Nations Unies A/75/590

Assemblée générale

Distr. générale
10 novembre 2020
Français
Original : anglais

Soixante-quinzième session
Point 70 b) de l'ordre du jour
Élimination du racisme, de la discrimination raciale, de la xénophobie et l'intolérance qui y est associée : application intégrale et suivi de la Déclaration et du Programme d'action de Durban

Formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée*

Note du Secrétaire général

Le Secrétariat a l'honneur de transmettre à l'Assemblée générale le rapport de la Rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, E. Tendayi Achiume, établi en application de la résolution 74/137 de l'Assemblée générale.

* Rapport soumis après la date limite du fait de circonstances indépendantes de la volonté de l'auteure.

Rapport de la Rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée

Résumé

Dans le cadre de la gestion des frontières et de l'immigration, les gouvernements et les institutions des Nations Unies développent et utilisent les nouvelles technologies numériques de manière particulièrement expérimentale, dangereuse et discriminatoire. Ce faisant, ils portent atteinte aux droits humains des réfugiés, des migrants, des apatrides et d'autres personnes et recueillent toute une masse de données dans des conditions qui dépouillent ces personnes de leur humanité et de leur dignité.

Le présent rapport met en lumière la manière dont les technologies numériques servent les idéologies xénophobes et raciales discriminatoires, qui sont désormais si répandues, en partie parce que les réfugiés et les migrants sont perçus comme une menace intrinsèque pour la sécurité nationale. Parfois, la discrimination et l'exclusion sont le produit non d'une intention délibérée, mais de la volonté de maximiser l'efficacité bureaucratique et l'action humanitaire, au détriment des garanties nécessaires en matière de droits de la personne. Le rapport dénonce également les vastes profits économiques découlant des activités de sécurisation et de numérisation des frontières, qui constituent une grosse part du problème.

Table des matières

I. Introduction

1. Le présent rapport approfondit la réflexion commencée par la Rapporteuse spéciale dans son dernier rapport au Conseil des droits de l'homme intitulé « Discrimination raciale et nouvelles technologies numériques : analyse sous l'angle des droits de l'homme »[1]. La Rapporteuse spéciale y recommandait d'adopter pour les nouvelles technologies numériques une approche de la gouvernance en matière de droits humains qui soit fondée sur l'égalité, en mettant l'accent sur la discrimination raciale résultant de la conception et de l'utilisation de ces technologies. Elle exhortait les acteurs étatiques et non étatiques à aller plus loin que les stratégies faisant abstraction de la couleur de peau ou de la race, qui ignorent l'impact racial et ethnique des nouvelles technologies numériques, et à s'attaquer directement aux formes croisées de discrimination qui résultent de l'adoption généralisée de ces technologies et sont exacerbées par elles. Le rapport s'intéressait avant tout aux personnes faisant l'objet de discrimination fondée essentiellement sur la race ou l'ethnicité (y compris l'appartenance à un peuple autochtone) et appelait l'attention sur l'incidence de l'appartenance sexuelle, de l'appartenance religieuse ou de la situation de handicap. Le présent rapport à l'Assemblée générale apporte une nuance supplémentaire car il est axé sur les conséquences xénophobes et discriminatoires que les nouvelles technologies numériques ont sur les migrants, les apatrides, les réfugiés et autres non-ressortissants ainsi que sur les peuples nomades et autres groupes pour lesquels les traditions migratoires sont essentielles. Le terme « réfugié » comprend le demandeur d'asile, qui répond à la définition de réfugié mais dont le statut de réfugié n'a pas encore été officiellement reconnu par un État.

2. Les nouvelles technologies numériques sont désormais omniprésentes dans tous les aspects de la société, mais dans la gestion des frontières et de l'immigration, elles posent des problèmes particuliers pour au moins deux raisons. Dans la plupart des dispositifs de gouvernance nationaux, si ce n'est dans tous :

a) Les non-ressortissants, les apatrides et les groupes apparentés ont moins de droits et de protection juridique contre l'abus de pouvoir par l'État et peuvent être la cible de formes uniques de violence xénophobe de la part d'acteurs privés ;

b) En matière de gestion des frontières et de l'immigration, l'exécutif et les autres branches du gouvernement ont de grands pouvoirs discrétionnaires, qui échappent aux contraintes de fond et de procédure classiques imposées par la Constitution ou d'autres instruments pour la protection des citoyens.

3. Comme il est indiqué dans le présent rapport, en matière de gestion des frontières et de l'immigration, les gouvernements et les acteurs non étatiques développent et utilisent les nouvelles technologies numériques de manière particulièrement expérimentale, dangereuse et discriminatoire. Ce faisant, ils portent atteinte aux droits humains des réfugiés, des migrants, des apatrides et d'autres personnes et recueillent toute une masse de données dans des conditions qui dépouillent ces personnes de leur humanité et de leur dignité. Le présent rapport s'intéresse à des innovations technologiques relativement récentes, mais nombre d'entre elles sont des avatars de technologies déjà utilisées à l'époque coloniale pour une gestion racialisée de la population, notamment par les contrôles migratoires. Non seulement la technologie n'est pas neutre, mais elle est conçue et utilisée de telle façon qu'elle renforce généralement les tendances sociales, politiques et économiques dominantes. Comme il est indiqué dans des rapports précédents, la résurgence du populisme ethnonationaliste à l'échelle mondiale a eu de graves conséquences xénophobes et discriminatoires sur le plan racial pour les réfugiés, les migrants et les

[1] A/HRC/44/57.

apatrides[2]. Le présent rapport met en lumière la manière dont les technologies numériques servent les idéologies xénophobes et raciales discriminatoires, qui sont désormais si répandues, en partie parce que les réfugiés et les migrants sont généralement perçus comme une menace intrinsèque pour la sécurité nationale. Parfois, la discrimination et l'exclusion sont le produit non d'une intention délibérée, mais de la volonté de maximiser l'efficacité bureaucratique et l'action humanitaire, au détriment des garanties nécessaires en matière de droits de la personne. Le rapport montre également que la sécurisation des frontières et les profits économiques massifs qui en découlent constituent une part importante du problème.

4. Les droits des réfugiés, des migrants et des apatrides sont violés, comme le mentionne le présent rapport, en raison de leur nationalité, de leur race, de leur ethnicité, de leur religion ou pour d'autres motifs inacceptables. On ne saurait tolérer ces violations sous prétexte qu'elles concerneraient des non-ressortissants. À cet égard, la Rapporteuse spéciale renvoie à son rapport précédent sur la discrimination raciale fondée sur la citoyenneté, la nationalité et le statut d'immigration, dans lequel elle dit bien que ces violations naissent des tendances discriminatoires dans l'application du droit international des droits de l'homme[3].

5. La Rapporteuse spéciale recommande que le présent rapport, qui reprend de nombreux points du rapport qu'elle a établi à l'intention du Conseil des droits de l'homme[4] soit lu conjointement avec celui-ci. Elle y explique comment les nouvelles technologies numériques sont à l'origine de la discrimination raciale et met la lumière sur les forces économiques, politiques et sociétales qui favorisent l'utilisation discriminatoire de ces technologies, d'où son intérêt particulier. Elle rappelle que même si les nouvelles technologies numériques sont généralement perçues comme neutres et objectives dans leur application, la race, l'appartenance ethnique, la nationalité et le statut de citoyen sont des facteurs déterminants pour la jouissance des droits humains dans tous les domaines où ces technologies sont désormais omniprésentes. Les États ont l'obligation de prévenir cette discrimination raciale, de la combattre et d'y remédier, de même que les acteurs privés, tels que les entreprises. Dans le cadre de la gestion des frontières et de l'immigration (comme dans d'autres contextes), protéger les droits humains peut signifier interdire ou supprimer purement et simplement des technologies s'il est impossible d'en contrôler ou d'en atténuer les effets.

6. Pour établir le présent rapport, la Rapporteuse spéciale s'est appuyée sur la précieuse contribution des réunions de groupes d'experts organisées par la Promise Institute for Human Rights at UCLA School of Law, le UCLA Center for Critical Internet Inquiry, l'Institute on Statelessness and Inclusion et le Migration and Technology Monitor ; des entretiens avec des chercheurs, y compris des apatrides, des migrants et des réfugiés ; et des communications de plusieurs parties prenantes reçues à la suite d'un appel au public. Les soumissions non confidentielles seront disponibles sur la page web des procédures spéciales.

II. Montée des frontières numériques

7. Des passeports aux murs physiques, qui n'en sont que des éléments parmi d'autres, la technologie a toujours fait partie de la gestion des frontières et de l'immigration. Le présent rapport s'intéresse plus particulièrement au rôle de plus en plus important des technologies numériques dans ce domaine, qui est tel que certains

[2] Voir, par exemple, A/73/312.
[3] A/HRC/38/52.
[4] A/HRC/44/57.

commentateurs parlent à juste titre de la montée des « frontières numériques »[5], qui, ici, désignent les frontières dont l'infrastructure et les méthodes qui y sont appliquées reposent de plus en plus sur l'apprentissage machine, les systèmes automatisés de prise de décision algorithmique, l'analyse prédictive et les technologies numériques connexes. Ces technologies sont intégrées aux documents d'identification, aux systèmes de reconnaissance faciale, aux capteurs au sol, aux drones de vidéosurveillance aérienne, aux bases de données biométriques, à la décision en matière d'asile et à de nombreux autres aspects de la gestion des frontières et de l'immigration.

8. D'une manière générale, les technologies numériques liées à la gestion des frontières renforcent des dispositifs de contrôle parallèles qui distinguent la mobilité et la migration de différents groupes en fonction de la nationalité et de la classe, par exemple. Les contrôles automatisés aux frontières en sont une illustration. Les portes « eGates » ont été mentionnées dans l'une des communications. Ces portes électroniques installées aux points d'entrée en Irlande (aéroport de Dublin, par exemple), permettent aux détenteurs de passeports électroniques de l'Union européenne ou de l'espace économique européen ainsi que de la Suisse de passer les contrôles de l'immigration en « libre-service »[6]. Il est précisé dans la communication que « seules certaines nationalités peuvent choisir la formule "libre-service" ; les pays concernés sont riches et blancs (à l'exception du Japon) [...] » Les non-ressortissants de l'Union européenne ou de l'espace économique européen ou de la Suisse qui voyagent d'un aéroport ou d'un port situé hors de l'Irlande doivent se présenter à un agent de l'immigration à leur arrivée.

