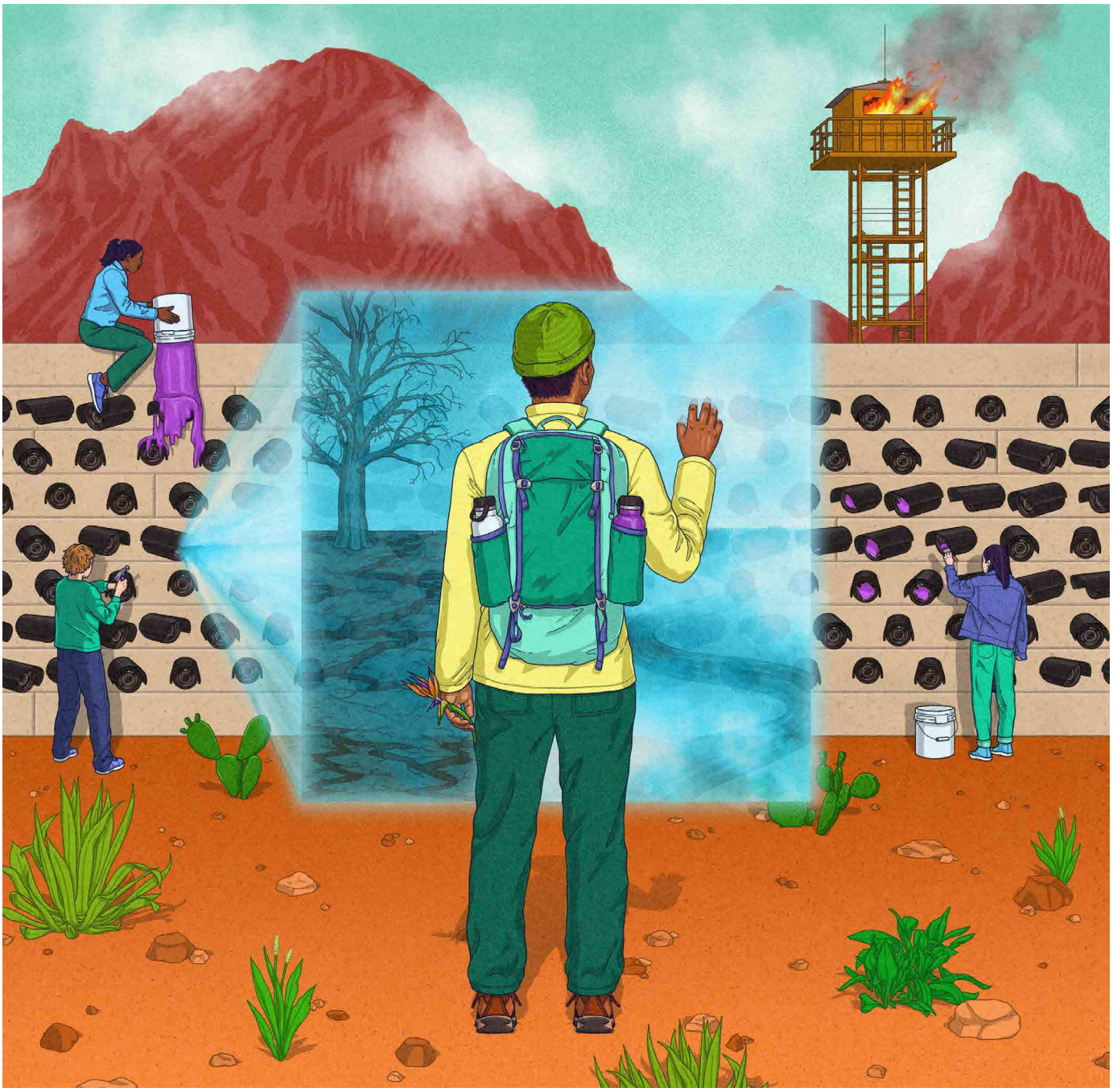

INTRODUCTION À LA DÉFENSE DES DROITS DES RÉFUGIÉ·E·S ET DES MIGRANT·E·S À L'ÈRE NUMÉRIQUE

AMNESTY INTERNATIONAL

Amnesty International est un mouvement rassemblant 10 millions de personnes qui fait appel à l'humanité en chacun et chacune de nous et milite pour que nous puissions toutes et tous jouir de nos droits humains. 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.

Édition originale publiée en 2024

par Amnesty International Ltd.
Peter Benenson House
1 Easton Street
London WC1X 0DW
Royaume-Uni

Illustration de couverture : 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.

Index : POL 40/7654/2024 French
Langue originale : anglais

amnesty.org

AMNESTY INTERNATIONAL

SOMMAIRE

Le présent exposé est une introduction au déploiement rapide et généralisé des technologies numériques dans les systèmes de gestion de l'asile et des migrations, qui engendre et entretient une discrimination systémique. Aperçu préliminaire de certaines évolutions majeures des technologies numériques dans ces systèmes de gestion de l'asile et des migrations, en particulier les dispositifs qui traitent de grandes quantités de données, il est également l'occasion pour Amnesty International de formuler certains de ses principaux questionnements découlant de leur utilisation, au sujet des droits humains. L'objectif de cet exposé introductif n'est pas de recenser l'intégralité des évolutions numériques dans ce domaine à ce jour, mais plutôt de servir de point de départ pour les personnes qui se demandent comment défendre les droits des réfugié·e·s et des migrant·e·s à l'ère numérique.

Nous remercions tout particulièrement Keren Weitzberg[1] et Roya Pakzad[2], qui, au terme de leurs recherches exploratoires, ont identifié les motifs de préoccupation liés aux droits humains décrits dans le rapport. Nous remercions également les organisations locales et les personnes qui ont pris part aux recherches et ont généreusement partagé leur savoir et leur expertise, notamment le Surveillance Resistance Lab, Derechos Digitales, Privacy International, le projet ChinaMade de l'université du Colorado, Human Rights Watch, Access Now et The Migration Technology Monitor du Refugee Law Lab, de l'université de York.

1. Les travaux de Keren Weitzberg, chercheuse dans le domaine des technologies et des migrations, se situent à l'intersection des études portant sur la science et les technologies, sur les migrations et sur les dimensions structurelles du racisme (critical race theory). Elle examine des problématiques liées à la mobilité, l'identité numérique, la biométrie et la technologie financière (fintech) en Afrique de l'Est et ailleurs.
2. Roya Pakzad est la fondatrice et la directrice de Taraaz, organisation à but non lucratif de recherche et de plaidoyer intervenant au croisement des technologies et des droits humains. Elle est aussi chercheuse affiliée du CITRIS Policy Lab de l'université de Californie à Berkeley.

1. LES TECHNOLOGIES NUMÉRIQUES DANS LES SYSTÈMES DE GESTION DE L'ASILE ET DES MIGRATIONS : POURQUOI SONT-ELLES UN MOTIF DE PRÉOCCUPATION À L'ÉGARD DES DROITS HUMAINS ?

Les technologies numériques interviennent de plus en plus dans l'orientation et l'exécution des politiques publiques relatives à l'asile et la gestion des migrations. Alors qu'Amnesty International et d'autres organisations de la société civile démontrent depuis longtemps que les gouvernements commettent de graves violations des droits humains lorsqu'ils dissuadent, entravent, repoussent et sanctionnent les personnes en déplacement, même lorsqu'elles sont réfugiées et demandeuses d'asile[3], les politiques et les pratiques de ces États s'appuient désormais sur des compétences numériques en plein essor, sous l'effet d'entreprises spécialisées du secteur privé[4]. La prolifération de technologies numériques et de solutions dites « intelligentes » de contrôle des frontières a abouti à la naissance de nouvelles formes de partenariat public-privé, s'accompagnant d'une vaste gamme de menaces pour les droits humains. Surveillance électronique, satellites, drones, reconnaissance faciale, « détecteurs de mensonges » ou lecture de l'iris sont autant de technologies qui, avec leurs conséquences, doivent de plus en plus faire l'objet de recherches urgentes pour bien les comprendre.

Les technologies numériques renforcent des régimes de contrôle des frontières qui opèrent une discrimination fondée sur l'appartenance ethnique, le pays d'origine et la nationalité. Un racisme inhérent est profondément enraciné dans les systèmes de gestion de l'asile et des migrations. Sous couvert de neutralité et d'objectivité, ces technologies risquent de perpétuer et dissimuler une discrimination et des préjugés racistes enracinés dans des pratiques coloniales historiques d'exclusion des personnes racisées[5]. En effet, leur utilisation touche de manière disproportionnée ces personnes racisées et crée différentes formes de discrimination. Des protections beaucoup plus solides contre ces technologies sont nécessaires,

3. Pour toutes les publications d'Amnesty International consacrées aux personnes réfugiées et demandeuses d'asile, veuillez consulter amnesty.org/fr, en particulier : https://www.amnesty.org/en/search/refugees/?language=fr
4. E. Tendayi Achiume, rapporteuse spéciale des Nations unies sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Rapport :*La discrimination raciale et la xénophobie et l'utilisation des technologies numériques dans le contrôle des frontières et de l'immigration,* doc. ONU A/HRC/48/76, 17 décembre 2021, https://documents.un.org/doc/undoc/gen/g21/379/62/pdf/g2137962.pdf?token=cGW4qNatJcjSUjkmfx&fe=true, § 47, ; Amnesty International, Mandatory Use of CBP One Application Violates the Right to Seek Asylum, 7 mai 2023 (index : AMR 51/6754/2023), https://www.amnesty.org/fr/documents/amr51/6754/2023/en/ ; Amnesty International, « Les technologies automatisées et l'avenir de la forteresse Europe », 28 mars 2019, https://www.amnesty.org/fr/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/
5. E. Tendayi Achiume, rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Rapport : *La discrimination raciale et la xénophobie et l'utilisation des technologies numériques dans le contrôle des frontières et de l'immigration* (op. cit.) ; Rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Rapport : *Formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée*, doc. ONU A/75/590, 10 novembre 2020, https://digitallibrary.un.org/record/3893019?ln=fr&v=pdf

car les risques pour les droits humains des personnes migrantes, réfugiées et demandeuses d'asile ne cessent de s'aggraver et continuent de perpétuer l'exclusion et la discrimination des personnes racisées.

Amnesty International reconnaît que les technologies numériques pourraient favoriser le respect, la protection et la promotion des droits des personnes réfugiées et migrantes dans certaines situations, par exemple en assurant l'accès des personnes en déplacement aux services essentiels et à des informations fiables[6]. Cependant, elles comportent encore des risques, notamment à l'égard des droits au respect de la vie privée et à la non-discrimination. Les personnes en mouvement sont de plus en plus perçues comme des « menaces pour la sécurité » et des mesures de défense de la « sécurité nationale » sont sans cesse mises en œuvre pour exclure des personnes au motif, entre autres, de leur appartenance ethnique ou de leur religion supposées. Par exemple, des mesures disproportionnées et illégales de surveillance, notamment, sont de plus en plus employées à des fins de profilage ethnique et dans des opérations de maintien de l'ordre préjudiciables aux personnes racisées. Donnant lieu à des violations des droits humains qu'elles entretiennent dans le temps, elles sont aussi adoptées de plus en plus souvent à l'encontre des personnes demandeuses d'asile, réfugiées et migrantes en général. Ces mesures et ces recours aux technologies numériques dessinent une tendance dangereuse à l'érosion de protections vitales pour les populations en mouvement. Le cumul entre intérêts d'entreprises, manque général de respect des droits des personnes en mouvement et racisme et discrimination systémiques peut permettre aux nouvelles technologies d'avancer plus vite que les garanties et le contrôle nécessaires pour obliger à rendre des comptes un secteur des nouvelles technologies en constante progression.

6. Mark Latonero et Paula Kift, "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control", 20 mars 2018, https://journals.sagepub.com/doi/full/10.1177/2056305118764432

2. GLOSSAIRE ALPHABÉTIQUE DES PRINCIPAUX TERMES

ALGORITHMES

Un algorithme est une liste de règles mathématiques permettant de résoudre un problème. Ces règles doivent suivre un ordre déterminé (comme dans une recette). Les algorithmes sont les éléments constitutifs de l'intelligence artificielle et de l'apprentissage automatique. Ils permettent aux technologies de l'intelligence artificielle et de l'apprentissage automatique de s'entraîner à partir des données déjà disponibles pour résoudre un problème, afin de résoudre d'autres problèmes alimentés par de nouvelles données.

