data Protection*, <https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection>

par les technologies. Dans un souci de transparence, les conclusions et analyses de ces évaluations doivent être publiées et être disponibles publiquement. Un organisme public et indépendant ayant pour mandat de veiller au respect du cadre de gouvernance numérique doit contrôler les résultats et la mise en œuvre des recommandations. Les évaluations doivent aussi être menées régulièrement, bien avant la mise en application des technologies et tout au long de leur cycle de vie. Tout risque identifié en matière de droits humains doit être atténué et écarté avant d'autoriser le déploiement de la technologie. Une attention spécifique sera portée aux préjudices intersectionnels et aux conséquences discriminatoires subies par les réfugié·e·s et les migrant·e·s, les populations racisées, les personnes vivant dans la pauvreté, les personnes âgées, les personnes en situation de handicap et les autres populations marginalisées, ainsi que les enfants et les jeunes. S'il s'avère que les risques relatifs aux droits humains ne peuvent pas être atténués, l'utilisation de ces technologies doit être interrompue.

- Évaluer et prendre en considération les conséquences environnementales du développement et du déploiement des technologies, en tenant compte des éléments de plus en plus nombreux tendant à prouver que ces technologies dépendent largement des énergies fossiles et exercent des pressions considérables sur les ressources naturelles, comme la terre et l'eau, ce qui amplifie le changement climatique et les dégradations de l'environnement<sup>15</sup>.
- Adopter des lois qui rendent la diligence raisonnable obligatoire, qui imposent aux entreprises impliquées dans le développement et la fourniture de technologies utilisées dans le contexte de l'asile, des migrations et des contrôles aux frontières, dont le big data, l'IA et les systèmes biométriques, de s'acquitter de leur responsabilité d'exercer la diligence nécessaire en matière de droits humains, conformément aux normes internationales, telles que les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme et le Guide de l'OCDE sur le devoir de diligence.
- Dans la mesure du possible, explorer d'autres pistes non invasives (ou qui restreignent moins les droits) qui permettraient de répondre aux besoins ou de mener à bien les tâches sans compromettre de façon inconsidérée les droits à la vie privée, à l'égalité et à la non-discrimination, ainsi que le droit de ne pas faire l'objet d'une surveillance, et d'éviter d'autres atteintes aux droits humains.
- Assurer un soutien aux populations affectées, aux organisations de la société civile et aux expert·e·s des droits humains pour qu'ils et elles participent de manière significative au développement et au déploiement de technologies d'IA, ainsi qu'à la mise en œuvre, au suivi et à l'évaluation d'une réglementation pertinente en matière d'IA.

<sup>15</sup> Déclaration de la société civile, 2025, *Within Bounds: Limiting AI's environmental impact*, <https://greenscreen.network/en/blog/within-bounds-limiting-ai-environmental-impact/#:~:text=AI%20technologies%20must%20not%20be,to%20power%20new%20data%20centres>

- Adopter des mesures de protection des lanceurs et lanceuses d'alerte pour soutenir l'obligation de rendre des comptes des acteurs responsables du développement et du déploiement des technologies d'IA.

## **Pendant le déploiement**

### ***Durant le cycle de vie des technologies, les États doivent :***

- Donner la possibilité aux particuliers de connaître et de donner ou de revenir librement sur leur consentement, et de contester les mesures prises pour recueillir, agréger, conserver et utiliser leurs données personnelles. Ils doivent pouvoir accéder à l'information, dans une langue qu'ils comprennent, et qui explique clairement qui collecte les données, quelles données sont collectées et quelle utilisation sera faite de ces données. Les particuliers doivent pouvoir faire un véritable choix, sans aucune forme de contrainte, de manipulation ou d'intimidation. Ils doivent pouvoir retirer facilement leur consentement et faire en sorte que leurs données soient supprimées, sans craindre de représailles. Cela vaut également lorsque les données sont collectées involontairement (un drone qui aurait mécaniquement enregistré des données personnelles, par exemple).
- Obliger les acteurs du déploiement de systèmes d'IA à informer les particuliers lorsque des décisions les concernant reposent sur des technologies d'IA, dont des systèmes algorithmiques de prise de décision. Cela suppose, au minimum, de fournir des informations utiles et accessibles sur la manière dont l'IA a abouti à un résultat, la façon dont leurs données ont été traitées, la part de l'IA dans la décision finale prise par le décideur humain, ainsi que des informations sur les voies de recours et leurs droits de faire appel et de demander réparation, ainsi que les mécanismes qui existent pour exercer ces droits.
- En cas de violations, tenir les acteurs du développement et du déploiement pour responsables des atteintes aux droits humains qu'ils ont causées ou auxquelles ils ont contribué, et du non-respect de leur obligation de diligence en matière de droits humains et de protection des données, et leur demander réparation, selon les besoins de la situation.
- Veiller à ce que les personnes victimes d'atteintes aux droits humains liées à l'utilisation abusive des technologies aient accès à des recours utiles, judiciaires et non judiciaires, sans craindre de compromettre une demande d'asile en cours ou un droit déjà obtenu de séjourner sur un territoire ou d'y entrer. Les organisations d'intérêt public doivent pouvoir venir en aide aux personnes affectées pour présenter des faits et déposer des plaintes, en leur permettant notamment de bénéficier d'une assistance juridique.
- Éliminer les conséquences ou effets discriminatoires de l'utilisation des technologies numériques et prendre des mesures pour prévenir toute forme de discrimination aux termes du droit international relatif aux droits humains.