9. L'une des particularités de la frontière numérique est l'utilisation étendue de la biométrie ou la « reconnaissance automatisée des individus sur la base de leurs caractéristiques biologiques et comportementales [...] »[7]. Les données biométriques comprennent les empreintes digitales, le balayage de la rétine et la reconnaissance faciale, ainsi que des éléments moins connus tels que la texture des veines et des vaisseaux sanguins, la forme des oreilles ou la démarche. La biométrie est utilisée pour établir, enregistrer et vérifier l'identité des migrants et des réfugiés. L'ONU, par exemple, a recueilli les données biométriques de plus de 8 millions de personnes, dont la plupart fuient les conflits ou ont besoin d'une aide humanitaire[8]. Des chercheurs se sont penchés sur les origines racialisées[9] des technologies biométriques, ainsi que sur l'utilisation discriminatoire qui est en faite de nos jours sur la base de la race, de l'ethnicité et de l'appartenance sexuelle[10]. Dans un rapport récent sur les technologies de reconnaissance faciale utilisées aux points de passage des frontières (aéroports, par exemple), il est dit que même pour les meilleurs algorithmes, il y a vingt fois plus d'erreurs dans la reconnaissance des femmes noires que des hommes blancs, et pourtant, ces technologies sont de plus en plus utilisées au niveau mondial[11]. Le rapport précise que « lorsque la reconnaissance faciale est l'une des méthodes de contrôle aux frontières, des voyageurs sont écartés sur la base de leur race, de leur

---

[5] Voir, par exemple, Dennis Broeders, « The new digital borders of Europe: EU databases and the surveillance of irregular migrants », International Sociology, vol. 22, No. 1 (janvier 2007), p. 71 à 92.

[6] Communication reçue du Immigrant Council of Ireland.

[7] Voir www.biometricsinstitute.org/what-is-biometrics/.

[8] Il est notoirement difficile d'assurer le suivi de ces masses énormes de données, qui peuvent inclure d'anciennes données recyclées avec de nouvelles données biométriques. Voir, par exemple, http://humanitarian-congress-berlin.org/2018/.

[9] Voir, par exemple, Simone Browne, Dark Matters: On the Surveillance of Blackness (Duke University Press 2015).

[10] Voir A/HRC/44/57.

[11] Tamir Israel, Facial Recognition at a Crossroads: Transformation at our Borders & Beyond (septembre 2020).

sexe et d'autres caractéristiques démographiques (comme le pays d'origine) ». Souvent, ce traitement différencié a pour résultat de perpétuer les stéréotypes négatifs voire d'entraîner la discrimination, qui, pour les demandeurs d'asile, pourrait conduire au refoulement.

10. Il ressort clairement des exemples ci-dessous que la collecte des données biométriques faite par les gouvernements ou les organismes humanitaires auprès des réfugiés et des migrants a donné lieu à de graves violations des droits humains, quels que soient les motifs bureaucratiques ou humanitaires avancés. En outre, on ne sait pas très bien ce qu'il advient de ces données biométriques ni si les groupes concernés y ont accès. On a reproché au Programme alimentaire mondial (PAM), par exemple, de s'être associé à la société d'exploration de données Palantir Technologies pour un contrat de 45 millions de dollars, et de compromettre ainsi le traitement, la sécurité et la chaîne de responsabilité des données de 92 millions de bénéficiaires qu'il gérait[12]. Les sociétés privées comme Palantir sont les grands fournisseurs de technologies entrant dans les programmes de détention et d'expulsion exploités par le service de l'immigration et des douanes (ICE) et le Département américain de la sécurité du territoire[13] ; on serait donc en droit de se poser des questions sur la complicité de ces entreprises dans les violations des droits humains associées à ces programmes. On ne sait pas encore quel dispositif d'application du principe de responsabilité sera mis en place pour le partage des données dans le cadre du partenariat entre le PAM et Palantir ni si les personnes concernées auront la possibilité de refuser leur consentement[14]. La collecte de données n'est pas un exercice apolitique, surtout lorsque ce sont les puissants du monde du Nord qui collectent des informations sur des populations vulnérables, en l'absence de toute règle de surveillance et de responsabilisation[15]. La collecte de plus en plus effrénée de données auprès des populations migrantes fait l'objet de critiques car elle pourrait donner lieu à d'importantes violations de la vie privée et des droits humains[16].

11. L'histoire fournit de nombreux exemples de l'utilisation discriminatoire voire mortelle de la collecte de données auprès de groupes marginalisés. L'Allemagne nazie a recueilli stratégiquement de grandes quantités de données sur les communautés juives pour faciliter l'Holocauste, en grande partie en partenariat avec une société privée : IBM[17]. D'autres génocides se sont également fondés sur la surveillance systématique de groupes, comme les registres des Tutsis basés sur les cartes d'identité ethniques, qui ont facilité l'ampleur du génocide rwandais en 1994[18]. Après le 11 septembre, les États-Unis ont expérimenté diverses méthodes de collecte de données sur les populations marginalisées, au moyen du système d'enregistrement des entrées et des sorties mis en place par le Département de la sécurité du territoire, qui a permis de recueillir des photographies, des données biométriques et même des entretiens à la première personne auprès de plus de 84 000 personnes qui avaient été

---

[12] Voir www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp.

[13] Voir www.technologyreview.com/2018/10/22/139639/amazon-is-the-invisible-backbone-behind-ices-immigration-crackdown/.

[14] Voir www.devex.com/news/opinion-the-wfp-and-palantir-controversy-should-be-a-wake-up-call-for-humanitarian-community-94307.

[15] Dragana Kaurin, Data protection and digital agency for refugees, World Refugee Council research paper No. 12 (mai 2019), disponible à l'adresse suivante : www.cigionline.org/publications/data-protection-and-digital-agency-refugees.

[16] Voir www.chathamhouse.org/2018/03/beware-notion-better-data-lead-better-outcomes-refugees-and-migrants.

[17] Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation* (Dialogue Press, 2012).

[18] Voir www.theengineroom.org/dangerous-data-the-role-of-data-collection-in-genocides/.

repérées et dont la plupart provenaient de pays arabes[19]. Dans tous ces exemples, différents acteurs, y compris des gouvernements, ont profité de l'idée que l'on se faisait de la neutralité ou du caractère inoffensif et nécessaire de la collecte de données auprès de groupes marginalisés pour ensuite appliquer des mesures discriminatoires à leur encontre.

12. Les technologies autonomes sont également de plus en plus utilisées pour surveiller et sécuriser les espaces frontaliers. Par exemple, Frontex, l'Agence européenne de garde-frontières et de garde-côtes, a testé divers drones de type militaire en Méditerranée et en mer Égée pour surveiller et bloquer les navires de migrants et de réfugiés espérant atteindre les côtes européennes[20]. En octobre 2020, une enquête conjointe menée par Bellingcat, *Lighthouse Reports*, *Der Spiegel*, TV Asahi et *Report Mainz* a mis en cause Frontex dans le cadre de refoulements ou renvois forcés de réfugiés et de migrants aux frontières sans que leur situation particulière ait été examinée et sans qu'il leur soit possible de demander l'asile ou de faire appel[21]. Facilités par les technologies de surveillance, ces refoulements violent probablement les règles sur le non-refoulement imposées par le droit international. Dans une communication, il est dit qu'une nouvelle loi en Grèce permet à la police d'utiliser des drones pour surveiller l'immigration clandestine dans les régions frontalières, mais ne prévoit pas les garanties juridiques requises pour protéger les droits humains des personnes soumises à cette surveillance[22].

13. L'utilisation de technologies autonomes militaires ou quasi-militaires renforce le lien entre l'immigration, la sécurité nationale et la tendance croissante à la criminalisation des migrations et au recours à une taxonomie basée sur les risques afin de distinguer et signaler les cas[23]. Les États, en particulier ceux dont les frontières connaissent un grand afflux de réfugiés et de migrants, utilisent divers moyens pour décourager les personnes qui cherchent à demander légalement l'asile. Cette évolution des règles vers la criminalisation de l'asile et des migrations justifie l'utilisation de technologies de plus en plus rigides et intrusives, comme les drones et autres dispositifs de contrôle aux frontières (appareils de télédétection et tours fixes équipées de caméras infrarouges intégrées appelées « tours de surveillance autonomes »), servant à contrôler « l'environnement de risque » aux frontières[24]. Ces technologies peuvent donner des résultats drastiques. Les technologies intelligentes utilisées aux frontières sont présentées comme des solutions plus humaines que d'autres dispositifs, mais des études montrent qu'à la frontière entre les États-Unis et le Mexique, par exemple, ces technologies ont, en fait, causé plus de décès de migrants et obligé ceux-ci à changer d'itinéraires pour emprunter des zones plus dangereuses à travers le désert de l'Arizona[25]. Dans un ouvrage collectif, Samuel Chambers et autres ont constaté que les décès de migrants ont plus que doublé depuis

---

[19] Voir www.aclu.org/issues/immigrants-rights/immigrants-rights-and-detention/national-security-entry-exit-registration.

[20] Petra Molnar, « Technological testing grounds: migration management experiments and reflections from the ground up » (novembre 2020).

[21] Voir www.bellingcat.com/news/2020/10/23/frontex-at-fault-european-border-force-complicit-in-illegal-pushbacks et www.spiegel.de/international/europe/eu-border-agency-frontex-complicit-in-greek-refugee-pushback-campaign-a-4b6cba29-35a3-4d8c-a49f-a12daad450d7.

[22] Communication reçue de Homo Digitalis.

[23] Communication reçue de Dimitri Van Den Meerssche.

[24] Raluca Csernatoni, « Constructing the EU's high-tech borders: Frontex and dual-use drones for border management » *European Security*, vol. 27, No. 2 (2018), p. 175 à 200.

[25] Samuel Norton Chambers et autres, « Mortality, surveillance and the tertiary 'funnel effect' on the U.S.-Mexico border: a geospatial modeling of the geography of deterrence », *Journal of Borderland Studies* (2019).

l'introduction de ces nouvelles technologies[26], créant ainsi une « terre de tombes ouvertes »[27].

14. Le recours à ces technologies par les services chargés du contrôle aux frontières ne peut qu'augmenter compte tenu de la « militarisation par la technologie » des zones frontalières, et ce sans consultation publique appropriée, sans dispositif d'application du principe de responsabilité et sans mécanisme de contrôle[28]. Dans une communication, il est donné en exemple la zone démilitarisée de la péninsule coréenne, où la République de Corée a déployé des armes semi-autonomes, fixes et télécommandées[29]. Le Gouvernement de la République de Corée a déclaré qu'il n'avait pas l'intention de développer ou d'acquérir des systèmes d'armes létaux autonomes[30]. Faute de transparence, il est souvent difficile de déterminer le statut du déploiement aux frontières des systèmes d'armes autonomes. Dans la perspective de l'installation de ces systèmes, il est crucial que les États prennent en compte et combattent les effets disproportionnés liés à la race, à l'ethnie et à la nationalité que des armes totalement autonomes auraient sur des groupes vulnérables, en particulier les réfugiés, les migrants, les demandeurs d'asile, les apatrides et les groupes apparentés.

15. Les États Membres et plusieurs organes de l'ONU s'appuient de plus en plus sur l'analyse de mégadonnées pour élaborer leurs politiques. Ainsi, l'Organisation internationale pour les migrations (OIM) surveille les populations en déplacement au moyen de sa matrice de suivi des déplacements, afin de mieux prévoir les besoins des personnes déplacées ; elle utilise l'enregistrement des appels téléphoniques et la géolocalisation ainsi que l'analyse de l'activité sur les médias sociaux[31]. Aux États-Unis d'Amérique, l'analyse des mégadonnées servent également à prédire quelles seraient, en fonction des liens communautaires préexistants, les chances de réussite des réfugiés réinstallés[32]. Dans un contexte mondial de plus en plus hostile aux immigrants, des voix se sont élevées contre le fait que les données sur les migrations soient mal interprétées ou déformées à des fins politiques, par exemple pour influencer la distribution de l'aide. Des données inexactes peuvent également servir à alimenter la peur et la xénophobie, comme le montrent la description du groupe de migrants qui demandent l'asile à la frontière entre les États-Unis[33] et le Mexique ou l'incitation à la haine des migrants dans le pourtour méditerranéen (voir la proposition récente d'un système de barrages flottants)[34]. La peur de la société sert alors de prétexte à l'adoption de mesures de plus en plus dures, qui contreviennent au droit international des droits de l'homme[35]. Comme il est indiqué dans une communication, dans des contextes politiques fortement divisés, hostiles aux immigrés voire xénophobes, « les données utilisées pour alimenter les algorithmes d'apprentissage automatique aux frontières ou reprises dans les campagnes politiques ou dans la législation peuvent être erronées ; dans un environnement où règnent des préjugés

[26] Ibid.