COMPLEXE INDUSTRIEL FRONTALIER

Parfois également désigné comme l'industrie de la surveillance des frontières ou le complexe industriel du contrôle de l'immigration, ce concept désigne les relations étroites entre des gouvernements et le secteur privé, notamment les entreprises des technologies numériques, dans les systèmes de gestion de l'asile et des migrations[7].

DISCRIMINATION INTERSECTIONNELLE

Lorsque différents facteurs de discrimination interviennent simultanément, induisant des préjudices conjugués ou spécifiques. Par exemple, si un demandeur d'asile noir ou musulman est plus susceptible d'être maintenu en détention pour des motifs liés à la migration, la discrimination et l'atteinte aux droits humains qu'il subit sont dues à une combinaison de facteurs réels ou perçus incluant son appartenance ethnique, son pays d'origine, son statut au regard de la législation sur l'immigration ou sa nationalité.

DISCRIMINATION RACIALE

Dans la Convention internationale sur l'élimination de toutes les formes de discrimination raciale, la discrimination raciale est définie comme suit :

> **« 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[8] ».**

DONNÉES BIOMÉTRIQUES

Données s'appuyant sur les caractéristiques physiques ou biologiques des personnes, par exemple, empreintes digitales, empreinte de l'iris, imagerie faciale et autres spécificités uniques de chaque personne. Souvent, ces données sont recueillies et stockées à des fins d'identification d'une personne ou d'authentification de son identité[9].

---

7. Todd Miller, "Why climate action needs to target the border industrial complex", 1er novembre 2019, Al Jazeera, https://www.aljazeera.com/opinions/2019/11/1/why-climate-action-needs-to-target-the-border-industrial-complex ; Tanya Golash-Boza, "The immigration industrial complex: why we enforce immigration policies destined to fail", Sociology Compass, vol. 3, no 2, 18 mars 2009, p. 295–309.
8. Convention internationale sur l'élimination de toutes les formes de discrimination raciale, https://www.ohchr.org/fr/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial, article 1.
9. The Engine Room, *Primer: Biometrics in the Humanitarian Sector*, juillet 2023, https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Primer-2023.pdf

EXTERNALISATION

Éventail de politiques de gestion des migrations consistant à transférer à d'autres pays la responsabilité d'accorder une protection internationale aux personnes réfugiées et demandeuses d'asile, ou à faire appel aux pays d'origine ou de transit pour qu'ils durcissent le contrôle de leurs frontières. Les politiques d'externalisation ont pour objectif de prévenir ou de sanctionner le franchissement illégal des frontières par les réfugié·e·s, les demandeurs/euses d'asile et les migrant·e·s, souvent en mobilisant ou en exploitant l'aide financière internationale.

FRONTIÈRES « INTELLIGENTES »

Utilisation de systèmes technologiques, par exemple, identification et enregistrement biométriques, détection automatique des mouvements humains et reconnaissance automatique des objets, systèmes automatisés d'entrée et de sortie à la frontière, utilisation d'applications pour gérer les demandes d'asile, afin de renforcer les frontières.

INTELLIGENCE ARTIFICIELLE

Il n'existe aucun consensus général sur la définition de l'intelligence artificielle, car le terme ne fait pas référence à une technologie en particulier mais désigne une myriade d'applications et de méthodes technologiques. Les définitions les plus conventionnelles font référence à un éventail de processus guidés par les données, qui permettent aux ordinateurs d'exécuter des tâches très spécifiques ou plus générales, comme la prise de décisions ou la résolution de problèmes, au lieu des humains ou pour les aider.

Amnesty International adopte volontairement une définition générale de l'intelligence artificielle, afin d'examiner de manière exhaustive et suffisante les conséquences sur les droits humains de toute la gamme de composantes, pratiques et processus qui entrent en jeu dans les systèmes d'intelligence artificielle.

De manière générale, l'intelligence artificielle est toute technique ou tout système qui permet à des ordinateurs d'imiter le comportement humain.

INTEROPÉRABILITÉ

Capacité d'un système ou d'une base de données à échanger ou trouver des informations au sein d'un autre système ou d'une autre base de données, sans discontinuité.

« NON-REFOULEMENT »

Obligation juridique faite aux États de ne pas renvoyer ou transférer quiconque dans un lieu ou un pays où cette personne risquerait de subir des persécutions ou d'être victime d'autres graves atteintes aux droits humains ou de violations de ceux-ci.

RACISME SYSTÉMIQUE

Le Comité consultatif du Conseil des droits de l'homme a souligné que le racisme est un problème systémique répondant aux caractéristiques suivantes :

> **« [il] 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, de jure ou intentionnelle, mais aussi une discrimination, une distinction, une exclusion, une restriction ou une préférence masquée, indirecte, de facto 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[10.] »**

10. Comité consultatif du Conseil des droits de l'homme, Éliminer le racisme systémique pour faire progresser la justice et l'égalité raciales, doc. ONU A/HRC/54/70, 8 août 2023, https://documents.un.org/doc/undoc/gen/g23/140/56/pdf/g2314056.pdf?token=80vnF4zMXPlWKzx3df&fe=true, § 7.

RECONNAISSANCE FACIALE

Technique de vision par ordinateur – à savoir, méthode d'identification visuelle des objets, des personnes et du terrain dans les systèmes informatiques – employée pour identifier les visages humains. Elle consiste à utiliser comme référence l'image d'un visage (par exemple, une photo provenant d'un enregistrement de vidéosurveillance) avec un algorithme entraîné au préalable à analyser, identifier et comparer des images lui étant transmises à partir d'autres bases de données (par exemple, fichier des permis de conduire, profils de réseaux sociaux, etc.).

La reconnaissance faciale à des fins d'identification (reconnaissance faciale de un-à-plusieurs ou « 1:n ») est par nature une technique de surveillance de masse et constitue, à ce titre, une violation du droit au respect de la vie privée.

La reconnaissance faciale à des fins d'authentification (reconnaissance faciale de un-à-un ou « 1:1 ») fait appel à un processus différent, par lequel deux images sont comparées directement, et implique généralement la participation de la personne en question, par exemple, lorsque l'image d'une personne est comparée directement à la photo de son passeport ou lorsque quelqu'un utilise son visage pour débloquer un téléphone.

SOLUTIONNISME TECHNOLOGIQUE

Idée selon laquelle les problèmes complexes d'ordre social, économique et politique peuvent être résolus par la technologie.

TECHNOLOGIE GPS

Système de navigation (de l'anglais global positioning system, « système de repérage universel ») employé pour définir l'emplacement de personnes, d'objets et de lieux sur toute la planète, à l'aide de leur latitude et leur longitude.

3. LES RÉPERCUSSIONS DES TECHNOLOGIES NUMÉRIQUES SUR LES DROITS DES MIGRANT·E·S ET DES RÉFUGIÉ·E·S

3.1 « MESURES DE SUBSTITUTION À LA DÉTENTION » FAISANT APPEL AUX NOUVELLES TECHNOLOGIES

Souvent, la détention pour des raisons liées à la migration (ci-après « détention de migrants ») est abusive et discriminatoire, tant parce que, généralement, elle est arbitraire et vise des personnes racisées, que parce que les États et les entités privées commettent fréquemment des atteintes aux droits humains pendant cette détention[11]. La détention de migrants comporte le risque d'avoir des conséquences disparates en fonction de facteurs racistes, car elle vise les personnes selon leur appartenance ethnique ou leur religion perçues[12]. Par ailleurs, la détention constitue en soi une grave restriction des droits humains et une sérieuse infraction au droit à la liberté en particulier, car celui-ci ne peut être restreint que dans des circonstances précises et absolument exceptionnelles. Aux termes du droit international, par défaut, toute personne doit pouvoir jouir de sa liberté individuelle. Les personnes migrantes, réfugiées ou demandeuses d'asile doivent, comme toute autre personne, bénéficier d'une présomption de liberté sur le plan juridique. En conséquence, toute privation de leur liberté doit être clairement inscrite dans la loi, être strictement justifiée par des fins légitimes, et être nécessaire, proportionnée et non discriminatoire.

Plusieurs États ont adopté des programmes de substitution à la détention (en anglais : alternatives to detention, ATD), prétendument pour réduire le recours à la détention de migrants, en adoptant des mesures telles que la liberté sous caution, l'assignation à résidence, le couvre-feu à domicile, la liberté surveillée par la communauté ou la gestion des cas[13]. Certains gouvernements ont également adopté des programmes de mesures non privatives de liberté reposant sur des produits électroniques de substitution à la détention faisant

11. Amnesty International, Forced Out or Locked Up: *Refugees and Migrants Abused and Abandoned*, 27 juin 2022 (index : EUR 53/5735/2022), https://www.amnesty.org/en/documents/eur53/5735/2022/en ; Amnesty International, *Lettonie. « Rentrez chez vous ou restez dans la forêt pour toujours » : Réfugié·es et migrant·es détenus arbitrairement, frappés et contraints à un retour « volontaire »*, 12 octobre 2022 (index : EUR 52/5913/2022), https://www.amnesty.org/en/documents/eur52/5913/2022/en (en anglais ; seuls le résumé et l'ajout ont été traduits en français) ; Amnesty International, *« Personne ne te cherchera » : la détention abusive des personnes réfugiées et migrantes débarquées en Libye*, 15 juillet 2021 (index : MDE 19/4439/2021), https://www.amnesty.org/fr/documents/mde19/4439/2021/fr/ Amnesty International, *Canada. « Je ne me sentais pas comme un être humain » : la détention des personnes migrantes au Canada et son impact en matière de santé mentale*, 17 juin 2021 (index : AMR 20/4195/2021), https://www.amnesty.org/fr/documents/amr20/4195/2021/fr/
12. Amnesty International, « Les États doivent mettre fin au traitement raciste réservé aux Haïtien·ne·s en quête d'asile », 20 juin 2023, https://www.amnesty.org/fr/latest/news/2023/06/americas-states-must-end-racist-treatment-of-haitian-asylum-seekers/ ; Amnesty International, *Arrêtez le racisme, pas les gens. Profilage ethnique et contrôle de l'immigration en Espagne*, 14 décembre 2011 (index : EUR 41/011/2011), https://www.amnesty.org/en/documents/eur41/011/2011/en ; Amnesty International, *« Entre la vie et la mort ». Les personnes refugiees et migrantes prises dans la tourmente des violences en Libye*, 24 septembre 2020 (index : MDE 19/3084/2020), https://www.amnesty.org/fr/documents/mde19/3084/2020/fr/
13. Le droit international relatif aux droits humains limite le recours aux mesures privatives de liberté et non privatives de liberté, à savoir la détention et les mesures sans incarcération – également appelées « mesures de substitution à la détention » –, à des fins de contrôle de l'immigration. Comme la détention, ces mesures de substitution doivent répondre aux principes de légalité, de nécessité, de proportionnalité et de non-discrimination.

appel aux nouvelles technologies (les « e-ATD »), notamment des bracelets de surveillance électronique ou des applications de reconnaissance vocale ou faciale. En 2004, par exemple, le Département de la sécurité intérieure des États-Unis a inauguré deux programmes, le programme de surveillance intensive (Intensive Supervision Appearance Program - ISAP) et le programme de dispositif de surveillance électronique (Electronic Monitoring Device Program), pour appliquer des mesures non privatives de liberté aux personnes migrantes et demandeuses d'asile. D'après le Service américain de contrôle de l'immigration et des douanes (ICE), l'intention derrière ces programmes était « d'élargir les options possibles pour la libération des personnes étrangères adultes, en aidant les fonctionnaires à surveiller étroitement les personnes étrangères libérées dans la population[14] ». L'ISAP s'est appliqué à plus de 350 000 personnes, mais recule désormais[15].

Alors que ces produits prolifèrent, des universitaires et des défenseur·e·s des droits humains ont établi un lien entre ces programmes et des atteintes aux droits humains, potentielles ou réelles[16]. Un motif de préoccupation important est le manque de transparence ou de contrôle au sujet des mesures de sécurité ou de confidentialité adoptées par les entreprises lors de la conception et du développement de leurs outils e-ATD. Le problème n'est pas seulement l'insuffisance éventuelle des mesures de cybersécurité ou les fuites possibles de données. Le respect de la vie privée des personnes migrantes et demandeuses d'asile – ainsi que des membres de leur famille, dans certains cas – risque aussi d'être enfreint, du fait de la surveillance constante de leurs mouvements, susceptible d'être injustifiée ou disproportionnée. Par ailleurs, des pratiques opaques de partage de données entre entreprises privées, partenaires tiers et organismes publics (notamment les organismes responsables de l'application des lois et les bureaux de contrôle des frontières) sont aussi une source d'inquiétude. Par exemple, des partenariats commerciaux entre l'ICE et des entreprises technologiques telles que Palantir ont été directement mis en cause pour expliquer la capacité de l'organisme public à détecter, identifier et arrêter les travailleurs et travailleuses migrants en situation irrégulière, à l'aide de pratiques de surveillance générale des données. En 2019, l'ICE a arrêté près de 700 travailleuses et travailleurs dans le Mississipi, lors d'une descente dans une usine de transformation de viande de poulet. Selon de multiples médias, l'utilisation de l'outil Falcon – qui permet d'établir des prévisions et de cartographier les relations –, fourni par l'entreprise Palantir, est à l'origine de l'opération[17].