## Recommandations aux entreprises

***Les entreprises qui participent à quelque étape du cycle de vie des technologies que ce soit, y compris le développement et la fourniture de technologies utilisées dans le contexte des migrations, de l'asile et du contrôle aux frontières, doivent :***

- Respecter les droits humains partout dans le monde pour toutes leurs activités, et respecter les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme ainsi que les Principes directeurs de l'OCDE à l'intention des entreprises multinationales sur la conduite responsable des entreprises<sup>16</sup>.
- S'acquitter de leur responsabilité d'exercer la diligence nécessaire en matière de droits humains, en menant systématiquement des évaluations de l'impact sur les droits humains et sur la protection des données, conformément aux normes internationales, telles que les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme et le Guide de l'OCDE sur le devoir de diligence pour une conduite responsable des entreprises<sup>17</sup>. Les acteurs du déploiement des technologies doivent réaliser ces évaluations dès le début et régulièrement, en allouant des ressources humaines et financières suffisantes, et en apportant une expertise en matière de droits humains. Les évaluations doivent comporter des données ventilées sur la race, l'appartenance ethnique, le genre, l'âge et d'autres facteurs de discrimination, et être menées en consultation avec les parties concernées, dont les personnes affectées par les technologies. Dans un souci de transparence, les conclusions et analyses de ces évaluations doivent être publiées et être disponibles publiquement. Un organisme public et indépendant ayant pour mandat de veiller au respect du cadre de gouvernance numérique doit contrôler les résultats et la mise en œuvre des recommandations. Les évaluations doivent être menées régulièrement, tout au long de leur cycle de vie. Tout risque identifié en matière de droits humains, y compris d'éventuelles conséquences discriminatoires, doit être atténué et écarté avant d'autoriser le déploiement de la technologie ou la poursuite de son utilisation. Une attention spécifique sera portée aux préjudices intersectionnels et aux conséquences discriminatoires subies par les groupes racisés, les personnes vivant dans la pauvreté, les personnes âgées, les personnes en situation de handicap et les autres populations marginalisées, ainsi que les enfants et les jeunes. S'il s'avère que les risques relatifs aux droits humains ne peuvent pas être atténués, l'utilisation de ces technologies doit être interrompue.
- Explorer d'autres pistes non invasives qui permettraient de répondre aux besoins identifiés sans compromettre de façon inconsidérée les droits à la vie privée, à l'égalité et à la non-

---

<sup>16</sup> Haut-Commissaire des Nations unies aux droits de l'homme, 2011, 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, doc. ONU HR/PUB/11/4, [https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf) ; Organisation de coopération et de développement économiques, 2023, Principes directeurs de l'OCDE à l'intention des entreprises multinationales sur la conduite responsable des entreprises, 2023, <https://doi.org/10.1787/81f92357-en>

<sup>17</sup> Organisation de coopération et de développement économiques, 2018, OCDE, Guide sur le devoir de diligence pour une conduite responsable des entreprises, <https://doi.org/10.1787/15f5f4b3-en>

discrimination, ainsi que le droit de ne pas faire l'objet d'une surveillance, et d'éviter d'autres atteintes aux droits humains.