[27] Jason De León, The Land of Open Graves: Living and Dying on the Migrant Trail (University of California Press, 2015).

[28] Raluca Csernatoni, « Constructing the EU's high-tech borders: Frontex and dual-use drones for border management ».

[29] Communication reçue de Campaign to Stop Killer Robots.

[30] Ibid.

[31] Voir https://dtm.iom.int/about.

[32] Voir https://news.stanford.edu/2018/01/18/algorithm-improves-integration-refugees/.

[33] Voir communication recue du Center on Race, Inequality and the Law de la New York University School of Law.

[34] Voir www.dezeen.com/2020/02/10/greece-floating-sea-border-wall-news/.

[35] Voir également Ana Beduschi, « International migration management in the age of artificial intelligence », *Migration Studies* (2020) ; et communication reçue d'Ana Beduschi.

structurels contre les minorités, une telle déformation des données peut alimenter la désinformation, les discours de haine et la violence »[36].

16. On ne saurait évaluer la situation des droits humains aux frontières numériques sans s'interroger sur le rôle des sociétés privées, dont la recherche du profit tient une place importante dans le développement de la technologie numérique pour la gestion de l'immigration et des frontières, souvent dans le cadre de partenariats qui permettent aux gouvernements de se dérober à leurs responsabilités et de ne pas prévenir les violations qui peuvent résulter de l'utilisation de ces technologies. L'expression « complexe militaro-industriel aux frontières » décrit « le lien entre la police des frontières, la militarisation et les intérêts financiers »[37], les gouvernements se tournant de plus en plus vers le secteur privé pour gérer les migrations au moyen des nouvelles technologies, invoquant des raisons de sécurité nationale, qui font fi des droits humains fondamentaux[38]. Le complexe militaro-industriel aux frontières repose, notamment, sur l'externalisation, la militarisation et l'automatisation des frontières[39]. Aux États-Unis, le budget consacré à la gestion des frontières et de l'immigration a augmenté de plus de 6 000 % depuis 1980[40]. Le budget dont dispose l'Union européenne pour la gestion des frontières extérieures, des migrations et des demandes d'asile pour 2021-2027 sera multiplié par 2,6, s'élevant à plus de 34,9 milliards d'euros, contre 13 milliards d'euros pour 2014-2020[41]. Selon des études de marché récentes, le taux composé de croissance annuelle de ce marché mondial de la sécurité des frontières devrait se situer entre 7,2 et 8,6 % (65 à 68 millions de dollars US) en 2025[42].

17. Parmi les nouvelles technologies numériques qui sous-tendent le complexe industriel frontalier, les drones (surveillance des frontières) et la biométrie (« frontières intelligentes ») jouent un rôle clé[43]. Les grands acteurs et bénéficiaires privés du secteur de la surveillance des frontières sont en grande partie des entreprises militaires du Nord, dont certaines, comme Lockheed Martin, sont les plus grands vendeurs d'armes au monde[44]. Les entreprises de technologie de l'information, telles qu'IBM, sont également des acteurs majeurs, notamment dans la collecte et le traitement des données[45]. Nombre de ces entreprises exercent une grande influence sur les décisions nationales et internationales en matière de gestion des frontières numériques[46]. Le système de la « porte tournante » entre le secteur public et les entreprises privées réduit et brouille encore plus la séparation entre les pouvoirs publics (contrôle aux frontières, armée) et le secteur (sociétés de sécurité et de conseil)[47]. Les entreprises sont également liées aux gouvernements par des coentreprises. Selon une communication, en 2016, par exemple, l'entreprise française publique-privée Civipol a mis en place des bases de données d'empreintes digitales

[36] Communication reçue du Groupement pour les droits des minorités.
[37] Voir www.aljazeera.com/opinions/2019/11/1/why-climate-action-needs-to-target-the-border-industrial-complex/.
[38] Communication reçue de Dhakshayini Sooriyakumaran et Brami Jegan.
[39] Ibid.
[40] Ibid.
[41] Voir https://ec.europa.eu/commission/presscorner/detail/fr/IP_18_4106.
[42] Voir www.issuewire.com/border-security-system-industry-projected-to-garner-usd-6781-billion-by-2025-flir-systems-lockhee-1631530966252699 et www.marketresearchfuture.com/reports/border-security-market-1662.
[43] Communication reçue de Dhakshayini Sooriyakumaran et Brami Jegan.
[44] Ibid.
[45] Ibid.
[46] Ibid, citant www.escr-net.org/corporateaccountability/corporatecapture.
[47] Communication reçue de Dhakshayini Sooriyakumaran et Brami Jegan.

pour le Mali et le Sénégal[48]. Financés à hauteur de 53 millions d'euros par le Fonds fiduciaire d'urgence en faveur de la stabilité et de la lutte contre les causes profondes de la migration irrégulière et du phénomène des personnes déplacées en Afrique, ces projets visent à identifier les réfugiés arrivant en Europe en provenance de ces deux pays afin de les expulser[49]. La France détient 40 % de Civipol, tandis que les fabricants d'armes Airbus, Safran et Thales possèdent chacun plus de 10 % des parts[50]. On voit ainsi comment les pays du Nord utilisent l'aide internationale au service de leurs intérêts dans les pays du Sud.

18. Dans une étude, l'inquiétude que suscite la montée du « technocolonialisme » est palpable. L'auteur met en lumière « le rôle constitutif que les données et l'innovation numérique jouent dans l'ancrage des inégalités entre réfugiés et agences humanitaires et, en fin de compte, des inégalités dans le monde », rôle alimenté en partie par la rapacité des entreprises et l'abdication par les gouvernements de leurs responsabilités en matière de droits humains[51]. Ces inégalités se perpétuent dans les formes d'expérimentation technologique, l'extraction de données et la valorisation et les formes de discrimination directe et indirecte décrites à la partie III ci-dessous.

19. En bref, nombre des technologies numériques utilisées aux frontières remplacent ou facilitent les processus décisionnels humains, parfois d'une manière qui suscite de graves préoccupations au sujet des droits humains. Ces technologies donnent également aux gouvernements et aux acteurs privés plus de pouvoir et de contrôle sur les migrants, les réfugiés, les apatrides et d'autres personnes, et les met en même temps à l'abri des conséquences juridiques et judiciaires. En d'autres termes, elles augmentent le risque de violations graves des droits de la personne et contournent les garanties de fond et de procédure, par ailleurs essentielles dans le cadre de la gestion des frontières. La partie III ci-dessous est un récapitulatif de toute la gamme de violations des droits humains et des formes de discrimination rendues possibles par les appareils et l'infrastructure numériques utilisés aux frontières, et met en lumière la progression de ces pouvoirs et le recul des restrictions.

III. La discrimination raciale et xénophobe dans la gestion numérique des frontières et de l'immigration : état des lieux

A. Discrimination directe et indirecte

1. Plateformes en ligne

20. Il est ressorti des consultations menées auprès des migrants, des réfugiés et des apatrides que les plateformes de médias sociaux telles que Facebook, Twitter et WhatsApp servent à diffuser la haine raciste et xénophobe, et certains répondants ont déclaré avoir été directement visés par des messages personnels transmis sur ces plateformes. Des participants en Malaisie, par exemple, ont fait état du foisonnement des messages de promotion du racisme et de la xénophobie sur les plateformes de médias sociaux dans le contexte de la pandémie de maladie à coronavirus

---

[48] Mark Akkerman, « Expanding the fortress: the policies, the profiteers and the people shaped by EU's border externalisation programme » (2018).

[49] Ibid., citant https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/eutf_rapport_annuel_2016_final_fr.pdf.

[50] Voir https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-securitycompany-quietly-building-mass-biometric et www.afronline.org/?p=42722.

[51] Mirca Madianou « Technocolonialism: digital innovation and data practices in the humanitarian response to refugee crisis » *Social Media + Society* (avril 2019).

(COVID-19). Dans certains cas, les utilisateurs des sites ont publié des photos de migrants et de réfugiés qu'ils considéraient comme « illégaux », ce qui permettait de craindre que ces personnes soient ensuite ciblées dans le monde réel, en plus de subir des injures en ligne.

21. Une communication a appelé l'attention sur un site web de *blacklisting* (d'exclusion) géré de manière anonyme, Canary Mission, qui critique les étudiants, les professeurs et les militants ayant milité en public pour les droits des Palestiniens et cible de manière disproportionnée les personnes d'ascendance arabe. Selon la communication, les responsables israéliens de l'immigration ont utilisé des informations publiées sur ce site dans le cadre de l'administration des frontières israéliennes et des frontières du territoire palestinien occupé et de la police de ces frontières, notamment pour y refuser l'entrée[52]. De telles pratiques violent les droits à l'égalité et à la non-discrimination ainsi que les protections relatives à la liberté d'expression, et laissent à ceux dont les droits sont bafoués des voies de recours limitées.

2. Profilage racial

22. Les consultations menées auprès des migrants, des réfugiés et des apatrides ont également mis en évidence le rôle que jouent les technologies numériques dans le profilage racial et ethnique dans la police des frontières. Les participants se sont dits préoccupés par le profilage ethnique des Roms aux frontières de la Macédoine du Nord. Une affaire de profilage racial de Roms en 2017 a révélé que les fonctionnaires consignent sur une « liste d'exclusion »[53] les données biométriques des personnes empêchées de franchir ces frontières. Non sans raison, les intervenants se sont dit inquiets du nombre démesuré de Roms figurant sur ces listes ; les Roms font l'objet de profilage ethnique et ont peu de moyens pour contester leur inscription sur ces listes.

3. Collecte obligatoire de données biométriques, systèmes d'identification numérique et déni d'accès aux services de base

23. De plus en plus, les États exigent la collecte de données biométriques considérables auprès de non-citoyens ; or la collecte et l'utilisation de ces données créent d'inquiétantes possibilités de formes directes et indirectes de discrimination fondées sur la race, l'appartenance ethnique, l'origine nationale, l'ascendance et même la religion. Comme indiqué ci-dessus, dans la plupart des cas, les réfugiés, les migrants et les apatrides n'ont aucun contrôle sur la manière dont les données les concernant sont partagées. Selon une communication reçue, l'Inde exige la collecte obligatoire de données biométriques auprès des non-citoyens, ces données étant principalement utilisées de manière discriminatoire à des fins de détention et d'expulsion ciblée, même pour les réfugiés tels que les Rohingya[54]. Une autre préoccupation soulevée dans le contexte de l'Inde concerne l'utilisation du système Aadhaar pour refuser l'accès aux services de base vitaux ; comme la prestation de ces services fait appel à des systèmes automatisés, dans les faits, les non-citoyens n'y ont absolument aucun accès[55]. Étant donné que les réfugiés sans permis de séjour ne peuvent pas obtenir de carte Aadhaar, ils sont victimes de discrimination et sont privés d'un accès aux services de base et de la jouissance des « droits qui garantissent un

[52] Communication reçue de l'organisation Palestine Legal.