Dans une réponse à Amnesty International, Palantir a nié toute infraction à la législation, déclarant « ne pas posséder ou contrôler de données mais permettre à ses clients d'analyser leurs propres données[18] ».

Qui plus est, les e-ATD – tant les bracelets de surveillance électronique que les dispositifs de reconnaissance vocale à des fins de surveillance – sont susceptibles de produire de faux positifs et de rencontrer des problèmes techniques pouvant pénaliser arbitrairement les personnes migrantes, notamment en raison de leur manière de parler ou de leur accent, qui caractérisent les personnes racisées de manière disproportionnée[19].

En 2016, le Royaume-Uni a introduit l'obligation de porter un émetteur électronique à la cheville pour toutes les personnes étrangères sous le coup d'une expulsion[20]. En août 2021, cette mesure a été élargie aux personnes en liberté sous caution pour des motifs liés à l'immigration. Fin septembre 2022, près de 15 000 personnes étaient sous surveillance électronique au Royaume-Uni. Ce nombre atteste de la progression d'un système qui met en danger les droits humains, notamment le droit à la dignité et au respect, le droit au respect de la vie privée et le droit de disposer de son corps. En mai 2022, des projets de déploiement de formes plus avancées de ces pratiques de surveillance déjà intrusives ont été lancés. Une

14. Wesley J. Lee, directeur par intérim des Opérations d'incarcération et d'expulsion, Service de contrôle de l'immigration et des douanes des États-Unis, Mémorandum à l'usage des directeurs et directrices des bureaux locaux, "Eligibility Criteria for Enrollment into the Intensive Supervision Appearance Program (ISAP) and the Electronic Monitoring Device (EMD) Program", 11 mai 2005, https://www.scribd.com/document/24704584/ICE-Guidance-Memo-Eligibility-Criteria-for-Enrollment-Into-the-Intensive-Supervision-Appearance-Program-ISAP-and-the-Electronic-Monitoring-Device
15. TRAC, Université de Syracuse, "Detained Immigrant Population Grows to Nearly 40,000, the Highest Point in Nearly Four Years", 16 novembre 2023, https://trac.syr.edu/whatsnew/email.231116.html
16. Johana Bhuiyan, "Migrant advocates sue US government for data from surveillance program", The Guardian, 14 avril 2022, https://www.theguardian.com/us-news/2022/apr/14/immigration-advocates-alternative-to-detention-lawsuit-ice
17. Amnesty International, *USA: Failing to do right: The urgent need for Palantir to respect human rights*, 28 septembre 2020 (index : AMR 51/3124/2020), https://www.amnesty.org/en/documents/amr51/3124/2020/en ; Mijente, "BREAKING: Palantir's technology used in Mississippi raids where 680 were arrested", 4 octobre 2019, https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Palantirs_technology_used_in_Mississippi_raids_where_680_were_arrested.pdf
18. La lettre de Palantir est disponible dans son intégralité à l'annexe du rapport suivant : Amnesty International, *USA: Failing to do right: The urgent need for Palantir to respect human rights*, 28 septembre 2020 (index : AMR 51/3124/2020), https://www.amnesty.org/en/documents/amr51/3124/2020/en
19. Jack Karsten et Darrell M. West, "Decades later, electronic monitoring of offenders is still prone to failure," Brookings Institute (blog du Techtank), 21 septembre 2017, https://www.brookings.edu/articles/decades-later-electronic-monitoring-of-offenders-is-still-prone-to-failure ; Bajorek, Joan Palmiter, "Voice Recognition Still Has Significant Race and Gender Biases", Harvard Business Review, 10 mai 2019, https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases
20. Ministère de la Justice du Royaume-Uni, Electronic Monitoring Statistics Publication, England and Wales: September 2022, 20 octobre 2022, https://www.gov.uk/government/statistics/electronic-monitoring-statistics-publication-september-2022/electronic-monitoring-statistics-publication-england-and-wales-september-2022 (dernière consultation le 25 janvier 2024).

évaluation de l'impact sur la protection des données communiquée par le ministère de l'Intérieur britannique en réponse à une demande adressée par Privacy International au titre de la liberté d'information a révélé l'existence de projets de déploiement d'un système de suivi par montre intelligente pour une surveillance périodique quotidienne des demandeurs et demandeuses d'asile présents au Royaume-Uni[21].

Alors que l'immixtion dans la vie privée d'une personne n'est autorisée par le droit international relatif aux droits humains que si elle n'est ni arbitraire, ni illégale, les personnes en déplacement – en situation précaire au regard de la législation sur l'immigration, qu'elles soient migrantes, réfugiées ou demandeuses d'asile – se voient de plus en plus souvent obligées de transiger sur leurs droits humains, en échange d'un passage éventuel.

Le droit et les normes internationaux relatifs aux droits humains établissent trois conditions permettant de déterminer si l'immixtion dans la vie privée est légitime ou si elle constitue une violation : premièrement, toute immixtion doit être prescrite par la loi et conforme à celle-ci (légalité) ; deuxièmement, elle doit poursuivre un objectif légitime ; troisièmement, elle doit être strictement nécessaire pour atteindre un objectif légitime, tel que la protection de la sécurité nationale ou de l'ordre public (nécessité) et être conduite d'une manière proportionnée à cet objectif et non discriminatoire, ce qui signifie qu'il faut trouver un équilibre entre la nature et l'étendue de l'immixtion d'une part, et la raison de l'immixtion d'autre part (proportionnalité). Les mesures de substitution à la détention faisant appel aux nouvelles technologies mettent en avant la question de leur proportionnalité, en particulier lorsqu'elles impliquent l'utilisation de technologies expérimentales ayant une multitude de répercussions sur la vie privée.

Un autre motif de préoccupation à l'égard des droits humains est la manière dont l'utilisation de ces technologies exacerbe le profilage ethnique et le maintien de l'ordre préjudiciable aux personnes racisées. Le racisme systémique engendre également des atteintes aux droits humains dans les systèmes de gestion de l'asile et des migrations, notamment dans l'utilisation de technologies e-ATD. Du fait du racisme inhérent aux systèmes de maintien de l'ordre et de gestion de l'immigration, les personnes et les populations racisées sont souvent prises pour cibles, ce qui contribue à la criminalisation des personnes racisées en déplacement[22].

ENCADRÉ 1 : LES ENTREPRISES ET LES DROITS HUMAINS

Toutes les entreprises ont la responsabilité de respecter les droits humains, où qu'elles opèrent dans le monde et dans le cadre de l'ensemble de leurs activités – un concept clairement énoncé dans les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, reconnus dans le monde entier[23]. Cette responsabilité est indépendante des obligations propres aux États en la matière et prévaut sur le respect des lois et règlements nationaux qui protègent les droits fondamentaux[24].

Elle impose aux entreprises d'éviter d'être à l'origine d'atteintes aux droits humains ou d'y contribuer par leurs propres activités, et de remédier aux effets néfastes auxquels elles ont contribué, notamment en remédiant à toute atteinte. Elle oblige en outre les entreprises à s'efforcer de prévenir ou d'atténuer les incidences négatives sur les droits humains qui sont directement liées à leurs activités, produits ou services par leurs relations commerciales, même si elles n'ont pas contribué à ces incidences[25]. Enfin, les entreprises doivent s'abstenir de faire pression sur les gouvernements pour obtenir des concessions ou des avantages, notamment des modifications de la législation ou des politiques en leur faveur, qui auraient un effet préjudiciable sur les droits humains.

21. Nicola Kelly, "Facial recognition smartwatches to be used to monitor foreign offenders in UK", The Guardian, 5 août 2022, https://www.theguardian.com/politics/2022/aug/05/facial-recognition-smartwatches-to-be-used-to-monitor-foreign-offenders-in-uk
22. Monish Bhatia, "Racial surveillance and the mental health impacts of electronic monitoring on migrants", Race & Class, vol. 62, no 3, 26 janvier 2021, p. 18-36, https://doi.org/10.1177/0306396820963485
23. Cette responsabilité a été expressément reconnue par le Conseil des droits de l'homme des Nations unies le 16 juin 2011, lors de l'adoption des Principes directeurs relatifs aux entreprises et aux droits de l'homme (« Principes directeurs des Nations unies »), et le 25 mai 2011, quand les 42 États qui avaient adhéré à la Déclaration de l'OCDE sur l'investissement international et les entreprises multinationales ont adopté à l'unanimité une version révisée des Principes directeurs à l'intention des entreprises multinationales. Voir Conseil des droits de l'homme des Nations unies, résolution 17/4 : les droits de l'homme et les sociétés transnationales et autres entreprises, doc. ONU A/HRC/RES/17/4, 6 juillet 2011, https://documents.un.org/doc/resolution/gen/g11/144/72/pdf/g1114472.pdf?token=Jv4y5rGcMExk9rEvEh&fe=true, Les principes directeurs de l'OCDE à l'intention des entreprises multinationales, 2011, https://www.oecd-ilibrary.org/fr/governance/les-principes-directeurs-de-l-ocde-a-l-intention-des-entreprises-multinationales_9789264115439-fr
24. Haut-Commissariat des Nations Unies aux droits de l'homme, Principes directeurs de l'ONU 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/11/04, 2011, https://www.ohchr.org/fr/publications/reference-publications/guiding-principles-business-and-human-rights-implementing, Principe 11 (commentaire inclus).
25. Ibid., principes 11 et 13 (commentaires inclus).

3.2 LES NOUVELLES TECHNOLOGIES ET L'EXTERNALISATION DU CONTRÔLE AUX FRONTIÈRES

Dans le cadre des efforts de prévention de l'arrivée clandestine de personnes réfugiées et migrantes, les pays du Nord ont adopté des mesures s'appliquant hors de leurs propres frontières, grâce à la coopération avec d'autres pays. Qualifiées d' « externalisation », ces mesures délocalisent les contrôles de l'immigration en amont le long des itinéraires de transit. Elles peuvent comporter des accords officiels ou des arrangements informels par lesquels ces pays du Nord fournissent un soutien technique et financier aux organismes de contrôle des frontières de pays partenaires, notamment des outils opérationnels pour faciliter la contention et les renvois[26].

De plus en plus de politiques d'externalisation du contrôle des frontières qui prévoient le déploiement de technologies numériques sophistiquées et intrusives sont adoptées. Ces technologies renforcent les formes racistes d'exclusion pour bloquer la mobilité des migrant·e·s, réfugié·e·s et demandeurs/euses d'asile issus des communautés noires, musulmanes et racisées[27]. Par exemple, l'Union européenne (UE) a étendu virtuellement ses frontières dans la Méditerranée et à travers les régions de transit en Afrique grâce à un éventail de technologies, notamment des radars, des caméras sophistiquées, des données transmises par satellite, des capteurs opto-électroniques (détecteurs de mouvement, par exemple), des drones et des systèmes biométriques, qui font sentir leurs effets sur les personnes migrantes, réfugiées et demandeuses d'asile noires africaines[28].

Ces technologies comportent des risques pour les droits humains. Les États-Unis et les pays de l'UE ont passé des accords d'externalisation impliquant des échanges de données et de technologies avec des pays connus pour leurs violations graves et généralisées des droits humains des personnes réfugiées et migrantes. En fournissant du matériel, une formation et une coordination de l'assistance aux autorités libyennes, par exemple, l'UE a donnés les moyens aux garde-côtes libyens d'intercepter des embarcations et de ramener les personnes réfugiées et migrantes en Libye, où elles font l'objet de détention arbitraire, de torture et d'autres mauvais traitements, notamment de violences sexuelles, entre autres atteintes aux droits humains[29]. Ce soutien est favorisé par le propre dispositif de surveillance aérienne en temps réel de l'UE : l'Italie et Frontex, l'Agence européenne de garde-frontières et de garde-côtes, survolent la Méditerranée centrale au moyen de drones et d'autres matériels aériens pour identifier les embarcations de réfugié·e·s et de migrant·e·s en mer et communiquer leur position aux autorités libyennes, déclenchant leur intervention. Le système de surveillance de Frontex, Eurosur, recueille également des informations par radar et par satellite, avant de les communiquer à différents pays à travers le réseau méditerranéen Seahorse[30].