- Protéger les données des particuliers de toute utilisation qui aurait pour but de violer des droits, notamment en garantissant les principes de minimisation des données et de sécurité pour toutes les données personnelles collectées et tous les appareils, applications, réseaux ou services qui participent à la collecte, à la transmission, au traitement et au stockage de ces données. Donner la possibilité aux particuliers de connaître et de donner ou de revenir librement sur leur consentement, et de contester les mesures prises pour recueillir, agréger, conserver et utiliser leurs données personnelles. Ils doivent pouvoir accéder à l'information, dans une langue qu'ils comprennent, et qui explique clairement qui collecte les données, quelles données sont collectées et quelle utilisation sera faite de ces données. Les particuliers doivent pouvoir faire un véritable choix, sans aucune forme de contrainte, de manipulation ou d'intimidation. Ils doivent pouvoir retirer facilement leur consentement et faire en sorte que leurs données soient supprimées, sans craindre de représailles. Cela vaut également lorsque les données sont collectées involontairement (un drone qui aurait mécaniquement enregistré des données personnelles, par exemple).
- Éviter de provoquer des atteintes aux droits humains ou d'y contribuer par leurs propres activités, ainsi que remédier aux conséquences dans lesquelles elles sont impliquées, notamment en éradiquant les atteintes en question. La chaîne d'approvisionnement et le cycle de vie du produit ou de l'activité, y compris les exportations, doivent être pris en considération. Cela inclut également les conséquences discriminatoires involontaires qui résultent de l'utilisation de technologies numériques.
- Prévenir ou atténuer les incidences négatives sur les droits humains qui sont liées à leurs activités, produits ou services par leurs relations commerciales, même si elles n'ont pas contribué à ces incidences. Exercer une influence sur les relations commerciales pour atténuer et prévenir ces risques et ces conséquences.
- Adopter des mécanismes de transparence et d'obligation de rendre des comptes, qui divulguent des informations sur leurs technologies d'IA, notamment comment et où les technologies seront/sont utilisées.
- S'abstenir de faire pression sur les États pour obtenir des concessions ou des avantages, tels que des changements dans les lois ou les politiques susceptibles de produire des effets négatifs sur les droits humains.
- Prendre l'initiative d'engager le dialogue avec des organisations locales et de les consulter véritablement, en particulier celles qui représentent des populations marginalisées et des acteurs de la société civile, au cours du développement des technologies.

## **Recommandations aux organisations internationales (notamment les agences des Nations unies)**

- Évaluer et démontrer la légalité, la nécessité et la proportionnalité du développement ou du déploiement d'une nouvelle technologie. Toute technologie adoptée doit être conforme

- au cadre et aux principes internationaux de défense des droits humains, dont l'interdiction de la discrimination, et
  - aux normes de protection des données, notamment les principes de légalité, d'équité, de transparence, de limitation des finalités, de minimisation des données, d'exactitude, de limite de stockage, d'intégrité, de confidentialité (sécurité) et d'obligation de rendre des comptes<sup>18</sup>.
- Prendre en considération le risque que ces outils contribuent à la discrimination et à d'autres atteintes aux droits humains, en établissant un processus d'évaluation du risque en matière de droits humains et en menant de manière systématique des évaluations de l'impact sur les droits humains et sur la protection des données pour identifier et atténuer les risques en matière de droits fondamentaux encourus par les personnes soumises aux technologies et politiques numériques de gouvernance aux frontières, dont les conséquences discriminatoires.
    - Des ressources humaines et financières suffisantes doivent être allouées à la réalisation de ces évaluations, et une expertise en matière de droits humains est requise. Les évaluations doivent comporter des données ventilées sur la race, l'appartenance ethnique, le genre et d'autres motifs de discrimination, et être menées en consultation avec les parties concernées, dont les personnes affectées par les technologies.
    - Dans un souci de transparence, les conclusions et analyses de ces évaluations doivent être publiées et être disponibles publiquement.
    - Un organisme public et indépendant ayant pour mandat de veiller au respect du cadre de gouvernance numérique doit contrôler les résultats et la mise en œuvre des recommandations.
    - Les évaluations doivent aussi être menées régulièrement, bien avant la mise en application des technologies et tout au long de leur cycle de vie.
    - Tout risque identifié en matière de droits humains doit être atténué et écarté avant d'autoriser le déploiement de la technologie. S'il s'avère que les risques relatifs aux droits humains ne peuvent pas être atténués, l'utilisation de ces technologies doit être interrompue.
    - Une attention spécifique sera portée aux préjudices intersectionnels et aux conséquences discriminatoires subies par les populations et personnes racisées, les réfugié·e·s et les migrant·e·s, les personnes vivant dans la pauvreté, les personnes âgées, les personnes en situation de handicap et les autres populations marginalisées, ainsi que les enfants et les jeunes.