[53] Voir www.errc.org/uploads/upload_en/file/5209_file1_third-party-intervention-kham-delchevo-and-others-v-north-macedonia-5-february-2020.pdf.

[54] Communication reçue de Anubhav Dutt Tiwari et Jessica Field.

[55] Ibid.

refuge digne en Inde »[56]. Selon cette communication, même les enfants réfugiés se sont vu refuser l'accès à l'enseignement primaire parce qu'ils n'avaient pas de carte Aadhaar[57].

24. S'agissant des apatrides en particulier, les participants aux consultations ont indiqué que le développement des systèmes d'identification numérique mettait à mal les moyens de survie informels dont ces groupes s'étaient dotés, faute de documents appropriés et de la reconnaissance par les États dans lesquels ils résidaient. Les apatrides, qui sont principalement membres de minorités raciales et ethniques, sont systématiquement exclus des bases de données et d'autres systèmes d'identité numériques. Les systèmes centralisés d'identification biométrique vont à l'encontre, à divers égards, des cadres internationalement reconnus relatifs à la nationalité et à la citoyenneté. Les principaux problèmes cités sont la prise de décision algorithmique et le fait que les décisions sur le statut juridique des personnes ne sont plus du ressort des fonctionnaires, mais qu'elles relèvent plutôt des ordinateurs ou des préposés à l'enregistrement qui administrent les kits de données biométriques. Cela peut aboutir à une dénaturalisation *de facto,* sans procédure ni garanties. Les mêmes principes qui doivent orienter toute décision concernant la privation de nationalité, notamment la non-discrimination, la prévention de l'apatridie, l'interdiction de l'arbitraire, la proportionnalité, la nécessité et la légalité, doivent également entrer en jeu lorsqu'on envisage d'adopter un système centralisé d'identification biométrique[58]. L'introduction de structures de gouvernance numériques risque de priver les personnes de leur nationalité par personne interposée, sans procédure régulière – à dessein ou du fait de systèmes d'enregistrement de l'état civil lacunaires ou défectueux[59]. Au cours des consultations, les participants issus des communautés nubienne et somalienne du Kenya et des communautés rohingya, par exemple, ont fait état de difficultés systématiques à obtenir une identification numérique, ce qui a ensuite compromis leurs possibilités de trouver un emploi formel et de satisfaire d'autres besoins fondamentaux. Dans certains cas, les systèmes d'identification numérique semblent exacerber l'apatridie en entraînant l'exclusion complète et la non-reconnaissance des groupes ethniques minoritaires.

4. Reconnaissance linguistique

25. Bien que les systèmes d'enregistrement automatisés puissent être adoptés dans le but d'améliorer l'efficacité bureaucratique, leur technologie peut engendrer des résultats discriminatoires. Selon une communication reçue, l'Office fédéral pour les migrations et les réfugiés de l'Allemagne[60] utilise TraLitA, un programme de translittération automatique, pour consigner les noms arabes au moyen de l'alphabet latin. Cependant, le système est plus sujet à l'erreur pour les demandeurs dont les noms sont originaires de la région du Maghreb : le taux d'exactitude pour ces derniers est en effet de 35 %, contre 85 à 90 % pour les noms des demandeurs d'origine iraquienne ou syrienne. Les candidats arabophones peuvent également avoir à subir une analyse dialectale lors de leur inscription. L'Office fédéral utilise en effet un logiciel pour analyser un échantillon de la langue parlée du demandeur afin de déterminer le degré de plausibilité de l'origine nationale déclarée. Ce logiciel repose sur le dialecte levantin de l'arabe[61], et la communication évoque la grave

[56] Ibid.
[57] Ibid.
[58] Institute on Statelessness and Inclusion *et al.*, « Principles: on deprivation of nationality as a national security measure » (2020) disponible à cette adresse : https://files.institutesi.org/PRINCIPLES.pdf.
[59] Ibid., principe nº 10.
[60] Communication reçue de *Geselleschaft für Freiheitsrechte*.
[61] Ibid.

préoccupation selon laquelle la « probabilité d'erreurs du logiciel n'a jamais été vérifiée par un contrôle de supervision spécialisé et ne peut être comprise par des acteurs externes qui n'ont pas accès aux algorithmes utilisés »[62]. Le risque évident est que les locuteurs des dialectes arabes qui ne sont pas pris en charge par le logiciel puissent être considérés à tort comme non crédibles, et donc qu'ils se voient refuser des protections légales et autres sur une base discriminatoire.

5. Extraction de données mobiles et renseignements sur les populations migrantes et réfugiées tirés des médias sociaux

26. Les gouvernements s'intéressent de plus en plus aux appareils électroniques des migrants et des réfugiés en tant que moyens de vérifier les informations que ces personnes donnent aux services responsables des frontières et de l'immigration. Pour ce faire, les agents de ces services peuvent utiliser des outils d'extraction qui téléchargent des données à partir de téléphones intelligents, notamment des contacts, des données d'appel, des messages texte, des fichiers stockés, des informations de localisation, etc.[63]. Dans certains cas, les agents vont jusqu'à retirer aux migrants et aux réfugiés leurs appareils personnels. Selon une communication, il est courant que « les migrants qui sont interceptés soient dépouillés de leurs biens par les autorités croates, en particulier leurs passeports et d'autres types de pièces d'identité, les téléphones portables et les batteries externes, et soient sommairement refoulés vers la Bosnie-Herzégovine »[64].

27. En Allemagne, en Autriche, en Belgique, au Danemark, en Norvège et au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, des lois permettent de saisir les téléphones portables des demandeurs d'asile ou des candidats à l'immigration pour en extraire les données, qui sont ensuite utilisées dans le cadre des procédures d'asile[65]. Cette pratique constitue une entrave grave et disproportionnée au droit des migrants et des réfugiés à la vie privée, sur la base de leur statut d'immigration et, effectivement, de leur origine nationale. En outre, il est erroné de présumer que les données obtenues à partir d'appareils numériques conduisent nécessairement à des preuves fiables[66]. Les gouvernements ont également eu recours aux renseignements tirés des médias sociaux, c'est-à-dire les techniques et technologies qui permettent aux entreprises ou aux gouvernements de surveiller les sites de réseaux sociaux, tels que Facebook ou Twitter[67]. Certaines de ces activités sont menées directement par les agents de l'État, mais dans certains cas, les gouvernements demandent aux entreprises de mettre à leur disposition les outils ou le savoir-faire nécessaires (ou les deux) pour effectuer cette surveillance[68].

28. Une communication reçue donnait des détails sur des activités préoccupantes menées en Allemagne[69]. Aux termes de l'article 15 de la loi modifiée sur l'asile (*Asylgesetz*), les demandeurs d'asile qui ne sont pas en mesure de présenter un passeport valide ou un document équivalent doivent remettre tous leurs supports de données – non seulement les téléphones portables, mais aussi les ordinateurs portables, les clés USB et même les moniteurs d'activité physique – ainsi que leurs identifiants de connexion ; ces données sont « lues » par l'Office fédéral des migrations et des réfugiés afin de confirmer leur identité ou leur nationalité[70]. La Loi

---

[62] Ibid.
[63] Ibid ; et communication reçue de Privacy International *et al*.
[64] Communication reçue du Border Violence Monitoring Network.
[65] Communication reçue de Privacy International *et al*.
[66] Communication reçue de *Geselleschaft für Freiheitsrechte*.
[67] Communication reçue de Privacy International *et al*.
[68] Ibid.
[69] Communication reçue de *Geselleschaft für Freiheitsrechte*.
[70] Ibid.

relative à une application plus rigoureuse de l'obligation de quitter le pays *(Gesetz zur besseren Durchsetzung der Ausreisepflicht)* autorise également l'Office à partager les données avec d'autres organismes gouvernementaux, tels que les autorités chargées de la sécurité et les services de renseignement[71]. Si cela est jugé nécessaire, la « lecture » des données a lieu avant l'audience relative à l'asile, à la demande du Secrétariat des procédures d'asile et avec le consentement signé du demandeur[72], bien qu'il soit indiqué dans la soumission que les demandeurs subissent « de très fortes pressions pour suivre les demandes gouvernementales » et qu'ils craignent les incidences négatives sur l'issue de leur procédure[73]. Plus de la moitié des demandeurs d'asile qui en étaient à leur première demande ont fait l'objet de cette pratique de routine au cours des deux dernières années, et le fait que certaines nationalités semblent plus visées que d'autres suscite de graves préoccupations concernant une possible discrimination de facto fondée sur l'origine nationale[74].

29. Cette extraction de données invasive effectuée sur des appareils personnels en Allemagne est sans précédent, elle ne vise que les demandeurs d'asile, et la légalisation de ces mesures est fondée sur un discours politique véhiculant des hypothèses racistes et xénophobes[75]. Il ressort aussi de la communication que ces analyses des supports de données se sont révélées inadaptées pour vérifier l'identité ou l'origine nationale du demandeur d'asile avec un quelconque degré de certitude, ou pour prévenir l'abus de la procédure d'asile[76]. Environ le quart des tentatives de lecture se soldent par un échec technique et, même si la lecture des données est possible, la plupart des rapports d'analyse sont inutilisables parce que la quantité de données examinées est trop faible ou autrement peu concluante[77]. Sur 21 505 téléphones mobiles dont les données ont été lues en 2018 et 2019, seuls 118 cas environ, soit 0,55 %, ont révélé une incohérence[78]. En outre, comme ni les algorithmes ni les données d'apprentissage ne sont connus du public, les juges et autres décideurs ne peuvent pas correctement en évaluer la fiabilité[79].

30. Bien que des règlements tels que le règlement général de l'Union européenne sur la protection des données visent à protéger les données et la vie privée, certains États prévoient des dérogations dans le contexte de l'application des lois relatives à l'immigration. Deux communications ont fait état de dérogations à ce règlement inscrites dans la Loi sur la protection des données du Royaume-Uni, de 2018[80]. En vertu de cette « exemption d'immigration », une entité ayant le pouvoir de traiter des données, appelée « responsable de traitement », peut contourner les droits fondamentaux d'une personne concernant l'accès à ses données si le fait de procéder autrement « porte préjudice à un contrôle efficace de l'immigration »[81]. Ces droits comprennent le droit de la personne de s'opposer (en tout ou en partie) au traitement de ses données et le droit de faire supprimer ses données personnelles[82]. L'exemption décharge également les responsables de traitement de leur obligation d'informer les personnes concernées lorsque leurs données sont collectées, y compris à partir de

[71] Ibid.
[72] Ibid.
[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Ibid ; et communication reçue de la Plateforme pour la coopération internationale concernant les sans-papiers.
[81] Communication reçue de la Plateforme pour la coopération internationale concernant les sans-papiers.
[82] Ibid.

sources tierces, comme une école, un employeur ou une autorité locale[83]. Au Royaume-Uni, la loi modifiée sur la police habilite non seulement la police mais aussi les agents de l'immigration à modifier les téléphones portables et autres appareils électroniques appartenant aux demandeurs d'asile[84]. La loi du Royaume-Uni sur la criminalité et les tribunaux de 2013 va bien plus loin que l'analyse des supports de données autorisée en Allemagne : elle permet à la police et aux agents de l'immigration de mettre en œuvre des mesures de surveillance secrètes, de placer des dispositifs d'écoute, de pirater des téléphones portables et des ordinateurs et de les perquisitionner[85]. Les personnes concernées sont ciblées de manière disproportionnée sur la base de l'origine nationale, alors que l'origine nationale ne devrait jamais constituer un motif d'atteinte à la vie privée ou à d'autres droits.