Selon des allégations de plus en plus nombreuses, l'utilisation des nouvelles technologies pour surveiller, suivre et intercepter les réfugié·e·s et les migrant·e·s au cours de leur voyage pourrait contribuer à leur mort et les pousser à emprunter des itinéraires plus dangereux pour contourner la surveillance. Ainsi, une étude récente fondée sur une analyse géospatiale a montré une corrélation positive entre « les épreuves et les souffrances » – et, par extension, la mortalité des migrant·e·s, le long de la frontière américano-mexicaine entre les États de l'Arizona et de Sonora – et l'essor des infrastructures de surveillance « intelligente » dans la zone, notamment des miradors complexes faisant appel à l'intelligence artificielle[31]. Ce cas est aussi un exemple de la manière dont le recours aux technologies a des répercussions hétérogènes en fonction de

26. Amnesty International, *The human rights risks of external migration policies*, 13 juin 2017 (index : POL 30/6200/2017), https://www.amnesty.org/en/documents/pol30/6200/2017/en/#:~:text=From%20the%20perspective%20of%20international,pose%20significant%20human%20rights%20risks
27. E. Tendayi Achiume, "Digital Racial Borders", AJIL Unbound, vol. 115, 11 octobre 2021, p. 333-38, https://doi.org/10.1017/aju.2021.52
28. Ruben Andersson, *Illegality, Inc.: Clandestine Migration and the Business of Bordering Europe*, University of California Press, 2014, p. 84-7 ; Agence européenne de garde-frontières et de garde-côtes (Frontex), *Artificial Intelligence-based capabilities for the European Border and Coast Guard*, 17 mars 2021, https://www.frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_executive_summary.pdf
29. Amnesty International, « Libye. De nouveaux éléments prouvent que les personnes réfugiées ou migrantes sont prises au piège dans un terrifiant cycle de violences », 24 septembre 2020, https://www.amnesty.org/fr/latest/press-release/2020/09/libya-new-evidence-shows-refugees-and-migrants-trapped-in-horrific-cycle-of-abuses/ ; Amnesty International, *« Personne ne te cherchera » : la détention abusive des personnes réfugiées et migrantes débarquées en Libye*, 15 juillet 2021 (index : MDE 19/4439/2021), https://www.amnesty.org/fr/documents/mde19/4439/2021/fr/
30. Amnesty International, "Contribution to European Ombudsman's Strategic Inquiry OI/3/2023/MHZ", 31 octobre 2023, amnesty.eu/news/contribution-to-european-ombudsmans-strategic-inquiry-oi-3-2023-mhz-the-role-of-the-european-border-and-coast-guard-agency-frontex-in-the-context-of-search-and-rescue-operations/
31. Samuel Norton Chambers, Geoffrey Alan Boyce, Sarah Launius et Alicia Dinsmore, "Mortality, surveillance and the tertiary 'funnel effect' on the US-Mexico border: a geospatial modeling of the geography of deterrence", Journal of Borderlands Studies, vol. 36, no 3, 31 janvier 2019, p. 443-468, https://www.tandfonline.com/doi/abs/10.1080/08865655.2019.1570861

l'appartenance ethnique des personnes et des communautés, qui subissent un risque accru de profilage ethnique le long de la frontière si elles sont noires, latino-américaines ou racisées en général[32].

En soi, les politiques migratoires externes ne sont pas illégales du point de vue du droit international. Néanmoins, les politiques axées sur l'externalisation du contrôle des frontières ou de l'instruction des demandes d'asile comportent des risques très élevés pour les droits humains. Leur mise en oeuvre aboutit souvent à la contention ou au renvoi des personnes migrantes, réfugiées et demandeuses d'asile dans des pays où elles subissent de graves atteintes aux libertés fondamentales. Ces libertés mises en danger sont notamment le droit de chercher asile et d'en bénéficier, le droit de ne pas faire l'objet d'une arrestation et d'une détention arbitraires, le droit à la protection contre toute mesure de « refoulement » – qui interdit aux États de renvoyer ou de transférer toute personne, d'une manière ou d'une autre, dans un lieu où elle risquerait de subir des actes de torture ou d'être victime d'autres atteintes graves aux droits humains[33] – et le droit de ne pas subir de discrimination.

Par ailleurs, les mesures d'externalisation, qui transfèrent à des pays tiers la responsabilité de fournir une protection internationale, aggravent le partage inégal de la responsabilité de la protection des réfugié·e·s entre les pays du Nord et les pays du Sud, qui reçoivent l'immense majorité des réfugié·e·s. Enfin, l'externalisation de la protection des réfugié·e·s n'est pas conforme aux principes de solidarité et de coopération internationale, sur lesquels repose le système de protection international.

3.3 LOGICIELS D'EXTRACTION DE DONNÉES

L'utilisation de logiciels d'extraction de données à des fins de contrôle de l'immigration est une tendance en pleine croissance. Comme l'a souligné l'ancienne rapporteuse spéciale sur les formes contemporaines de racisme, elle « ne vise que les demandeurs d'asile et sa légalisation repose sur un discours politique raciste et xénophobe[34] ». Dans des pays tels que l'Allemagne, l'Autriche, la Belgique, le Danemark, la Norvège et le Royaume-Uni, la loi autorise la saisie des téléphones des migrant·e·s et des demandeurs/euses d'asile ainsi que l'extraction de données de ceux-ci afin de corroborer (ou non) leurs témoignages lors de l'instruction de leur demande d'asile[35]. Ainsi, il peut être procédé à une analyse des recherches, de la navigation et de l'activité sur les réseaux sociaux, au suivi de l'historique des déplacements grâce aux enregistrements GPS et aux métadonnées, et même à la consultation des informations stockées sur un nuage que l'utilisateur pense avoir supprimées[36].

L'utilisation de logiciels d'extraction des données des téléphones a fait l'objet d'un procès intenté par l'ONG allemande Gesellschaft für Freiheitsrechte (GFF) au nom de trois personnes demandeuses d'asile[37]. L'Office fédéral allemand des migrations et des réfugié·e·s (BAMF) a d'abord introduit cette politique en 2017, autorisant « l'extraction et l'analyse des données stockées sur les supports d'information tels que les téléphones, afin de vérifier l'exactitude de l'origine et de l'identité déclarées de leur propriétaire[38] ». Seuls les avocats peuvent consulter ce système, qui produit un rapport pour chaque cas d'extraction. Les demandeurs et demandeuses d'asile n'y ont pas accès. D'après un rapport de GFF, 64 % des cas n'aboutissent à aucun résultat utilisable, 34 % confirment l'origine et l'identité déclarées par les propriétaires des téléphone et seulement 2 % contredisent les déclarations des demandeurs/euses. Au cours du procès, la partie demanderesse a argumenté que les autorités allemandes avaient violé le droit au respect de la vie privée en ordonnant systématiquement aux personnes de débloquer leur téléphone portable et de le leur remettre pour « évaluation[39] ». Le tribunal a jugé que, dans ce cas spécifique, les recherches étaient

32. Amnesty International, *In Hostile Terrain: Human Rights Violations in Immigration Enforcement in the US Southwest*, 28 mars 2012 (index : AMR 51/018/2012, https://www.amnesty.org/en/documents/amr51/018/2012/en
33. Amnesty International, *The human rights risks of external migration policies*, 13 juin 2017 (index : POL 30/6200/2017), https://www.amnesty.org/en/documents/pol30/6200/2017/en
34. E. Tendayi Achiume, rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Rapport : *La discrimination raciale et la xénophobie et l'utilisation des technologies numériques dans le contrôle des frontières et de l'immigration* (op. cit.), § 33.
35. Petra Molnar, *Technological Testing Grounds: Border Tech Is Experimenting with People's Lives*, European Digital Rights (EDRi) et Refugee Law Lab, novembre 2020, https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf, p. 18.
36. Privacy International, *The UK's Privatised Migration Surveillance Regime: A rough guide for civil society,* février 2021, https://www.privacyinternational.org/sites/default/files/2021-01/PI-UK_Migration_Surveillance_Regime.pdf
37. TRT World, "Refugees take Germany to court over mobile phone data checks", 6 mai 2020, https://www.trtworld.com/europe/refugees-take-germany-to-court-over-mobile-phone-data-checks-36057
38. Anna Biselli et Lea Beckmann, *Invading Refugees' Phones: Digital Forms of Migration Control in Germany and Europe*, février 2020, https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Gesellschaft_fur_Freiheitsrechte.pdf
39. Gesellschaft für Freiheitsrechte, 'Invading Refugees' Phones: Digital Forms of Migration Control', décembre 2019, https://freiheitsrechte.org/uploads/publications/Digital/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control-Gesellschaft_fuer_Freiheitsrechte_2019.pdf

systématiquement disproportionnées, car des mesures moins intrusives auraient pu être appliquées. Il a laissé ouverte la question de savoir si cette pratique pourrait être légale dans d'autres circonstances.

En mars 2022, la Haute Cour du Royaume-Uni a conclu que le ministère de l'Intérieur a agi de manière illégale, enfreignant les lois relatives aux droits humains et à la protection des données, lorsqu'il a saisi les téléphones d'au moins trois personnes demandeuses d'asile arrivant dans le pays à bord de petites embarcations, puis a fait pression sur celles-ci pour connaître leur mot de passe[40]. L'opacité des politiques relatives à la saisie et la conservation des dispositifs perpétue et renforce un environnement hostile et dangereux pour les personnes demandeuses d'asile.

Sans le consentement libre de leur propriétaire, l'extraction de données pour l'instruction de demandes d'asile comporte une multitude de risques pour les droits humains, notamment le droit au respect de la vie privée et le droit de chercher asile. Elle expose les personnes au danger d'être renvoyées de force dans un pays où elles risquent de subir des persécutions et autres atteintes graves aux droits humains. L'extraction de données peut représenter une immixtion disproportionnée et injustifiée dans la vie privée des personnes réfugiées et migrantes au motif de leur situation ; elle repose souvent sur de la discrimination fondée sur des facteurs tels que l'appartenance ethnique, le pays d'origine et la nationalité[41]. Or, même lorsque ces systèmes d'extraction de données recueillent toutes les données disponibles, sans discrimination – en raison des spécificités techniques des instruments utilisés –, ils constituent en soi une immixtion disproportionnée dans le droit au respect de la vie privée. La fiabilité des données obtenues par des méthodes si intrusives soulève également des inquiétudes. L'extraction de données peut servir à nuire au droit à une procédure d'asile équitable lorsqu'elle permet aux autorités de tirer des conclusions hâtives et douteuses au sujet d'une demande d'asile[42]. Par ailleurs, elle renforce également la stigmatisation et la discrimination existant déjà à l'égard des personnes et des populations racisées.

ENCADRÉ 2 : L'INTERSECTIONNALITÉ

Cet exposé introductif donne un aperçu général des conséquences néfastes des technologies numériques sur les droits humains dans la vie des personnes migrantes, réfugiées et demandeuses d'asile, mais la gravité de ces répercussions peut augmenter considérablement en fonction de l'âge, du genre, de l'orientation sexuelle, de l'origine ou l'appartenance ethnique, de la classe sociale ou de la caste, de la situation de handicap et de facteurs socio-economiques, notamment. En d'autres termes, l'âge, le genre, l'orientation sexuelle, l'origine ou l'appartenance ethnique, la classe ou la caste, la situation de handicap et les facteurs socio-économiques jouent tous un rôle dans la détermination et, d'une certaine manière, l'aggravation des risques de la technologie pour les personnes migrantes, réfugiées et demandeuses d'asile. Comme la discrimination structurelle n'est pas un phénomène isolé, certaines personnes peuvent être victimes de formes uniques ou supplémentaires de discrimination en raison d'un ensemble de différentes formes de discrimination qui s'ajoutent les unes aux autres.

Par exemple, les enfants migrants et réfugiés peuvent être plus exposés à une collecte de données et une surveillance intrusives en raison de leur âge, à une autonomie plus limitée et à des déséquilibres de pouvoir entre eux et les adultes qui recueillent ces données, alors que leur compréhension des répercussions à court et à long termes de la collecte de leurs données personnelles est encore plus limitée. Les gouvernements, les entreprises et les acteurs humanitaires doivent prendre en compte ces facteurs lorsqu'ils collectent les données biométriques d'enfants.