<sup>18</sup> Data Protection Commission, *Principles of Data Protection*, <https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection>

- Explorer d'autres pistes non invasives qui permettraient de répondre aux besoins identifiés sans compromettre de façon inconsidérée les droits à la vie privée, à l'égalité et à la non-discrimination, ainsi que le droit de ne pas faire l'objet d'une surveillance, et d'éviter d'autres atteintes aux droits humains.
- Protéger les données des particuliers de toute utilisation qui aurait pour but de violer des droits, notamment en garantissant les principes de minimisation des données et de sécurité pour toutes les données personnelles collectées et tous les appareils, applications, réseaux ou services qui participent à la collecte, à la transmission, au traitement et au stockage de ces données.
- Donner la possibilité aux particuliers de connaître et de donner ou de revenir librement sur leur consentement, et de contester les mesures prises pour recueillir, agréger, conserver et utiliser leurs données personnelles, dont les données biométriques. Ils doivent pouvoir accéder à l'information, dans une langue qu'ils comprennent, et qui explique clairement qui collecte les données, quelles données sont collectées et quelle utilisation sera faite de ces données. Les particuliers doivent pouvoir faire un véritable choix, sans aucune forme de contrainte, de manipulation ou d'intimidation. Ils doivent pouvoir retirer facilement leur consentement et faire en sorte que leurs données soient supprimées, sans craindre de représailles, notamment la privation de droits ou de services. Cela vaut également lorsque les données sont collectées involontairement.
- Informer les particuliers lorsque des décisions les concernant reposent sur des technologies d'IA, dont des systèmes algorithmiques de prise de décision. Cela suppose, au minimum, de fournir des informations utiles et accessibles sur la manière dont l'IA a abouti à un résultat, la façon dont leurs données ont été traitées, la part de l'IA dans la décision finale prise par le décideur humain, ainsi que des informations sur les voies de recours et leurs droits de faire appel et de demander réparation, et les mécanismes qui existent pour exercer ces droits.
- Veiller à ce que les personnes victimes d'atteintes aux droits humains liées à l'utilisation abusive des technologies aient accès à des recours utiles.
- Intégrer des garanties spécifiques et explicites contre l'utilisation abusive des technologies, dont le partage de données avec des organes de sécurité nationale ou des États, pouvant donner lieu à des violations.
- Faire en sorte que les populations affectées puissent participer de manière significative au développement et au déploiement de technologies d'IA, ainsi qu'à leur mise en œuvre, suivi et évaluation.
- Agir en respectant leurs responsabilités au regard des droits humains et veiller à ce que l'aide apportée, dont les programmes d'aide technique et financière, ne conduise pas à la prolifération de technologies qui conduisent à des violations des droits des migrant-e-s, des réfugié-e-s et des personnes en quête d'asile.

## Recommandations aux autres prestataires de services

***Aux prestataires de services qui déploient des technologies numériques dans les domaines de l'asile, des migrations, des contrôles aux frontières et de l'aide humanitaire, dont les organisations non gouvernementales (ONG) et les prestataires de services humanitaires à but non lucratif :***

- Respecter les droits humains partout dans le monde, y compris pour leurs activités, en respectant notamment les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, les Principes directeurs de l'OCDE à l'intention des entreprises multinationales sur la conduite responsable des entreprises<sup>19</sup> ainsi que les normes Sphère<sup>20</sup>.
- Prendre en considération le risque que les technologies numériques contribuent à la discrimination et à d'autres atteintes aux droits humains, en menant notamment des évaluations de l'impact en matière des droits humains qui portent une attention particulière aux conséquences intersectionnelles pour les populations et personnes racisées, les réfugié·e·s et les migrant·e·s, les personnes vivant dans la pauvreté, les personnes âgées, les personnes en situation de handicap et les autres populations marginalisées, ainsi que les enfants et les jeunes.
- Explorer d'autres pistes non invasives qui permettraient de répondre aux besoins identifiés sans compromettre de façon inconsidérée les droits à la vie privée, à l'égalité et à la non-discrimination, ainsi que le droit de ne pas faire l'objet d'une surveillance, et d'éviter d'autres atteintes aux droits humains.
- Protéger les données des particuliers de toute utilisation qui aurait pour but de violer des droits, notamment en garantissant les principes de minimisation des données et de sécurité pour toutes les données personnelles collectées et tous les appareils, applications, réseaux ou services qui participent à la collecte, à la transmission, au traitement et au stockage de ces données. Donner la possibilité aux particuliers de connaître et de donner ou de revenir librement sur leur consentement, et de contester les mesures prises pour recueillir, agréger, conserver et utiliser leurs données personnelles, dont les données biométriques. Ils doivent pouvoir accéder à l'information, dans une langue qu'ils comprennent, et qui explique clairement qui collecte les données, quelles données sont collectées et quelle utilisation sera faite de ces données. Les particuliers doivent pouvoir faire un véritable choix, sans aucune forme de contrainte, de manipulation ou d'intimidation. Ils doivent pouvoir retirer facilement leur consentement et faire en sorte que leurs données soient supprimées, sans craindre de représailles, notamment la privation de droits ou de services.