B. Structures discriminatoires

31. Dans le rapport présenté au Conseil des droits de l'homme, la Rapporteuse spéciale a cité des exemples montrant que la combinaison, intentionnelle ou non, de la conception et de l'utilisation de différentes nouvelles technologies numériques peut créer des structures discriminatoires sur le plan racial qui, globalement ou systématiquement, entravent la jouissance des droits humains de certains groupes de personnes, en raison de leur race, de leur appartenance ethnique ou de leur origine nationale, qui viennent s'ajouter à d'autres caractéristiques. Autrement dit, il faut, a-t-elle souligné, comprendre que les nouvelles technologies numériques peuvent non seulement compromettre 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. Dans cette sous-section, la Rapporteuse spéciale met en évidence les façons dont les migrants, les réfugiés, les apatrides et les membres de groupes apparentés sont l'objet d'interventions technologiques qui les exposent à un large éventail de violations réelles et possibles de leurs droits en raison de leur origine nationale ou de leur statut d'immigration, réels ou perçus.

1. Humanitarisme de surveillance et asile de surveillance

32. Les auteurs de commentaires ont émis une mise en garde contre la montée de l'« humanitarisme de surveillance »[86], en vertu duquel le recours accru aux technologies numériques dans la prestation de services et les autres processus bureaucratiques a pour effet pervers de priver les réfugiés et les demandeurs d'asile de services de base tels que l'accès à la nourriture[87]. Le concept d'humanitarisme de surveillance ? fait référence à « d'énormes systèmes de collecte de données déployés par les organisations d'aide qui accroissent involontairement la vulnérabilité des personnes en situation d'urgence »[88]. Même un nom mal orthographié peut entraîner le « chaos bureaucratique » et donner lieu à une accusation d'avoir fourni de fausses informations, ralentissant ainsi une procédure d'asile qui est déjà lente[89]. Dans les zones de conflit, les préjudices potentiels liés à la confidentialité des données sont souvent latents et peuvent être violents, par exemple lorsque les données piratées ou

[83] Ibid.
[84] Communication reçue de *Geselleschaft für Freiheitsrechte*.
[85] Ibid.
[86] Voir www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
[87] Communication reçue de Beduschi.
[88] Voir www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
[89] Mark Latonero *et al.*, « Digital identity in the migration and refugee context: Italy case study » (*Data & Society*, avril 2019).

divulguées à une partie adverse pourraient entraîner des représailles pour ceux qui sont perçus comme étant dans le mauvais « camp »[90].

33. À cet égard, dans une des communications reçues, il est question des dangers liés à l'utilisation croissante des technologies numériques par le Haut-Commissariat des Nations Unies pour les réfugiés (HCR) pour gérer la distribution de l'aide[91]. Dans des camps de réfugiés en Afghanistan, le HCR a imposé l'enregistrement de l'iris aux réfugiés afghans qui retournent dans leur pays comme condition préalable à l'obtention d'une aide[92]. Bien que le HCR présente la collecte, la numérisation et le stockage des images de l'iris des réfugiés dans le système de gestion de l'identité biométrique comme un moyen de détecter et de prévenir la fraude[93], les conséquences du traitement de ces données sensibles peuvent être graves lorsque les systèmes sont défectueux ou utilisés à mauvais escient[94]. Il a également été prouvé qu'en suscitant une aversion pour le système, ces outils de surveillance biométrique occasionnent indirectement la perte de l'accès aux biens et services de première nécessité[95]. Cette communication fait état, par exemple, d'une défaillance de la technologie dans les camps de réfugiés rohingya au Bangladesh qui a eu pour effet que les réfugiés se sont vu refuser des rations alimentaires[96].

34. La collecte d'importantes quantités de données relatives aux migrants et aux réfugiés pose de graves problèmes et peut entraîner des violations des droits humains liées au partage des données et à l'accès à celles-ci, en particulier dans des contextes tels que les camps de réfugiés où les rapports de force inégaux entre les organismes des Nations Unies, les organisations non gouvernementales internationales et les groupes concernés sont déjà très marquées. Bien que l'échange de données sur les crises humanitaires et l'identification biométrique soient souvent présentés comme des moyens d'accroître l'efficacité et la coopération entre les organismes et les États, les avantages de la collecte ne sont pas les mêmes pour tous. La collecte de données et l'utilisation des nouvelles technologies, en particulier dans des situations caractérisées par des rapports de force inégaux, soulèvent les questions du consentement éclairé et de la possibilité de refus. Dans divers contextes de migration forcée et d'aide humanitaire, comme à Mafraq, en Jordanie, les technologies biométriques revêtent la forme d'un balayage de l'iris (plutôt que l'utilisation de cartes d'identité) en échange de rations alimentaires[97]. Cependant, le fait d'assujettir l'accès à la nourriture à la collecte de données supprime tout semblant de choix ou d'autonomie de la part des réfugiés : le consentement ne peut être donné librement lorsque la famine constitue le seul autre choix. En effet, une enquête menée dans le camp de réfugiés d'Azraq a révélé que la plupart des réfugiés interrogés étaient mal à l'aise face à de telles expériences technologiques mais qu'ils estimaient ne pas pouvoir refuser s'ils voulaient manger[98]. L'objectif ou la promesse d'une amélioration

---

[90] https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
[91] Communication reçue de Amnesty International.
[92] Ibid.
[93] Ibid.
[94] Ibid., renvoyant à A/HRC/39/29.
[95] Communication reçue de Amnesty International.
[96] Ibid.
[97] Fleur Johns, « Data, detection, and the redistribution of the sensible in international law », *American Journal of International Law*, vol. 111, nº 1 (2017). Voir également https://medium.com/unhcr-innovation-service/managing-risk-to-innovate-in-unhcr-91fe9294755b.
[98] Voir http://www.irinnews.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan.

de la prestation de services ne saurait justifier le degré de coercition implicite qui sous-tend de tels systèmes[99].

35. Les consultations ont mis en évidence les préoccupations des réfugiés rohingya au Bangladesh et en Inde, qui craignent que leurs données soient partagées de manière à accroître leur risque de refoulement, ou encore partagées avec le Gouvernement du Myanmar, ce qui augmenterait leur vulnérabilité aux violations de leurs droits humains en cas de retour forcé ou d'autres formes de rapatriement de ces groupes. Dans ce contexte, une possibilité qui suscite l'inquiétude est celle du « détournement de fonction », c'est-à-dire d'une situation où les données collectées dans un but précis (par exemple, la surveillance de la fraude de faible niveau) sont partagées et réutilisées à des fins différentes (par exemple, pour alimenter les registres de terroristes potentiels), sans aucune protection, sur le fond ou la procédure, pour les personnes dont les données sont partagées et réutilisées[100].

36. Dans certains cas, c'est la nature même de la collecte de données qui peut produire des résultats profondément discriminatoires. Depuis août 2017, plus de 742 000 réfugiés rohingya apatrides ont traversé la frontière pour se rendre au Bangladesh afin d'échapper au génocide au Myanmar[101]. Or le système d'enregistrement du HCR et du Gouvernement bangladais ne proposait pas le terme « Rohingya » parmi les options d'identité ethnique, mais plutôt « ressortissants du Myanmar », terme que le Myanmar ne reconnaît pas, et qui ne rend pas compte de la réalité selon laquelle les Rohingya sont apatrides parce qu'ils ont été arbitrairement privés de leur droit à la nationalité du Myanmar[102]. Comme il est indiqué dans une communication, la catégorisation utilisant ce terme méconnaissable sur leurs cartes d'identité numériques équivaut à une forme d'« anéantissement symbolique » des Rohingya qui sont contraints d'utiliser ces cartes[103].

37. Ce n'est pas que dans les camps de réfugiés que les technologies numériques privent les réfugiés et les demandeurs d'asile de l'accès aux services de base essentiels. Une communication reçue cite un cas survenu en Allemagne. Dans ce pays, en vertu de la Loi sur les avantages accordés aux demandeurs d'asile, les personnes sans papiers ont le même droit aux soins de santé que les demandeurs d'asile[104]. Toutefois, le bureau d'aide sociale qui gère les soins de santé pour les sans-papiers a le devoir de communiquer leurs données personnelles aux autorités de l'immigration en vertu de l'article 87 de la Loi sur la résidence, qui régit le « transfert de données et d'informations pour les autorités étrangères » par toutes les autorités publiques[105]. Cela signifie que l'accès légal aux soins de santé peut entraîner l'application des lois relatives à l'immigration, ce qui a probablement un effet dissuasif sur le recours des migrants et des réfugiés aux soins de santé, même en cas d'urgence.

2. Expérimentation technologique

38. Les communications reçues pour l'établissement du présent rapport sont très préoccupantes s'agissant de l'expérimentation technologique généralisée menée par

---

[99] Voir https://www.unhcr.org/innovation/wp-content/uploads/2020/04/Space-and-imagination-rethinking-refugees%E2%80%99-digital-access_WEB042020.pdf ; et Dragana Kaurin, « Data protection and digital agency for refugees ».

[100] Communication reçue de Mirca Madianou.

[101] Voir www.unhcr.org/en-us/rohingya-emergency.html.

[102] Mirca Madianou, « Technocolonialism: digital innovation and data practices in the humanitarian response to refugee crises ».

[103] Communication reçue de Mirca Madianou.

[104] Communication reçue de la Plateforme pour la coopération internationale concernant les sans-papiers.

[105] Ibid.

des acteurs étatiques et non étatiques sur les réfugiés, les migrants et les apatrides. Les expériences décrites consistent à tester divers produits technologiques dans des circonstances où les groupes ciblés n'ont que peu ou pas de moyens de donner leur consentement éclairé et où les conséquences des tests et de l'expérimentation sur les droits humains sont défavorables ou inconnues. En règle générale, les réfugiés, les migrants et les apatrides n'ont aucune voie de recours (ou des voies très limitées) pour s'opposer à cette expérimentation technologique et aux violations des droits humains qui peuvent y être associées. En outre, ce sont l'origine nationale et le statut de citoyenneté ou d'immigration qui exposent les réfugiés, les migrants et les apatrides à cette expérimentation, ce qui suscite de vives préoccupations quant à l'existence de schémas de vulnérabilité discriminatoires.