Du point de vue de la justice raciale, ces technologies entraînent également de graves conséquences discriminatoires. Tendayi Achiume, ancienne rapporteuse spéciale des Nations unies sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est

40. La décision de justice est disponible dans son intégralité à l'adresse suivante : Cour royale de Justice du Royaume-Uni, affaire no CO/4793/2020, CO/577/2021, 25 mars 2022, https://dpglaw.co.uk/wp-content/uploads/2022/03/MA-KH-judgment.pdf
41. Généralement, ce processus suppose une intention de tromper et fait appel à des variables réductrices (langue de l'appareil, lieu de son achat, langue utilisée pour les communications à partir de celui-ci) pour déterminer automatiquement le pays de provenance. Gesellschaft für Freiheitsrechte, "Germany: Invading refugees' phones – security or population control?", 11 mars 2020, https://edri.org/our-work/germany-invading-refugees-phones-security-or-population-control ; E. Tendayi Achiume, rapporteuse spéciale des Nations unies sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Rapport : *La discrimination raciale et la xénophobie et l'utilisation des technologies numériques dans le contrôle des frontières et de l'immigration* (op. cit.).
42. Amnesty International, "Open Letter to the Rapporteurs on the EU Artificial Intelligence Regulation (AI ACT) to ensure Protection of Rights of Migrants, Asylum Seekers and Refugees", 26 avril 2023, https://www.amnesty.eu/wp-content/uploads/2023/04/TIGO_IOR_10_2023_3987_Open-letter-to-the-Rapporteurs-on-the-EU-AI-Act-1.pdf

associée, a publié de nombreux documents et prononcé de nombreuses interventions à ce sujet. Elle a déjà argumenté ce qui suit :

« des exemples de différentes régions du monde montrent que la conception et l'utilisation de différentes nouvelles technologies numériques peuvent être conjuguées, intentionnellement ou non, pour créer des structures discriminatoires sur le plan racial qui entravent globalement ou systématiquement la jouissance des droits de l'homme de certains groupes de personnes en raison de leur race, de leur appartenance ethnique ou de leur origine nationale, venant s'ajouter à d'autres caractéristiques. Autrement dit, il faut comprendre que les nouvelles technologies numériques peuvent non seulement entraver l'accès à tel ou tel droit humain et la jouissance de ce droit, mais aussi créer et entretenir une exclusion raciale et ethnique systémique ou structurelle[43]. »

3.4 BIOMÉTRIE

La biométrie est l'une des technologies les plus répandues déployées à des fins d'identification, de vérification et d'authentification le long des frontières. Le recueil et l'utilisation de données biométriques soulèvent des inquiétudes parce qu'ils impliquent des formes directes et indirectes de discrimination en fonction de l'appartenance ethnique, du pays d'origine, de l'ascendance et de la religion. Ces formes de discrimination sont notamment les erreurs de reconnaissance des personnes noires commises par les technologies de reconnaissance faciale ou les exclusions de fait fondées sur le pays d'origine. Une multitude d'organismes nationaux et internationaux se constituent des bases de données biométriques afin de recouper les informations fournies par les personnes avec des listes de surveillance, d'identifier les pays d'origine et de transit et de vérifier l'identité des personnes réfugiées et migrantes[44]. Des organisations humanitaires telles que l'Agence des Nations unies pour les réfugiés (HCR[45]) et le Programme alimentaire mondial des Nations unies (PAM) ont mis au point de vastes bases de données mondiales pour regrouper les empreintes digitales ou iriennes, dans une tentative manifeste d'empêcher les enregistrements multiples et les duplications de données relatives aux réfugié·e·s. Les États membres de l'UE s'en remettent largement à des bases contenant des données biométriques, comme Eurodac[46], qui aide, entre autres, à déterminer quel État est responsable de l'instruction d'une demande d'asile déposée dans l'UE[47].

En octobre 2018, l'UE a annoncé avoir octroyé des financements à un nouveau système de contrôle automatisé aux frontières, mis à l'essai en Grèce, en Hongrie et en Lettonie. Ce projet, appelé iBorderCtrl, est un système de « détection de mensonges » conçu à partir de technologies d'intelligence artificielle, dont l'interface consiste en un garde-frontière virtuel chargé de poser des questions aux voyageurs souhaitant franchir la frontière en même temps qu'il évalue les détails infimes de leurs expressions faciales (les « micro-expressions »), à l'aide de technologies de reconnaissance des visages et des émotions. Les personnes dont les réponses sont jugées honnêtes par le système se voient remettre un code les autorisant à passer la frontière, tandis que celles qui n'ont pas eu cette chance sont orientées vers des gardes-frontières en chair et en os pour être à nouveau interrogées[48].

43. E. Tendayi Achiume, rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Rapport : *Discrimination raciale et nouvelles technologies numériques : analyse sous l'angle des droits de l'homme*, doc. ONU A/HRC/44/57, 18 juin 2020, https://documents.un.org/doc/undoc/gen/g20/151/07/pdf/g2015107.pdf?token=j0YISQx66ANFZQkZH3&fe=true, § 38.
44. Claire Walkey, Caitlin Procter et Nora Bardelli, "Biometric refugee registration: between benefits, risks and ethics", Blog de la London School of Economics and Political Science (LSE), 18 juillet 2019, https://blogs.lse.ac.uk/internationaldevelopment/2019/07/18/biometric-refugee-registration-between-benefits-risks-and-ethics/
45. HCR, "Biometric Identity Management System: Enhancing registration and data management", https://www.unhcr.org/media/biometric-identity-management-system
46. Irma Van der Ploeg, "The illegal body: Eurodac and the politics of biometric identification", Ethics and Information Technology, vol. 1, décembre 1999, https://doi.org/10.1023/A:1010064613240, p. 295-302 ; Règlement (UE) no 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) no 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) no 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte), https://eur-lex.europa.eu/eli/reg/2013/603/oj?locale=fr
47. Règlement (UE) no 604/2013 du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (refonte), https://eur-lex.europa.eu/eli/reg/2013/604/oj
48. Amnesty International, « Les technologies automatisées et l'avenir de la forteresse Europe », 28 mars 2019, https://www.amnesty.org/fr/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/

iBorderCtrl n'est qu'un exemple des nombreux projets d'automatisation du contrôle aux frontières de l'UE, dont l'objectif est de lutter contre l'immigration clandestine. Cette nouvelle tendance qui se dessine en Europe soulève toute une série de graves préoccupations en matière de droits humains. L'une d'entre elles – et pas des moindres – est que cette « détection de mensonges » à partir des « micro-expressions » a été discréditée car elle repose sur la phrénologie, qui entretient des liens étroits avec la pensée eugéniste[49]. Nommées pour la première fois dans les travaux de Paul Ekman, les « micro-expressions » sont un prétendu moyen d'établir la vérité en fonction de la fréquence des clignements d'yeux, de la direction du regard, des mouvements des muscles du visage et des changements de ton de la voix. L'outil iBorderCtrl classe ces données selon différents degrés de duplicité, en fonction d'une échelle de référence universelle établie autour de l'intersection entre les expressions faciales et la moralité.

De telles présomptions nuisent sans aucun doute à la dignité du traitement des personnes migrantes, dont l'intention est mesurée en disséquant leurs expressions faciales selon une méthode pseudo-scientifique pour les opposer à leur intention déclarée. Non seulement imprécise et injustifiée, cette technique a également de graves répercussions sur les droits au respect de la vie privée, à l'égalité et à la non-discrimination, ainsi que sur le droit d'asile et sur le droit de circuler librement.

Les systèmes de surveillance des frontières entourant l'UE ne sont qu'une manifestation parmi d'autres de la tendance au solutionnisme technologique, selon laquelle les gouvernements et les entreprises technologiques ont recours à des solutions techniques sophistiquées pour résoudre tous les problèmes, depuis le changement climatique jusqu'à la famine et les migrations, détournant souvent l'attention des solutions politiques structurelles requises indépendamment de tout recours aux nouvelles technologies. Le montant des investissements dans des projets reposant sur des technologies automatisées à des fins de contrôle frontalier financés par Horizon 2020[50], le plus gros programme européen pour la recherche et l'innovation à ce jour, témoigne très clairement de l'intérêt de l'UE pour ce domaine.

Entre 2014 et 2020, par exemple, Frontex a investi 434 millions d'euros dans les infrastructures de surveillance et des technologies de l'information. Pour la période 2021-2027, la Commission européenne a réservé 34,9 milliards d'euros pour le contrôle des frontières en général[51], affectés notamment au futur système européen d'information et d'autorisation concernant les voyages (ETIAS). L'ETIAS recoupe les informations en accès libre sur Internet, notamment les publications sur les réseaux sociaux, les informations médicales et autres, pour évaluer l'identité numérique d'un voyageur/d'une voyageuse et déterminer la menace que cette personne peut représenter pour la sécurité de l'Europe. Ces types de systèmes favorisent et renforcent l'exclusion des personnes racisées[52].

En 2016 et en 2020, la Commission européenne a proposé des révisions successives du règlement Eurodac, dans le but d'élargir la base de données biométriques sur les personnes migrantes. Le 20 décembre 2023, le Conseil et le Parlement européen sont parvenus à un accord politique au sujet de ce règlement, dans le cadre d'une ensemble de réformes plus vaste. Ces réformes, qui seront adoptées officiellement en 2024, entraîneront l'adoption des mesures suivantes : élargir les catégories des données personnelles stockées dans Eurodac, comme les images faciales ; rendre obligatoire la collecte des données biométriques à l'égard de toute personne âgée de plus de six ans (contre 14 ans selon les règles actuelles) ; élargir le champ d'application personnel d'Eurodac ; faciliter l'accès aux données pour les autorités chargées de l'application des lois[53].

Les données biométriques sont considérées comme des données particulièrement sensibles, car elles permettent d'identifier une personne à l'aide d'un fichier où sont enregistrées des caractéristiques personnelles immuables. La création de fichiers permanents contenant les données biométriques des personnes réfugiées et migrantes pose des problèmes particuliers en matière de droits humains. Les informations concernant les personnes réfugiées et demandeuses d'asile risquent d'être communiquées

49. Amnesty International, « Amnesty International et plus de 170 organisations demandent l'interdiction de la surveillance biométrique », 7 juin 2021, https://www.amnesty.org/fr/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/ ; Catherine Stinson, "The Dark Past of Algorithms That Associate Appearance and Criminality", American Scientist, vol. 109, no 1, janvier-février 2021, https://www.americanscientist.org/article/the-dark-past-of-algorithms-that-associate-appearance-and-criminality, p. 26 ; Javier Sánchez-Monedero et Lina Dencik, "The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl", Information, Communication & Society, vol. 25, no 3, 2020, https://doi.org/10.1080/1369118X.2020.1792530, p. 413-430.
50. Commission européenne, Horizon 2020, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en (dernière consultation le 25 janvier 2024).
51. Frontex, *Artificial Intelligence-based capabilities for the European Border and Coast Guard* (op. cit.).
52. E. Tendayi Achiume, "Racial Borders", Georgetown Law Journal, vol. 110, no 3, 2022, https://www.law.georgetown.edu/georgetown-law-journal/in-print/volume-110/volume-110-issue-3-may-2022/racial-borders
53. Conseil de l'Union européenne, « Le Conseil et le Parlement européen parviennent à une avancée dans la réforme du système d'asile et de migration de l'UE », 20 décembre 2023, https://www.consilium.europa.eu/fr/press/press-releases/2023/12/20/the-council-and-the-european-parliament-reach-breakthrough-in-reform-of-eu-asylum-and-migration-system/

– intentionnellement (dans le cadre, par exemple, d'une politique publique) ou par inadvertance (à cause de fuites de données ou de lacunes dans la sécurité des systèmes, notamment) – aux autorités du pays qu'elles ont fui, aggravant les risques de persécutions et d'atteintes aux droits humains pour elles et les membres de leurs familles[54]. Les motifs d'inquiétude proviennent également des risques de surveillance, de fuites de données, de restrictions du droit de circuler librement, de profilage discriminatoire et de criminalisation de groupes ethniques ou religieux, entre autres groupes racisés, déjà marginalisés.

En dehors du contexte des migrations, par exemple, les recherches d'Amnesty International dans les territoires palestiniens occupés ont démontré que le système de reconnaissance faciale déployé aux postes de contrôle militaires d'Hébron, Red Wolf, était utilisé pour empêcher la population palestinienne de circuler librement dans la zone. Amnesty International a découvert que les restrictions de la liberté de circuler imposées aux postes de contrôle à l'aide de la reconnaissance faciale n'étaient pas temporaires ou limitées, mais systématiques et discriminatoires, avec des bases de données comprenant seulement des données sur les Palestinien·ne·s, à des postes de contrôle réservés aux Palestinien·ne·s, sans aucune répercussion sur les colons juifs israéliens[55].