---

<sup>19</sup> Haut-Commissaire des Nations unies aux droits de l'homme, 2011, 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, doc. ONU HR/PUB/11/4, [https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf) ; Organisation de coopération et de développement économiques, 2023, Principes directeurs de l'OCDE à l'intention des entreprises multinationales sur la conduite responsable des entreprises, 2023, <https://doi.org/10.1787/81f92357-en>

<sup>20</sup> Sphère, *Les standards humanitaires*, <https://www.spherestandards.org/humanitarian-standards/>

- Intégrer des garanties spécifiques et explicites contre l'utilisation abusive des technologies, dont le partage de données avec des organes de sécurité nationale ou des États, pouvant donner lieu à des violations.

## Contact

Veillez adresser vos questions et commentaires, y compris concernant l'accessibilité de ce document, ainsi que toute demande de traduction aux personnes suivantes : [charlotte.phillips@amnesty.org](mailto:charlotte.phillips@amnesty.org) et [mher.hakobyan@amnesty.org](mailto:mher.hakobyan@amnesty.org).

## Ressources

- Amnesty International, *Introduction à la défense des droits des réfugié·e·s et des migrant·e·s à l'ère numérique*, février 2024 (index AI : POL 40/7654/2024), <https://www.amnesty.org/fr/documents/pol40/7654/2024/fr/>
- Amnesty International, Lettre, *The EU must respect human rights of migrants in the AI Act*, avril 2023, Bureau européen d'Amnesty International, <https://www.amnesty.eu/news/the-eu-must-respect-human-rights-of-migrants-in-the-ai-act/>
- Amnesty International, *Realising the Right to Social Security: Submission to the Office of the United Nations High Commissioner for Human Rights*, 2024 (index AI : IOR 40/7558/2024), <https://www.amnesty.org/en/documents/ior40/7558/2024/en/>
- Amnesty International, *Danemark: Coded Injustice: Surveillance and Discrimination in Denmark's automated welfare state*, 2004 (index AI : EUR 18/8709/2024), <https://www.amnesty.org/en/latest/news/2024/11/denmark-ai-powered-welfare-system-fuels-mass-surveillance-and-risks-discriminating-against-marginalized-groups-report/#:~:text=The%20Danish%20welfare%20authority%2C%20Udbetaling%20Danmark%20%28UDK%29%2C%20risks,Amnesty%20International%20said%20today%20in%20a%20new%20report>
- *Denmark: Easy-to-read version: Coded Injustice: Surveillance and Discrimination in Denmark's Automated Welfare State*, 21 mai 2025 (index AI : EUR 18/9419/2025), <https://www.amnesty.org/en/documents/eur18/9419/2025/en/>
- Amnesty International, *The Digital Border: Migration, Technology and Inequality*, 21 mai 2024 (index AI : POL 40/7772/2024), <https://www.amnesty.org/en/documents/pol40/7772/2024/en/>
- Coalition #Protect Not Surveil, dont Amnesty fait partie, voir le site Internet : EU AI | Protect Not Surveil, <https://protectnotsurveil.eu/>
- Coalition #ProtectNotSurveil, *Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move*, 13 mars 2024, <https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/>
- #ProtectNotSurveil, *Joint Statement, the EU Migration Pact: a dangerous regime of migrant surveillance*, 10 avril 2024, <https://www.accessnow.org/press-release/joint-statement-eu-migration-pact-a-dangerous-regime-of-migrant-surveillance/>

- Amnesty International, *États-Unis/Monde. La technologie de Palantir et Babel Street fait planer une menace de surveillance sur les manifestant·e·s étudiants propalestiniens et les migrant·e·s*, août 2025, <https://www.amnesty.org/fr/latest/news/2025/08/global-tech-made-by-palantir-and-babel-street-pose-surveillance-threats-to-pro-palestine-student-protestors-migrants/>