39. Une communication a appelé l'attention sur le système iBorderCtrl (le « système intelligent de gestion des frontières »), qui, dans le cadre du programme Horizon 2020 de l'Union européenne, « vise à permettre un contrôle aux frontières plus rapide et plus rigoureux pour les ressortissants de pays tiers qui traversent les frontières terrestres des États membres de l'Union »[106]. Ce système fait appel à des technologies matérielles et logicielles qui ont pour but d'automatiser la surveillance des frontières[107]. Une de ses fonctionnalités permettrait la détection automatisée de la tromperie[108]. L'Union européenne a mis ce « détecteur de mensonges » à l'essai dans des aéroports en Grèce, en Hongrie et en Lettonie[109]. En 2019, iBorderCtrl aurait aussi fait l'objet d'essais (sans succès) à la frontière serbo-hongroise[110]. Le système iBorderCtrl illustre la tendance consistant à tester les technologies de surveillance (et autres) sur les demandeurs d'asile en se basant sur des principes scientifiques douteux[111]. S'appuyant sur la théorie contestée de la « science de la reconnaissance des affects », le système iBorderCtrl remplace les garde-frontières humains par un système de reconnaissance faciale qui cherche à repérer les expressions anormales chez les voyageurs pendant qu'ils répondent à une série de questions[112]. D'autres pays, comme la Nouvelle-Zélande, mettent également à l'essai l'utilisation des technologies de reconnaissance faciale automatisée pour identifier les soi-disant « fauteurs de troubles » éventuels, ce qui a incité les organisations de la société civile à engager des poursuites judiciaires pour discrimination et profilage racial[113].

40. Certains États mettent actuellement à l'essai l'automatisation de diverses facettes de la prise de décisions en matière d'immigration et d'asile. Par exemple, depuis 2014 au moins, le Canada utilise une forme de prise de décision automatisée dans son système de gestion de l'immigration et des réfugiés[114]. Un rapport de l'Université de Toronto datant de 2018 portait sur les risques qu'entraîne pour les droits humains l'utilisation de l'intelligence artificielle pour remplacer ou renforcer les décisions en matière d'immigration, indiquant que ces processus « créent un

---

[106] Communication reçue de Privacy International *et al*.

[107] Pour des renseignements généraux sur le projet, voir Commission européenne, « Smart lie-detection system to tighten EU's busy borders » (24 octobre 2018), disponible (en anglais) à cette adresse : https://ec.europa.eu/research/infocentre/article_en.cfm?artid=49726.

[108] Communication reçue de Privacy International *et al*.

[109] Communication reçue de Maat for Peace, Development and Human Rights (Maat), p. 6. Voir également Petra Molnar, « Technology on the Margins: AI and global migration management from a human rights perspective » (2019) ; et communication reçue de Minority Groups International.

[110] Communication reçue de Privacy International *et al*.

[111] Ibid.

[112] Communication reçue de Minority Groups International.

[113] Voir www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12026585.

[114] Petra Molnar et Lex Gill, « Bots at the gate: a human rights analysis of automated decision-making in Canada's immigration and refugee system » (2018), programme Citizen Lab and International Human Rights, Faculté de droit, Université de Toronto, rapport de recherche nº 114 (septembre 2018).

laboratoire pour des expériences à haut risque dans un système déjà très discrétionnaire et opaque »[115]. Le recours à la prise de décision automatisée dans le contexte de l'immigration et des réfugiés entraîne de vastes conséquences. Bien que le Gouvernement canadien ait confirmé que ce type de technologie sert uniquement à faciliter la prise de décision humaine et qu'il est réservé à certaines demandes d'immigration seulement, il n'existe actuellement aucun mécanisme juridique destiné à protéger les garanties judiciaires en faveur des non-citoyens et à empêcher les violations des droits humains. Des algorithmes similaires sont actuellement utilisés au Royaume-Uni pour les visas et ont été contestés devant les tribunaux en raison de leur potentiel discriminatoire[116]. Le Canada, le Royaume-Uni et la Suisse utilisent également un processus décisionnel automatisé ou algorithmique « pour la sélection et la réinstallation des réfugiés »[117]. L'introduction de nouvelles technologies a une incidence à la fois sur les processus et sur les résultats associés aux décisions qui autrement relèveraient de tribunaux administratifs, d'agents d'immigration, de garde-frontières, d'analystes juridiques et d'autres fonctionnaires responsables de l'administration des systèmes d'immigration et de réfugiés, de la police des frontières et de la gestion de l'action en faveur des réfugiés. Il y a un important manque de clarté quant à la manière dont les tribunaux interprètent les principes de droit administratif tels que les règles de bonne justice, la justice procédurale et les normes de contrôle lorsqu'il s'agit d'un système de décision automatisé ou d'une utilisation opaque de la technologie.

41. Dans certains contextes, l'expérimentation technologique a trait à la collecte de données génétiques et repose sur des motifs ténus, qui soulèvent néanmoins des préoccupations sérieuses et concrètes en matière de droits humains. Une communication reçue fait état du système CODIS (Combined DNA Index System), une base de données génétiques médico-légales utilisée aux États-Unis et grâce à laquelle les États et le Gouvernement fédéral collectent, stockent et partagent des informations génétiques[118]. Depuis janvier 2020, le Gouvernement fédéral prélève l'ADN de toute personne se trouvant dans un centre de détention pour immigrants[119]. Cela signifie que « pour la première fois, le système CODIS va servir à stocker les données génétiques de personnes qui n'ont été accusées d'aucun crime, à des fins de détection des crimes », contournant ainsi l'exigence de longue date d'un comportement criminel présumé pour justifier le prélèvement d'ADN[120]. En règle générale, les non-citoyens en garde à vue dans ces centres ne sont pas des criminels[121]. En fait, dans la grande majorité des cas, les infractions à la législation sur l'immigration pour lesquelles un immigrant est détenu sont de nature civile[122]. S'agissant des demandeurs d'asile, qui constituent une proportion de plus en plus importante de la population de détenus non-citoyens, les lois internationales et nationales leur permettent expressément d'entrer aux États-Unis pour y demander le droit au refuge[123]. Dans la communication, il est souligné à juste titre que la nouvelle politique d'immigration élargissant le système CODIS rapproche les États-Unis de la création d'un « observatoire génétique », dont les objectifs et les effets pourraient

[115] Ibid.

[116] Voir www.foxglove.org.uk/news/home-office-says-it-will-abandon-its-racist-visa-algorithm-nbsp-after-we-sued-them.

[117] Communication reçue de Maat for Peace, Development and Human Rights ; communication reçue d'Ana Beduschi, citant Petra Molnar et Lex Gill, « Bots at the gate: a human rights analysis of automated decision-making in Canada's immigration and refugee system ».

[118] Communication reçue de Daniel I. Morales, Natalie Ram et Jessica L. Roberts.

[119] Ibid.

[120] Ibid.

[121] Ibid.

[122] Ibid.

[123] Ibid.

bien être discriminatoires. Le système CODIS risque de devenir l'instrument d'une sinistre surveillance génétique « qui finira par englober toute personne se trouvant en territoire américain, y compris de simples citoyens qui n'ont été ni condamnés pour actes criminels, ni même soupçonnés de tels actes », faisant ainsi peser une menace sur la démocratie et les droits humains[124], notamment sur la base de la nationalité d'origine.

42. Comme la pandémie de COVID-19 tend à motiver et à légitimer les technologies de surveillance qui ciblent les réfugiés et les migrants, ces groupes font l'objet d'autres expériences[125]. Le déploiement expérimental d'un passeport d'immunité appelé « COVI-Pass » en Afrique de l'Ouest en est un exemple[126]. Fruit d'un partenariat entre Mastercard et GAVI (alliance privée-publique pour la vaccination), cette initiative numérique conjugue la biométrie, la recherche des contacts, les services de paiement sans espèces, les documents d'identité nationaux et l'application de la loi[127]. En plus d'échapper au cadre des études d'impact sur les droits humains et de la réglementation en la matière, ces initiatives risquent de porter atteinte aux droits humains, notamment la liberté de circulation, le droit à la vie privée, le droit à l'autonomie corporelle et le droit à l'égalité et à la non-discrimination, surtout en ce qui concerne les réfugiés et les migrants[128].

3. Externalisation des frontières

43. L'externalisation des frontières – l'extraterritorialisation des frontières nationales et régionales vers d'autres régions géographiques afin d'empêcher l'arrivée de migrants et de réfugiés – est devenue un outil standard de contrôle des frontières pour de nombreux pays et régions. Il existe de nombreuses preuves écrites des violations des droits humains associées à ce phénomène[129]. Or l'externalisation des frontières n'a pas la même incidence sur tous les groupes de nationalité ou d'origine nationale. Elle a un impact démesuré sur les personnes originaires d'Afrique, d'Amérique centrale et du Sud et d'Asie du Sud et, dans de nombreuses régions, elle est favorisée par des politiques racistes, xénophobes et ethnonationalistes destinées à exclure certains groupes nationaux et ethniques sur des bases discriminatoires. De plus en plus, les États et les blocs régionaux font appel aux technologies numériques pour mener à bien cette externalisation des frontières, et, ce faisant, consolider et élargir les régimes de discrimination et d'exclusion.

44. Dans une des communications reçues, le Système européen de surveillance des frontières (EUROSUR) est présenté comme un programme qui exploite les mégadonnées « pour prévoir, surveiller et maîtriser les flux transfrontaliers au sein de l'Union européenne »[130]. Ce système permet notamment de déployer des drones de surveillance en mer Méditerranée, de manière à alerter des garde-côtes libyens qui souhaiteraient intercepter les bateaux de réfugiés et de migrants et renvoyer les migrants en Libye[131]. Bien que la Commission européenne insiste sur le fait que les

---

[124] Ibid.
[125] Communication reçue de Amnesty International.
[126] Ibid.
[127] Ibid.
[128] Ibid.
[129] Voir, par exemple, A/HRC/23/46, A/HRC/29/36 et A/72/335.
[130] Communication reçue de Maat for Peace, Development and Human Rights, ciant Btihaj Ajana, « Augmented borders: big data and the ethics of immigration control », *Journal of Information, Communication and Ethics in Society*, vol. 13, nº 1 (2015).
[131] Communication reçue de Franciscans International, citant https://www.middleeastmonitor.com/20190819-eu-using-israel-drones-to-track-migrant-boats-in-the-med/.

drones ne sont utilisés qu'à des fins de surveillance civile[132], le Haut-Commissariat des Nations Unies aux droits de l'homme s'est prononcé contre les refoulements coordonnés et la non-assistance aux migrants et aux réfugiés en Méditerranée, qui font de cette mer une des routes migratoires les plus meurtrières au monde [133]. Les technologies de surveillance sont un élément essentiel de la coordination dans ce contexte.