ENCADRÉ 3 : RECONNAISSANCE FACIALE, SURVEILLANCE DE MASSE ET RACISME

Les outils de reconnaissance faciale utilisés à des fins d'identification violent le droit au respect de la vie privée, car ils ne peuvent satisfaire aux principes de nécessité et de proportionnalité inscrits dans le droit international relatif aux droits humains. Ils impliquent une surveillance, une collecte, un stockage, une analyse ou une autre utilisation à grande échelle des données, ainsi qu'une collecte de données sensibles à caractère personnel (données biométriques). En outre, les systèmes de reconnaissance faciale sont entraînés grâce à des algorithmes de reconnaissance d'image qui, pour améliorer leur « taux de réussite », utilisent en guise de données entrantes de vastes quantités d'images de visages collectées à l'insu et sans le consentement des personnes concernées. Même si les données entrantes ou les données d'entraînement sont effacées, l'algorithme du système a déjà tiré profit des visages ayant alimenté le système auparavant et les utilise de fait à l'insu et hors de tout contrôle des personnes concernées.

Qui plus est, les préjudices causés par la reconnaissance faciale aux droits humains ne sont pas ressentis de manière égale et soulèvent des risques bien connus en matière de discrimination. Par exemple, certains groupes peuvent être représentés de manière disproportionnée dans les bases de données d'images faciales, en raison de pratiques discriminatoires des forces de l'ordre, notamment. Par ailleurs, il est attesté que le fonctionnement des systèmes de reconnaissance faciale est source d'inégalités se manifestant en fonction de caractéristiques essentielles telles que la couleur de la peau, l'appartenance ethnique et le genre. Plusieurs experts des Nations unies ont souligné ces risques de discrimination[56].

En janvier 2021, Amnesty International a lancé la campagne mondiale Ban the Scan en vue d'interdire l'utilisation des systèmes de reconnaissance faciale, une forme de surveillance de masse qui décuple le risque de racisme lors des opérations policières et menace le droit de manifester. La campagne Ban the Scan a mis en évidence la manière dont la reconnaissance faciale enfreint les droits humains dans des villes comme New York, Hyderabad, Hébron et Jérusalem-Est, dans les territoires palestiniens occupés. En particulier, Amnesty International continue de dénoncer la manière dont les technologies sont déployées de manière discriminatoire à l'égard de populations traditionnellement marginalisées.

De manière plus générale, il existe aussi un danger de détournement de fonction, c'est-à-dire d'élargissement de l'usage d'une technologie ou de données au-delà de leur objectif initial, comme dans le cas de l'utilisation à des fins de contrôle des migrations des données collectées par des organismes humanitaires pour l'enregistrement et l'accès à des services. L'ancienne rapporteuse spéciale sur les

54. Ben Hayes et Massimo Marelli, "Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases", *Regulating Biometrics: Global Approaches and Urgent Questions*, Amba Kak (sous la direction de), Institut AI NOW, 2020, https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions
55. Amnesty International, *Apartheid automatisé – Comment la reconnaissance faciale fragmente, ségrègue et contrôle la population palestinienne dans les TPO*, 2 mai 2023 (index : MDE 15/6701/2023), https://www.amnesty.org/fr/documents/mde15/6701/2023/fr/ ; L'article 49 de la Quatrième Convention de Genève dispose : « La puissance occupante ne pourra procéder à la déportation ou au transfert d'une partie de sa propre population civile dans le territoire occupé par elle. » Il interdit également « les transferts forcés, en masses ou individuels […], ainsi que les déportations de personnes protégées hors du territoire occupé ».
56. Comité pour l'élimination de la discrimination raciale, projet de recommandation générale (n°36) concernant la prévention du profilage racial et la lutte contre cette pratique, 14 mai 2019, https://www.ohchr.org/sites/default/files/Documents/HRBodies/CERD/GC36/DraftGC36.docx [en anglais], § 23.

formes contemporaines de racisme a averti que la nature même de la collecte de données peut avoir des effets profondément discriminatoires[57]. En particulier, l'utilisation de systèmes centralisés de stockage des données biométriques peut faciliter la surveillance et l'utilisation abusive des informations, ainsi qu'aggraver les préjudices causés par les éventuelles fuites de données. En 2018, il a été signalé que le gouvernement du Bangladesh partageait avec le Myanmar des données biométriques collectées par le HCR sur les réfugié·e·s rohingyas, alors même que le Myanmar est le pays que ces personnes ont fui pour échapper au nettoyage ethnique et aux violences.Ces informations ont ensuite été confirmées par Human Rights Watch, qui a accusé le HCR de fournir les informations à caractère personnel de réfugié·e·s au gouvernement du Bangladesh[58]. Des données biométriques collectées initialement pour permettre l'enregistrement de réfugié·e·s afin d'avoir accès à des services ont été partagées à des fins de rapatriement, sans le consentement libre et éclairé des personnes concernées, les exposant à des risques.

Un facteur favorisant ces relations dangereuses est l'essor de l'interopérabilité sur laquelle s'appuie le partage de données entre organisations humanitaires, gouvernements nationaux et organismes en charge de la sécurité. Bien qu'elle soit certes utile dans certains contextes, cette interopérabilité comporte des risques importants dans le contexte des migrations[59]. Malgré des freins à l'interopérabilité liés à la bureaucratie, aux gouvernements, aux entreprises et aux droits de propriété, les accords internationaux d'échange de données progressent entre les organisations humanitaires ainsi qu'entre les institutions en charge du contrôle des frontières et de l'immigration. En 2019, deux règlements européens sont entrés en vigueur en faveur de l'interopérabilité, fusionnant « six bases de données existant au sein de l'UE, créées à des fins de sécurité et de gestion des frontières, [...] en un seul système d'information global pour toute l'UE[60] ».

La biométrie et l'échange de données peuvent aussi servir à définir et à refuser l'accès à des services. Même lorsque les gouvernements ou les organisations humanitaires obtiennent le consentement des personnes réfugiées et migrantes au traitement de leurs données, ce consentement ne peut être compris comme ayant nécessairement été donné librement car, en général, les personnes ne peuvent refuser de se soumettre au recueil de données biométriques sans perdre la possibilité de s'enregistrer et d'accéder aux services essentiels[61].

Dans son rapport présenté en 2013 à l'Assemblée générale des Nations unies, le rapporteur spécial sur les droits de l'homme des migrants, François Crépeau, a exhorté les États à permettre aux personnes migrantes d'avoir accès aux services publics nécessaires à l'exercice de leurs droits sans crainte d'être arrêtées, détenues ou expulsées du territoire. Pour ce faire, les États devraient mettre en place des « pare-feu » entre les services publics et ceux chargés du contrôle de l'immigration, en vertu desquels les services publics (soins de santé, éducation, logement, inspection de la main-d'œuvre, police locale) auraient pour instruction de ne pas demander d'information sur le statut d'immigration à moins que ce ne soit essentiel, et les services de contrôle de l'immigration n'auraient pas accès à l'information recueillie par les services publics en rapport avec le statut d'immigration[62].

3.5 PRISE DE DÉCISIONS ALGORITHMIQUE DANS LES SYSTÈMES DE GESTION DE L'ASILE ET DES MIGRATIONS

Dans un rapport intitulé *Bots at the Gate*, une équipe de recherche du Citizen Lab, de l'université de Toronto, a enquêté sur différents outils de prise de décisions algorithmique mis au point pour le système canadien de gestion de l'asile et de l'immigration, à la frontière et dans les villes. L'utilisation d'outils algorithmiques

57. E. Tendayi Achiume, rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Rapport : *La discrimination raciale et la xénophobie et l'utilisation des technologies numériques dans le contrôle des frontières et de l'immigration* (op. cit.), § 40.
58. Human Rights Watch, "UN Shared Rohingya Data Without Informed Consent", 15 juin 2021, https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent
59. Voir, par exemple, Statewatch et PICUM, "Weak anti-discrimination safeguards", *Protection des données, application des lois migratoires et droits fondamentaux : quelles sont les conséquences des régulations de l'UE en matière d'interopérabilité pour les personnes en situation irrégulière ?*, novembre 2019, https://www.statewatch.org/media/documents/analyses/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf, [en anglais ; seul le résumé a été traduit en français], p. 33-34.
60. Cristina Blasi Casagran, "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU", Human Rights Law Review, vol. 21, no 2, juin 2021, https://doi.org/10.1093/hrlr/ngaa057, p. 433–457.
61. Entretien d'Amnesty International avec Marwa Fatafta, membre de la direction d'Access Now, 16 mars 2021 ; Ben Hayes et Massimo Marelli, "Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases" (op. cit.).
62. Rapporteur spécial sur les droits de l'homme des migrants, Rapport, doc. ONU A/68/287, 7 août 2013, https://www.un.org/fr/ga/68/resolutions.shtml, § 82.

d'évaluation du risque par les agents canadiens des services d'immigration afin d'approuver ou de rejeter les demandes d'asile et de visa est particulièrement alarmante[63]. Les universitaires Petra Molnar et Lex Gil ont appelé ces initiatives un « laboratoire d'expériences à haut risque », pointant du doigt des préoccupations au sujet de leurs retombées sur les droits humains[64].

Les décisions prises par des algorithmes dans les systèmes de gestion de l'asile et des migrations sont susceptibles d'être arbitraires et impossibles à contester en l'absence de garanties de procédure. Exposée aux biais, aux dysfonctionnements et autres erreurs, l'utilisation de ces outils pourrait avoir des conséquences dévastatrices sur les personnes réfugiées et migrantes, notamment la séparation de familles, des expulsions du territoire et des refus d'accorder l'asile. Elle peut aussi aboutir à du profilage ethnique et au refus discriminatoire d'accorder des visas pour des caractéristiques réelles ou perçues liées notamment à l'appartenance ou l'origine ethnique, au pays d'origine, à l'ascendance ou à la religion, souvent à cause du présupposé abusif selon lequel les personnes ayant certaines nationalités ou certaines caractéristiques représentent un « risque » pour le respect des politiques migratoires ou des « menaces » pour la sécurité nationale[65]. Ces présupposés reposent sur des idéologies, des discours et des structures racistes et xénophobes, qui servent à les justifier.

Le ministère de l'Intérieur du Royaume-Uni a déployé le même type de méthodes automatisées de prévision des risques[66]. En 2020, l'organisation à but non lucratif Foxglove, qui se bat pour que les nouvelles technologies soient justes pour tous et toutes, et le Conseil commun pour le bien-être des immigrant·e·s (Joint Council for the Welfare of Immigrants, JCWI) ont réussi à faire abandonner les algorithmes de criblage des demandes de visa utilisés par le ministère de l'Intérieur. Ils avaient argumenté que ce dispositif consolidait le racisme et les préjugés dans le système de traitement des demandes de visa[67] en attribuant à certaines nationalités une notation du risque renforçant la discrimination, alors qu'à cause de problèmes dans les boucles de rétroaction, cette discrimination et des biais antérieurs servaient de référence à l'évaluation des dossiers ultérieurs.

ENCADRÉ 4 : LE RACISME SYSTÉMIQUE ET L'INTERDICTION DE LA DISCRIMINATION RACIALE

Le racisme systémique est ancré dans les politiques et les pratiques de contrôle des migrations et des frontières, engendrant des formes directes et indirectes de discrimination à caractère raciste. Les principes d'égalité et de non-discrimination concernent l'ensemble du droit international relatif aux droits humains et des normes connexes. Ils ont pour but d'instaurer une égalité devant la loi, en théorie et en pratique. Or, comme l'a fait remarquer l'ancienne rapporteuse spéciale sur les formes contemporaines de racisme, les lois et les politiques relatives à l'immigration ne sont pas neutres à l'égard des personnes racisées et renforcent les inégalités et la discrimination qu'elles subissent. Les technologies numériques ont donc des conséquences discriminatoires exacerbées à l'égard des personnes réfugiées et migrantes racisées, fondées notamment sur des caractéristiques telles que l'appartenance ou l'origine ethnique, le pays d'origine, l'ascendance, la nationalité et la religion. Les technologies numériques sont de plus en plus souvent employées au profit de programmes, discours et structures racistes et xénophobes contraires aux normes internationales relatives aux droits humains.