45. Une autre communication reçue fait état de la participation de treize nations européennes au projet ROBORDER, un « système de surveillance des frontières pleinement fonctionnel et autonome »[134]. Le projet ROBORDER se compose de robots sans pilote, mobiles et capables de fonctionner de manière isolée ou en essaim, dans des milieux très divers – dans les airs, à la surface de l'eau, sur terre ou sous la mer[135]. Ce projet préconisant un recours accru aux drones pour surveiller les frontières de l'Europe accentue la décomposition de la zone frontalière en diverses couches de surveillance verticales et horizontales, asseyant le pouvoir de l'État dans le ciel, et, en élargissant la frontière visuellement et virtuellement, elle fait des êtres humains des objets de sécurité et des coordonnées à analyser, stocker, collecter et décortiquer[136]. L'utilisation de technologies autonomes militaires ou quasi-militaires resserre les liens entre, d'une part, l'immigration et la sécurité nationale et, d'autre part, la tendance croissante à la criminalisation des migrations ainsi qu'à l'utilisation d'une taxonomie basée sur les risques pour caractériser et signaler les cas[137]. À l'échelle mondiale, les États, en particulier ceux aux frontières desquels les réfugiés et les migrants arrivent en grand nombre, utilisent divers moyens pour décourager les personnes qui cherchent à demander l'asile légalement. Ce type de politique de dissuasion est très évident en Espagne, en Grèce et en Italie[138], trois pays qui se trouvent aux frontières géographiques de l'Europe et qui recourent de plus en plus à la dissuasion violente et aux politiques de refoulement.

46. Une des communications reçues portait sur l'utilisation par la Croatie de technologies financées par l'Union européenne pour détecter, appréhender et refouler les réfugiés et les migrants le long de la route des Balkans, qui part de la Bosnie-Herzégovine et de la Serbie et traverse la Croatie pour atteindre la frontière de l'espace Schengen[139]. Cette communication fait état de centaines d'atteintes aux droits humains qui auraient été commises au cours des trois dernières années, y compris des « refoulements illégaux » qui traduiraient « des clivages foncièrement racistes »[140]. Les technologies de surveillance telles que les drones et les hélicoptères équipés de projecteurs automatisés « sont utilisées agressivement contre les personnes en

---

[132] Communication reçue de Franciscans International, citant https://www.europarl.europa.eu/doceo/document/E-9-2019-003257-ASW_EN.pdf.

[133] Voir https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25875&LangID=E.

[134] Communication reçue de Homo Digitalis. Voir également https://roborder.eu. Les États participants sont les suivants : Allemagne, Belgique, Bulgarie, Espagne, Estonie, Finlande, Grèce, Hongrie, Italie, Portugal, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et Suisse.

[135] Ibid.

[136] Raluca Csernatoni, « Constructing the EU's high-tech borders: Frontex and dual-use drones for border management ».

[137] Communication reçue de Dimitri van den Meerssche.

[138] Voir www.statewatch.org/news/2017/november/eu-spain-new-report-provides-an-x-ray-of-the-public-funding-and-private-companies-in-spain-s-migration-control-industry/ ; https://www.efadrones.org/countries/italy/.

[139] Communication reçue de Border Violence Monitoring.

[140] Ibid.

situation de déplacement, ce qui rend ces dernières plus faciles à repérer et aggrave ainsi leur vulnérabilité et les dangers auxquels elles sont confrontées »[141].

47. L'externalisation discriminatoire des frontières est également facilitée par les programmes transnationaux de partage de données biométriques entre plusieurs pays. Une des communications reçues faisait état d'un programme de partage de données biométriques entre les gouvernements du Mexique et des États-Unis[142]. En date d'août 2018, le Mexique avait mis en place ce programme financé par les États-Unis dans l'ensemble des 52 centres de traitement des migrations[143]. Ce programme bilatéral utilise des données biométriques pour exclure les migrants détenus au Mexique qui auraient tenté de traverser la frontière américaine ou qui seraient membres d'une bande criminelle[144]. Cependant, l'Institut national des migrations du Mexique a nié avoir traité des données biométriques en réponse à des demandes d'accès à l'information[145].

4. Surveillance de l'immigration[146]

48. Dans une communication reçue, il est question de la construction en cours, à la frontière entre les États-Unis et le Mexique, d'« un réseau de cinquante-cinq tours équipées de caméras, de capteurs de chaleur, de détecteurs de mouvement, de systèmes radar et d'un système GPS »[147]. Ce système de police des frontières sert également à la surveillance de la réserve de la nation Tohono O'odham, située en Arizona à environ un *mile* de la frontière avec le Mexique [148]. Ce système « intelligent » de surveillance des frontières remplace un autre système, qui, selon les chercheurs, n'avait pas réussi à empêcher les personnes sans papiers de franchir la frontière, mais les avait plutôt incitées à modifier leur trajet, augmentant ainsi « leur vulnérabilité aux blessures, à l'isolement, à la déshydratation, à l'hyperthermie et à l'épuisement » – et les risques de décès[149]. Une autre communication indique que les chercheurs et les organisations de la société civile se sont opposés à ces technologies frontalières parce qu'« elles exacerberaient les inégalités raciales et ethniques dans les activités policières et l'application des lois relatives à l'immigration, tout en limitant la liberté d'expression et le droit à la vie privée »[150]. D'autres communications ont également mis en évidence le recours, à la frontière entre les États-Unis et le Mexique, à d'autres infrastructures autonomes de surveillance faisant appel à l'intelligence artificielle, notamment des drones conçus pour détecter la présence humaine et, le cas échéant, alerter les garde-frontières[151]. Le Comité pour l'élimination de la discrimination raciale a fait part à l'Assemblée générale de son inquiétude face aux « trajets de plus en plus précaires empruntés par les demandeurs d'asile, les réfugiés et les migrants en quête de sécurité et de dignité, qui entraînent

---

[141] Ibid.

[142] Communication reçue de Privacy International *et al*.

[143] Ibid.

[144] Ibid.

[145] Ibid.

[146] Anil Kalhan, « Immigration Surveillance », (2014), *Maryland Law Review*, vol. 74, No. 1 (article dans lequel la surveillance de l'immigration est définie comme le produit d'une identification, d'un suivi et d'un contrôle de la mobilité et d'un partage d'informations considérablement accrus, ainsi que d'un contournement des protections juridiques traditionnelles de fond et de procédure qui ont généralement été utilisées pour protéger les non-citoyens d'une foule de violations des droits humains).

[147] Communication reçue de Campaign to Stop Killer Robots.

[148] Ibid.

[149] Samuel Norton Chambers *et al*., « Mortality, surveillance and the tertiary "funnel effect" on the U.S.-Mexico border: a geospatial modeling of the geography of deterrence ».

[150] Communication reçue de Minority Groups International.

[151] Communication reçue de Mijente et communication reçue d'Iván Chaar-López.

des morts et des souffrances inutiles »[152], [153]. Comme indiqué plus haut, les renseignements les plus récents portent à croire que c'est la technologie frontalière dite « intelligente » qui impose ces trajets toujours plus périlleux, et que les conséquences sont démesurées pour certains groupes nationaux, ethniques et raciaux.

49. Aux États-Unis, les communications des immigrants détenus et de leurs familles et amis font l'objet d'une surveillance[154]. Selon le modèle de fonctionnement des entreprises qui fournissent les technologies utilisées, les immigrants détenus et leurs familles « obtiennent des avantages pratiques sous forme d'appels, de *chats* vidéo, de messages vocaux, de partage de photos et de SMS, tandis que leurs véritables clients », les responsables de l'immigration, obtiennent des données sur les utilisateurs[155]. Le logiciel de surveillance, accessible en ligne, est présenté comme un logiciel gratuit qui fournit aux fonctionnaires, partout où il est mis en œuvre, « l'analyse des schémas d'appel et des relations ainsi que des outils de visualisation des données »[156].

50. Un autre aspect de la surveillance de l'immigration consiste à filtrer les médias sociaux. Depuis avril 2019, le Département d'État américain exige des demandeurs de visa qu'ils divulguent les informations relatives à leur compte de médias sociaux pour les cinq années précédant la date de leur demande[157]. En septembre 2019, le Département américain de la sécurité du territoire (Department of Homeland Security) a formulé une proposition tendant à obliger les non-citoyens déjà présents (même à titre de résidants) au pays à divulguer ces informations lorsqu'ils demandent des avantages liés à l'immigration, notamment la naturalisation, la résidence permanente ou l'asile[158]. Comme il est indiqué dans la communication, cette approche élargie du filtrage des médias sociaux est particulièrement troublante quand on connaît les antécédents confirmés des responsables américains de l'immigration s'agissant d'utiliser les données relatives aux médias sociaux d'une manière qui nuit de façon disproportionnée aux membres de groupes raciaux, ethniques et religieux minoritaires[159]. Le Département américain de la sécurité du territoire s'est déjà servi des contacts des jeunes noirs ou latinos sur les médias sociaux pour les accuser à tort d'appartenir à des bandes criminelles, entraînant ainsi une ou plusieurs des conséquences suivantes : détention, expulsion, refus d'avantages d'immigration[160]. Le United States Immigration and Customs Enforcement, agence constitutive du Département américain de la sécurité du territoire, effectue souvent des recherches exhaustives dans les médias sociaux pour étayer les allégations d'adhésion à des bandes criminelles[161]. Dans un de ces cas, le Département américain de la sécurité du territoire s'est servi, pour étayer ses allégations, d'une photo trouvée sur Facebook du jeune immigrant concerné portant une casquette des Chicago Bulls. Le tribunal de l'immigration lui a refusé une libération sous caution et a rejeté ses demandes d'asile et de résidence permanente, l'expulsant vers un pays où il craignait pour sa vie, en violation des interdictions de non-refoulement prévues par le droit international[162].

---

[152] Communication reçue de Franciscans International.

[153] Voir A/72/18.

[154] Communication reçue de Mijente, citant www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.htm.

[155] Ibid.

[156] Ibid.

[157] Communication reçue du Harvard Immigration and Refugee Clinical Program.

[158] Ibid, citant https://www.govinfo.gov/content/pkg/FR-2019-09-04/pdf/2019-19021.pdf.

[159] Communication reçue du Harvard Immigration and Refugee Clinical Program.

[160] Ibid, citant https://www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-20180521.pdf.

[161] Communication reçue de Harvard Immigration and Refugee Clinical Program.

[162] Ibid.

51. En outre, le filtrage des médias sociaux a aggravé le risque démesuré touchant les personnes de confession musulmane (ou présumées l'être) ou d'origine arabe, « en créant une infrastructure reposant sur des inférences erronées et sur le principe de la culpabilité par association »[163]. Ainsi, l'automne dernier, le Bureau des douanes et de la protection des frontières des États-Unis, autre organisme relevant du Département américain de la sécurité du territoire, a refusé l'entrée au pays à un étudiant palestinien en raison des messages de ses amis sur Facebook exprimant des opinions politiques contre les États-Unis, même s'il n'avait pas publié ces opinions lui-même[164]. En plus du fardeau qu'elles font peser directement sur les non-citoyens, les exigences de divulgation élargies du gouvernement américain à l'égard des médias sociaux ont vraisemblablement une incidence sur la liberté d'expression et d'association.