Comme l'a souligné l'ancienne rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée dans son rapport de 2020 sur les nouvelles technologies numériques et la discrimination raciale :

« Il ne fait plus aucun doute que les nouvelles technologies numériques ont une capacité remarquable de reproduire, de renforcer et même d'exacerber les inégalités raciales que l'on constate au sein des sociétés et entre elles. Un certain nombre d'études universitaires importantes ont montré que la conception et l'utilisation des technologies avaient déjà cet effet précis dans différents contextes. »

63. Petra Molnar et Lex Gil, *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System*, 2018, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf
64. Ibid.
65. E. Tendayi Achiume, rapporteuse spéciale des Nations unies sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Rapport : *La discrimination raciale et la xénophobie et l'utilisation des technologies numériques dans le contrôle des frontières et de l'immigration* (op. cit.).
66. Foxglove, "Home Office says it will abandon its racist visa algorithm—after we sued them", 4 août 2020, https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them ; Joe Tomlinson, "EU Settlement Scheme ushers in a new era of automated decision-making at the Home Office", 16 juillet 2019, Free Movement, https://www.freemovement.org.uk/eu-settlement-scheme-automated-decision-making
67. Foxglove, "Home Office says it will abandon its racist visa algorithm—after we sued them" (op. cit.).

Par ailleurs, les systèmes automatisés d'évaluation du risque représentent des dangers pour les droits et les principes relatifs à la protection des données. Même lorsque le profilage ne repose pas directement sur des catégories spécifiques de données personnelles protégées par des garanties renforcées par la législation applicable, comme le règlement général de l'UE sur la protection des données (RGPD), il peut découler d'informations révélant indirectement ces données. Par exemple, les convictions religieuses ou les données de santé d'un voyageur peuvent être déduites de ses préférences alimentaires, ce qui donne lieu à une infraction du droit à la protection des données et à du profilage ethnique. Compte tenu du déséquilibre de pouvoir entre les autorités en charge de la gestion des migrations et les personnes réfugiées, migrantes et demandeuses d'asile, les informations utilisées pour les systèmes de profilage peuvent aussi être extraites de manière coercitive et illégale, sans que les personnes concernées donnent librement leur consentement spécifique et éclairé, comme le prévoit le RGPD[68].

Qui plus est, les outils d'évaluation du risque représentent d'autres dangers pour le droit à la liberté et à la sécurité inscrit dans le droit international relatif aux droits humains. Dans un avis publié sur une proposition d'accord entre l'UE et le Canada au sujet du transfert et du traitement des données des dossiers passagers (« PNR »), la Cour de justice de l'Union européenne a averti que le traitement automatisé des données PNR pouvait aboutir à des décisions contraignantes lourdes de conséquences pour les droits d'une personne, sans aucune preuve du caractère dangereux de la personne en question pour la sécurité publique[69]. Aux États-Unis, la modification d'un outil d'évaluation du risque afin qu'il recommande automatiquement la détention des immigrant·e·s[70] est un autre exemple de la manière dont ces outils peuvent faciliter les arrestations et les détentions arbitraires, pourtant interdites par le droit international relatif aux droits humains. Dans ce cas, le logiciel utilisé pour évaluer le dossier d'une personne a été modifié afin d'éliminer la possibilité de la libération, provoquant une augmentation du nombre de détentions injustifiées[71].

Compte tenu des risques qu'ils comportent pour les droits à la non-discrimination, au respect de la vie privée et à la protection des données, ainsi que pour le droit à la liberté et la sécurité, Amnesty International soutient que les systèmes automatisés de profilage et d'évaluation du risque dans le contexte de la gestion des migrations, de l'asile et du contrôle des frontières doivent absolument être interdits[72].

ENCADRÉ 5 : LE RESPECT DE LA VIE PRIVÉE

Les technologies mettant en œuvre l'intelligence artificielle reposent sur la collecte et le traitement de masses de données. Leur adoption de plus en plus fréquente favorise l'expansion des infrastructures de collecte de données, qui demande à son tour un élargissement des capacités de surveillance.

Aux termes du droit international, les États doivent prouver qu'une immixtion dans le droit au respect de la vie privée constitue un moyen légal, nécessaire et proportionné d'atteindre un objectif légitime, ce qui implique que la nature et l'ampleur de l'immixtion doivent être en adéquation avec la raison de l'atteinte au droit à la vie privée. Ils doivent aussi veiller à recourir aux moyens les moins intrusifs possible.

La surveillance, la collecte, le stockage, l'analyse ou toute autre utilisation à grande échelle des données, ainsi que la collecte de données sensibles à caractère personnel et de données biométriques, qui ne reposent pas sur la base de soupçons raisonnables et individualisés d'infraction équivalent à une surveillance de masse non ciblée. Amnesty International estime que la surveillance de masse non ciblée ne constitue jamais une immixtion proportionnée dans le droit à la vie privée et les droits aux libertés d'expression, d'association et de réunion pacifique. En outre, les systèmes de reconnaissance faciale sont entraînés grâce à des algorithmes de reconnaissance d'image qui, pour améliorer leur « taux de réussite », utilisent en guise de données entrantes de vastes quantités d'images de visages collectées à l'insu et sans le consentement des personnes concernées. Ces systèmes ne pouvant fonctionner sans

68. Amnesty International, "Open Letter to the Rapporteurs on the EU Artificial Intelligence Regulation (AI ACT) to ensure Protection of Rights of Migrants, Asylum Seekers and Refugees" (op. cit.).
69. Cour de justice de l'Union européenne, affaire C-817/19, 21 juin 2022, https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105fr.pdf
70. Daniel Oberhaus, "ICE Modified its 'Risk Assessment' Software so it Automatically Recommends Detention", Vice, 26 juin 2018, https://www.vice.com/en/article/evk3kw/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention
71. Mica Rosenberg et Reade Levinson, "Trump's catch-and-detain policy snares many who have long called U.S. home", Reuters, 20 juin 2018, https://www.reuters.com/investigates/special-report/usa-immigration-court
72. Amnesty International, "Open Letter to the Rapporteurs on the EU Artificial Intelligence Regulation (AI ACT) to ensure Protection of Rights of Migrants, Asylum Seekers and Refugees" (op. cit.).

bases de données biométriques de référence, ils sont incompatibles par nature avec le droit au respect de la vie privée – comme évoqué plus haut.

3.6 ÉTUDE DE CAS : L'APPLICATION POUR TÉLÉPHONE PORTABLE « CBP ONE »

En mai 2023, un nouveau règlement fédéral s'appliquant aux personnes migrantes est entré en vigueur aux États-Unis. En application de ce texte, lorsque des personnes demandeuses d'asile et leurs familles arrivent à la frontière méridionale du pays sans autorisation préalable, elles sont tenues d'utiliser une application pour téléphone portable, CBP One, pour prendre rendez-vous afin de se présenter à un point d'entrée dans le pays[73]. CBP One était déjà utilisée avant mai 2023, mais le nouveau règlement l'a rendue obligatoire. L'application impose aux demandeurs et demandeuses d'asile d'être physiquement présents à des endroits spécifiques du Mexique pour demander un rendez-vous afin de se présenter à un point d'entrée. Elle les oblige également à fournir des données à caractère personnel, notamment une photographie de leur visage à des fins de reconnaissance faciale.

Avant le déploiement généralisé de CBP One, en mai 2023, Amnesty International et d'autres organisations avaient déjà reçu des informations attestant de nombreux problèmes, extrêmement préoccupants, rencontrés avec CBP One. Il n'était pas rare, par exemple, que l'application cesse brusquement de fonctionner ; par ailleurs, les lacunes de la reconnaissance faciale lui faisaient porter préjudice de manière disproportionnée aux personnes racisées, notamment haïtiennes, cubaines, nicaraguayennes et vénézuéliennes[74]. Les demandeurs et demandeuses d'asile sont obligés d'installer l'application sur leur dispositif mobile, ce qui permet à l'office des douanes et de la protection des frontières de recueillir des données sur leur emplacement en localisant leur téléphone.

Les écueils toujours importants concernent les difficultés à consulter l'application – en raison des langues disponibles ou de problèmes d'illettrisme –, l'accès insuffisant à des téléphones portables ou à Internet et l'absence de créneaux disponibles pour les rendez-vous. L'une des conséquences les plus graves est que la pénurie de rendez-vous disponibles implique que de nombreuses personnes demandeuses d'asile se retrouvent bloquées et attendent pendant des mois dans des régions du Mexique où elles sont exposées au risque de subir de graves atteintes aux droits humains, notamment des viols et des enlèvements, comme en informent des organisations[75]. Celles qui choisissent de franchir la frontière sans rendez-vous, afin d'échapper aux menaces qui pèsent sur leur sécurité tant qu'elles restent au Mexique, s'exposent à ne pas réunir les conditions jugées nécessaires pour déposer une demande d'asile et risquent plus encore d'être placées en détention au motif de leur statut migratoire[76].

L'utilisation obligatoire et exclusive de CBP One porte préjudice aux droits des personnes qui arrivent à la frontière méridionale des États-Unis pour chercher asile et risque de violer le principe de « non-refoulement », norme inscrite dans le droit international coutumier. Compte tenu du recours à la reconnaissance faciale dans CBP One, qui semble être répertoriée dans plusieurs « bases de données dérogatoires », il existe un risque de surveillance de masse à l'égard de groupes de populations précaires en déplacement, rendue possible par les technologies GPS et la collecte numérique de données sur les demandeurs et demandeuses d'asile avant leur entrée aux États-Unis. De ce fait, l'application soulève de graves préoccupations au sujet du respect de la vie privée et du droit à la non-discrimination[77].

---

73. Services de la citoyenneté et de l'immigration des États-Unis, Proposed Rule, Circumvention of Lawful Pathways, USCIS-2022-0016-0001, 23 février 2023, https://www.regulations.gov/document/USCIS-2022-0016-0001
74. Melissa del Bosque, "Facial recognition bias frustrates Black asylum applicants to US, advocates say", The Guardian, 8 février 2023, https://www.theguardian.com/us-news/2023/feb/08/us-immigration-cbp-one-app-facial-recognition-bias ; Amnesty International, Mandatory Use of CBP One Application Violates the Right to Seek Asylum (op. cit.).
75. Christina Asencio, "Asylum ban strands asylum seekers and migrants in Mexico and returns them to danger", 28 novembre 2023, https://humanrightsfirst.org/library/asylum-ban-strands-asylum-seekers-and-migrants-in-mexico-and-returns-them-to-danger
76. Stephanie Leutert et Caitlyn Yates, *Asylum Processing at the U.S.-Mexico Border: February 2023*, 28 février 2023, https://www.strausscenter.org/publications/asylum-processing-at-the-u-s-mexico-border-february-2023, p. 3 ; Amnesty International, "Amnesty International statement for hearing on "Examining the Human Rights and Legal Implications of DHS's 'Remain in Mexico' Policy", 18 novembre 2019, https://www.amnestyusa.org/updates/amnesty-international-statement-for-hearing-on-examining-the-human-rights-and-legal-implications-of-dhss-remain-in-mexico-policy
77. E. Tendayi Achiume, rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Rapport : *La discrimination raciale et la xénophobie et l'utilisation des technologies numériques dans le contrôle des frontières et de l'immigration* (op. cit.), § 47.

3.7 ÉTUDE DE CAS : LA LÉGISLATION SUR L'INTELLIGENCE ARTIFICIELLE DE L'UNION EUROPÉENNE

L'utilisation de systèmes d'intelligence artificielle est déjà généralisée en Europe, où les drones, les « détecteurs de mensonges », la biométrie, la reconnaissance faciale et d'autres technologies souvent expérimentales sont autorisés, ce qui crée un vaste réseau de surveillance de masse aux frontières de l'Europe, à l'intérieur de celles-ci et parfois au-delà[78]. Ces nouveaux outils technologiques sont « susceptible[s] d'aggraver le racisme, la discrimination raciale, la xénophobie et d'autres formes d'exclusion[79]. » En décembre 2023, le Parlement européen, les États membres et la Commission européenne sont parvenus à un accord sur une législation relative à l'utilisation de l'intelligence artificielle, consacré dans le règlement établissant des règles harmonisées concernant l'intelligence artificielle (« législation sur l'intelligence artificielle[80] »). Bien que le texte définitif n'ait pas encore été adopté, ce règlement représente une grande avancée à ce jour, car il offre la possibilité d'améliorer les protections des personnes auxquelles l'intelligence artificielle porte préjudice. Néanmoins, la société civile et d'autres acteurs ont manifesté leurs inquiétudes au sujet d'aspects de la proposition de règlement ayant trait à l'utilisation de dispositifs d'intelligence artificielle dans le contexte des migrations[81], car ce texte ne protège pas suffisamment les personnes en déplacement et autres groupes marginalisés contre le racisme, la discrimination et tout un éventail d'autres violations des droits humains[82]. Dans certains cas, la législation sur l'¡ntelligence artificielle risque non seulement de ne pas résoudre les problèmes liés aux droits humains dans le contexte des migrations, mais même de les favoriser, par exemple en fournissant un fondement juridique aux systèmes de surveillance de masse et de surveillance discriminatoire, comme les technologies de reconnaissance faciale et de reconnaissance des émotions employées pour viser de manière disproportionnée les personnes en déplacement, entre autres populations marginalisées[83].

La législation sur l'intelligence artificielle ne suffit pas à prévenir les préjudices et les risques possibles que ces technologies impliquent. Actuellement, elle n'interdit même pas, purement et simplement, les plus dangereuses d'entre elles, comme les systèmes d'analyse prévisionnelle utilisés à des fins de prévention, de restriction et d'interdiction des migrations ou les « détecteurs de mensonges » pseudo-scientifiques, notamment les polygraphes reposant sur l'intelligence artificielle[84]. Par ailleurs, les États membres de l'UE font pression pour inscrire des exceptions généralisées dans la législation sur l'intelligence artificielle, à l'usage des autorités employant l'intelligence artificielle à des fins de « sécurité nationale ». Si elles étaient adoptées, ces exceptions représenteraient un risque d'utilisation abusive de l'intelligence artificielle à l'encontre des personnes en déplacement. Elles permettraient également, au titre de la sécurité nationale, de soustraire les autorités en charge de l'application des lois, du contrôle des migrations et de la sécurité

78. Access Now, European Digital Rights (EDRi), Migration and Technology Monitor, la plateforme pour la coopération internationale en faveur des personnes migrantes sans papiers (PICUM) et Statewatch, *Uses of AI in migration and border control: A fundamental rights approach to the Artificial Intelligence Act,* 2022, https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf
79. E. Tendayi Achiume, rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, Rapport : *La discrimination raciale et la xénophobie et l'utilisation des technologies numériques dans le contrôle des frontières et de l'immigration* (op. cit.), § 24.
80. Commission européenne, *Proposition de Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union,* 21 avril 2021, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021PC0206 ; Amnesty International, « Union européenne. La loi sur l'IA doit interdire les technologies dangereuses basées sur l'IA », 28 septembre 2023, https://www.amnesty.org/fr/latest/news/2023/09/eu-ai-act-must-ban-dangerous-ai-powered-technologies-in-historic-law/ ; Thierry Breton, publication sur Twitter : "Historic! The EU becomes the very first continent to set clear rules for the use of AI. The #AIAct is much more than a rulebook – it's a launch pad for EU startups and researchers to lead the global AI race. The best is yet to come!", 8 décembre 2023, https://twitter.com/ThierryBreton/status/1733256557448630344
81. Voir par exemple le site Internet #Protéger au lieu de surveiller (#Protect not Surveil) : https://protectnotsurveil.eu/index_fr.html
82. Amnesty International, "The EU must respect human rights of migrants in the AI Act", 26 avril 2023, https://www.amnesty.eu/news/the-eu-must-respect-human-rights-of-migrants-in-the-ai-act
83. Amnesty International, "AI Act must protect all people, regardless of migration status", 6 décembre 2022, https://www.amnesty.eu/news/eu-ai-act-must-protect-all-people-regardless-of-migration-status ; Amnesty International, « UE. La décision du Bloc de ne pas interdire la surveillance publique de masse dans la loi sur l'IA crée un précédent mondial désastreux », 9 décembre 2023, https://www.amnesty.org/fr/latest/news/2023/12/eu-blocs-decision-to-not-ban-public-mass-surveillance-in-ai-act-sets-a-devastating-globalprecedent/ ; Amnesty International, "Council risks failing human rights in the AI Act", 29 novembre 2023, https://www.amnesty.eu/news/council-risks-failing-human-rights-in-the-ai-act/
84. EDRi, *The EU's Artificial Intelligence Act: Civil society amendments*, 3 mai 2022, https://edri.org/our-work/the-eus-artificial-intelligence-act-civil-society-amendments
85. Amnesty International, "EU policymakers : regulate police technology", 21 septembre 2023, https://www.amnesty.eu/news/eu-policymakers-regulate-police-technology

nationale aux mesures d'obligation de rendre des comptes et de transparence publique, en ce qui concerne leur utilisation des systèmes d'intelligence artificielle.

En outre, la législation sur l'intelligence artificielle ne résout pas le problème de l'exportation des dispositifs d'intelligence artificielle à partir de l'Europe, ce qui signifie que des technologies illégales, notamment de surveillance, interdites au sein de l'UE pourraient être exportées vers des pays voisins de l'UE afin d'arrêter les personnes en déplacement avant qu'elles atteignent les frontières européennes[85]. La coalition transdisciplinaire #Protéger au lieu de Surveiller (#Protectnotsurveil[86]), qui regroupe Amnesty International et d'autres partenaires, demande que la législation sur l'intelligence artificielle de l'UE réglemente tous les systèmes d'intelligence artificielle à haut risque déployés dans le contexte des migrations, interdise les systèmes d'intelligence artificielle qui représentent un risque inacceptable et garantisse que son application s'étende aux énormes bases de données migratoires de l'UE[87].

86. Voir https://protectnotsurveil.eu/index_fr.html
87. Voir #Protéger au lieu de surveiller, « La loi sur l'IA doit être mise à jour de quatre manières principales: » https://protectnotsurveil.eu/index_fr.html

4. CONCLUSIONS ET RECOMMANDATIONS

Les technologies sont devenues un outil dangereux et omniprésent dans l'orientation et l'exécution des politiques publiques de gestion de l'asile et des migrations. Susceptibles de créer et d'entretenir un racisme, une discrimination et une oppression systémiques, elles sont sans cesse utilisées au profit de programmes, discours et structures racistes et xénophobes. Lorsque les États veulent implanter un programme en contradiction avec leurs obligations en matière de droits humains à l'égard des personnes réfugiées et migrantes, ces technologies risquent de favoriser des violations des droits humains, voire de les aggraver. Les technologies utilisées pour la gestion de l'asile et des migrations peuvent aussi poser problème en soi, car les dispositifs en question sont susceptibles de subir des biais et de rencontrer des erreurs ou car ils aboutissent à la collecte, au stockage et à l'utilisation d'informations qui menacent le droit au respect de la vie privée, la non-discrimination et d'autres libertés fondamentales.

Amnesty International formule les recommandations suivantes au sujet de l'utilisation de technologies numériques impliquant un grand volume de données dans les systèmes de gestion de l'asile et des migrations :

LES ÉTATS DEVRAIENT :

- s'attaquer au racisme, à la xénophobie et à la discrimination systémiques qui ont toujours orienté et qui orientent de plus en plus la gestion des migrations, les systèmes d'asile, la surveillance des frontières et le contrôle de l'immigration ;
- réaliser des études d'impact sur les droits humains et sur la protection des données avant de déployer des technologies numériques et pendant tout leur cycle de vie ;
- avant de déployer tout système, évaluer et définir la nécessité et la proportionnalité de la mesure, car toute technologie ou mesure de surveillance adoptée doit être légale, nécessaire et proportionnée, en même temps qu'elle doit servir un but légitime aux termes du droit international relatif aux droits humains ;
- ne pas éluder le risque que ces outils facilitent la discrimination et d'autres atteintes aux droits humains à l'égard des minorités ethniques, des personnes vivant dans la pauvreté et d'autres populations marginalisées ;
- intégrer des garanties contre les atteintes aux droits humains dans toute technologie utilisée ;
- donner à chacun·e la possibilité de connaître et de contester toute mesure prise pour recueillir, agréger, conserver et utiliser ses données personnelles, ainsi que d'accorder ou de retirer son consentement à celle-ci ;
- obliger les entreprises participant à la mise au point et la fourniture de technologies dans le contexte de l'enregistrement des personnes réfugiées et de la surveillance des frontières, notamment les systèmes de mégadonnées, d'intelligence artificielle et de biométrie, à exercer la diligence requise 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 OCDE sur le devoir de diligence ;

- tenir les entreprises technologiques pour responsables des préjudices qu'elles ont causés aux droits humains ou auxquels elles ont contribué, notamment par non-respect de leur obligation de diligence en la matière ;
- protéger les données des particuliers, notamment en respectant le principe de limitation de la quantité de données à caractère personnel collectées et en garantissant la sécurité de celles-ci ainsi que de tous les appareils, applications, réseaux ou services qui participent à la collecte, à la transmission, au traitement et au stockage de ces données ;
- veiller à ce que les personnes ayant fait l'objet d'atteintes aux droits humains provoquées par l'utilisation abusive de technologies aient accès à des recours utiles ;
- adopter des lois interdisant l'usage, l'élaboration, la production, la vente et l'exportation de technologies de reconnaissance biométrique à distance destinées à des missions de surveillance de masse, ainsi que de technologies biométriques ou de reconnaissance faciale à distance utilisées pour identifier les personnes sur leur propre territoire ;
- interdire les systèmes automatisés d'évaluation des risques et de profilage dans le cadre de la gestion des migrations, de l'asile et des contrôles aux frontières ;
- interdire toute utilisation de technologies prédictives qui menacent à tort le droit d'asile ;
- interdire l'utilisation d'outils de reconnaissance des émotions basés sur l'intelligence artificielle, en particulier dans le contexte de la gestion des migrations, de l'asile et des contrôles aux frontières.

LES ORGANISATIONS ET LES FOURNISSEURS DE SERVICES DÉPLOYANT DES TECHNOLOGIES NUMÉRIQUES DOIVENT :

- réaliser des études d'impact obligatoires sur la diligence requise en matière de droits humains et sur la protection des données avant de déployer des technologies numériques et pendant tout leur cycle de vie ;
- avant de déployer tout système, évaluer et définir la nécessité et la proportionnalité de la mesure, car toute technologie ou mesure de surveillance adoptée doit être légale, nécessaire et proportionnée, en même temps qu'elle doit servir un but légitime aux termes du droit international relatif aux droits humains ;
- ne pas éluder le risque que ces outils facilitent la discrimination et d'autres atteintes aux droits humains à l'égard des personnes et des populations racisées, des personnes vivant dans la pauvreté et d'autres populations marginalisées ;
- explorer toute solution alternative non intrusive qui puisse répondre aux besoins identifiés par les fournisseurs de services sans nuire inutilement aux droits au respect de la vie privée, à l'égalité et à la non-discrimination, ainsi qu'au droit d'être libre de toute surveillance ;
- intégrer des garanties contre les atteintes aux droits humains dans toute technologie utilisée ;
- donner à chacun·e la possibilité de connaître et de contester toute mesure prise pour recueillir, agréger, conserver et utiliser ses données personnelles, ainsi que d'accorder ou de retirer son consentement à celle-ci.

AMNESTY INTERNATIONAL EST UN MOUVEMENT MONDIAL DE DÉFENSE DES DROITS HUMAINS. LORSQU'UNE INJUSTICE TOUCHE UNE PERSONNE, NOUS SOMMES TOUS ET TOUTES CONCERNÉ·E·S.

NOUS CONTACTER

info@amnesty.org

+44 (0)20 7413 5500

PRENDRE PART À LA CONVERSATION

www.facebook.com/AmnestyGlobal

@amnesty

INTRODUCTION À LA DÉFENSE DES DROITS DES RÉFUGIÉ·E·S ET DES MIGRANT·E·S À L'ÈRE NUMÉRIQUE

Cet exposé est une introduction au déploiement rapide et généralisé des technologies numériques dans les systèmes de gestion de l'asile et des migrations à travers le monde, notamment aux États-Unis, au Royaume-Uni et au sein de l'Union européenne.

Intitulé ***Défense des droits des réfugié·e·s et des migrant·e·s à l'ère numérique***, il met en évidence certaines évolutions majeures des technologies numériques dans les systèmes de gestion de l'asile et des migrations, en particulier les systèmes qui traitent de grandes quantités de données, ainsi que les questionnements en termes de droits humains découlant de leur utilisation. Le but de cet exposé introductif est de renforcer notre compréhension collective de ces nouvelles technologies, dans l'espoir d'étayer les efforts généraux de plaidoyer contre leurs effets néfastes.

INDEX : POL 40/7654/2024
JANVIER 2024
LANGUE : FRANÇAIS

amnesty.org

AMNESTY INTERNATIONAL