52. Homeland Security Investigations, la division des enquêtes de l'Immigration and Customs Enforcement, met à l'essai des modalités de profilage automatisé des médias sociaux depuis 2016[165] et renforce ses logiciels libres d'exploitation des médias sociaux dans le but de pister les demandeurs et les détenteurs de visas avant et après leur arrivée aux États-Unis[166]. Les communications reçues faisaient également état des inquiétudes suscitées par le fait que le Gouvernement américain examinait certaines technologies dont le but est de « déterminer de manière automatisée » si un individu demandant ou détenant un visa américain est susceptible de devenir un « membre contribuant positivement à la société » ou s'il a l'intention de « commettre des attentats criminels ou terroristes »[167]. Dans une communication, il était question de l'utilisation aux États-Unis d'outils d'évaluation des risques dans les décisions relatives à la détention d'immigrants, notamment d'un outil faisant appel à un algorithme programmé de manière à recommander systématiquement la détention, indépendamment des antécédents criminels des immigrants concernés[168]. Cet exemple illustre la pratique consistant à manipuler la technologie de sorte qu'elle favorise, en matière d'immigration, des mesures punitives ancrées dans la vision raciste, xénophobe et ethnonationaliste de l'immigration défendue par l'Administration du président Donald Trump.

53. Les exemples cités plus haut sont révélateurs d'une tendance dans la surveillance de l'immigration, selon laquelle des modèles font appel à l'intelligence artificielle pour prédire si des personnes n'ayant aucun lien avec une quelconque activité criminelle risquent néanmoins de commettre des crimes à l'avenir. Ces modèles « prédictifs » ont cependant tendance à créer et à reproduire des schémas de discrimination raciale en circuit fermé[169]. En outre, des préjugés raciaux sous-tendent déjà les ensembles de données sur lesquels reposent ces modèles[170]. Or en traitant des ensembles de données discriminatoires comme s'ils étaient neutres, on élaborera des modèles discriminatoires de la criminalité qui « perpétuent les inégalités raciales et contribuent au ciblage et à la surveillance policière excessive des non-citoyens »[171].

---

[163] Ibid.

[164] Ibid.

[165] Communication reçue de Mijente, citant Sarah Lamdan, « When Westlaw fuels ICE Surveillance: legal ethics in the era of big data policing », *New York University Review of Law and Social Change*, vol. 43 (2019).

[166] Communication reçue de Mijente, citant https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.htm.

[167] Ibid.

[168] Communication reçue de Minority Groups International.

[169] Communication reçue de Mijente.

[170] Ibid.

[171] Ibid.

IV. Recommandations

54. **Dans le rapport qu'elle a présenté au Conseil des droits de l'homme, la Rapporteuse spéciale propose aux États une méthodologie structurelle et intersectionnelle, axée sur les droits humains, permettant d'aborder la question de la discrimination raciale dans la conception et l'utilisation des nouvelles technologies numériques. Elle y énumère les obligations internationales applicables en matière de droits humains, en insistant notamment sur :**

a) la portée des dispositions juridiques interdisant la discrimination raciale dans la conception et l'utilisation des nouvelles technologies numériques ;

b) l'obligation de prévenir et de combattre la discrimination raciale dans la conception et l'utilisation des nouvelles technologies numériques ;

c) l'obligation d'offrir des recours utiles aux victimes de discrimination raciale dans la conception et l'utilisation des nouvelles technologies numériques.

55. **La Rapporteuse spéciale y explique également les notions et principes que définit le droit international des droits de l'homme s'agissant de la discrimination raciale directe, indirecte et structurelle, et elle énonce les obligations qui en découlent, pour les États, dans le contexte de l'essor des nouvelles technologies numériques. Elle fait valoir que ces obligations concernent également des acteurs non étatiques, notamment les entreprises, qui, à bien des égards, exercent un plus grand contrôle sur ces technologies que les États. Elle réitère l'analyse et les recommandations figurant dans ce rapport et invite les États à les prendre en compte parallèlement aux recommandations énoncées dans le présent document. La présente série de recommandations concerne l'exécution des obligations relatives à l'égalité, aux droits humains et à la non-discrimination mises en évidence dans le rapport présenté au Conseil des droits de l'homme, dans le contexte spécifique de l'application des lois relatives aux frontières et à l'immigration.**

56. **Les États doivent s'attaquer aux idéologies et structures racistes et xénophobes qui contribuent de plus en plus à orienter l'administration et la police des frontières et de l'immigration. Les effets de la technologie sont, dans une large mesure, le produit des forces sociales, politiques et économiques sous-jacentes qui motivent la conception et l'utilisation de la technologie. Sans un abandon généralisé des approches politiques racistes, xénophobes, anti-migrants, anti-apatrides et anti-réfugiés en matière de gouvernance des frontières, les effets discriminatoires de la numérisation des frontières mis en évidence dans le présent rapport ne pourront être réparés. Les États doivent se conformer aux obligations qui leur incombent en vertu du droit international des droits de l'homme pour prévenir la discrimination raciale dans l'application des lois relatives aux frontières et à l'immigration et mettre en œuvre les recommandations formulées dans le rapport de la Rapporteuse spéciale intitulé « Discrimination raciale et nouvelles technologies numériques : analyse sous l'angle des droits de l'homme » (A/HRC/44/57). Les États devraient également suivre les orientations fournies par des documents tels que les Principes sur la privation de nationalité en tant que mesure de sécurité nationale[172] et les Principes de protection des migrant-e-s, des réfugié-e-s et des autres personnes**

[172] Institute on Statelessness and Inclusion *et al*., Principles on Deprivation of Nationality as a National Security Measure.

déplacées dans le contexte de la pandémie de COVID-19[173], qui énoncent les obligations incombant actuellement aux États, notamment en matière d'égalité et de non-discrimination, pour garantir les droits humains des migrants, des réfugiés, des apatrides et des groupes apparentés.

57. **Les États doivent adopter et renforcer des approches juridiques et politiques fondées sur les droits de l'homme en matière d'égalité raciale et de non-discrimination s'agissant de l'utilisation des technologies numériques dans l'administration et la police des frontières et de l'immigration. Il n'existe actuellement aucun cadre réglementaire intégré de gouvernance mondiale régissant l'utilisation des technologies automatisées et d'autres technologies numériques, ce qui rend plus essentielles que jamais les obligations juridiques internationales existantes en matière de droits humains dans la réglementation de la conception et de l'utilisation de ces technologies.**

58. **Au niveau tant national qu'international, les États Membres doivent veiller à ce que l'administration et la police des frontières et de l'immigration soient soumises à des obligations juridiques contraignantes visant à prévenir et combattre la discrimination raciale et xénophobe dans la conception et l'utilisation des technologies frontalières numériques, et à y remédier. Ces obligations comprennent (sans s'y limiter) :**

a) l'adoption rapide de mesures efficaces visant à prévenir et atténuer les risques de discrimination raciale dans la conception et l'utilisation des nouvelles technologies numériques, notamment en exigeant que les autorités publiques mènent des études d'impact sur l'égalité raciale et la non-discrimination préalablement à l'adoption de systèmes reposant sur ces technologies. Des représentants de minorités raciales ou ethniques, y compris des réfugiés, des migrants, des personnes apatrides et des membres de groupes apparentés, devront pouvoir être associés de façon effective à ces études, tant au stade de la mise au point qu'au stade de l'exécution. En outre, les études en question ne pourront être purement facultatives, ni même essentiellement facultatives ; il est primordial qu'elles soient obligatoires.

b) l'imposition d'un moratoire immédiat sur l'acquisition, la vente, le transfert et l'utilisation de technologies de surveillance, jusqu'à ce que de solides garanties en matière de droits humains soient mises en place pour réglementer ces pratiques. Ces garanties comprennent une diligence raisonnable en matière de droits humains qui respecte les interdictions du droit international relatif aux droits de l'homme concernant la discrimination raciale, un mécanisme de contrôle indépendant, des lois strictes sur la protection de la vie privée et des données, et une transparence totale concernant l'utilisation d'outils de surveillance tels que l'enregistrement d'images et la reconnaissance faciale. Dans certains cas, il sera nécessaire d'imposer l'interdiction catégorique de technologies qui ne peuvent pas répondre aux normes inscrites dans les cadres juridiques internationaux des droits humains interdisant la discrimination raciale ;

c) la mise en place de garanties de transparence et de responsabilité effective s'agissant de l'utilisation des technologies frontalières numériques par les secteurs privé et public, et l'autorisation d'analyses et de vérifications indépendantes faisant appel uniquement à des systèmes pouvant faire l'objet d'un contrôle ;

---

[173] Zolberg Institute on Migration and Mobility *et al.*, « Mobilité des personnes et droits humains dans le contexte de la pandémie de COVID-19 : Principes de protection des migrant-e-s, des réfugié-e-s et des autres personnes déplacées » (2020).

d) l'imposition aux entreprises privées d'obligations légales visant à prévenir et à combattre la discrimination raciale et xénophobe occasionnée par les technologies frontalières numériques, et à remédier à la situation, le cas échéant ;

e) la mise en place de mesures pour faire en sorte que les partenariats public-privé relatifs à la fourniture et à l'utilisation des technologies frontalières numériques soient transparents et soumis à un contrôle indépendant en matière de droits humains et pour éviter que l'État abdique ses responsabilités en matière de droits humains.

59. **La Rapporteuse spéciale a eu l'occasion de s'entretenir avec des représentants du HCR et de l'OIM au sujet de leur utilisation des différentes technologies frontalières numériques. Sur la base de ces consultations, elle recommande que les deux organismes adoptent et mettent en œuvre des mécanismes favorisant, de manière durable et authentique, la participation et la prise de décision des migrants, des réfugiés et des apatrides concernant l'adoption, l'utilisation et la révision des technologies numériques aux frontières. Elle a formulé les recommandations ci-après :**

60. **L'OIM devrait :**

a) intégrer et renforcer les obligations et principes internationaux en matière de droits humains, notamment en ce qui concerne l'égalité et la non-discrimination dans l'utilisation et le contrôle des technologies frontalières numériques, y compris dans tous ses partenariats avec des entités privées ou publiques. Pour ce faire, il convient de ne pas se limiter aux questions de protection de la vie privée liées au partage et à la protection des données, mais d'exiger plutôt que de recommander des mesures de protection en matière d'égalité et de non-discrimination ;

b) mettre en place des politiques et des pratiques obligatoires pour l'analyse systémique des impacts potentiellement nuisibles et discriminatoires des technologies frontalières numériques avant d'adopter ces technologies, et interdire l'adoption de technologies dont il ne peut être démontré qu'elles répondent aux exigences d'égalité et de non-discrimination ; fournir également des lignes directrices plus claires et plus concrètes, fondées sur les droits humains, concernant les critères de désignation des technologies numériques « option zéro », et veiller à ce que ces directives soient appliquées ;

c) adopter des protocoles obligatoires d'évaluation continue des droits humains pour les technologies frontalières numériques une fois qu'elles ont été déployées ;

d) créer des mécanismes de contrôle indépendant en matière de droits humains concernant l'utilisation par l'OIM des technologies frontalières numériques et mettre en œuvre des réformes visant à rendre plus transparente la manière dont les décisions sont prises concernant l'adoption de ces technologies ;

e) fournir aux migrants, réfugiés, apatrides et groupes apparentés des mécanismes obligeant l'OIM à répondre directement des violations de leurs droits humains du fait de l'utilisation des technologies numériques aux frontières.

61. **Comparativement à l'OIM, le HCR a pris des mesures plus poussées pour intégrer les normes d'égalité et de non-discrimination dans ses cadres d'orientation relatifs aux technologies frontalières numériques, mais il lui reste encore beaucoup à faire pour garantir que ces normes soient appliquées dans le**

cadre de ses activités. À cet égard, la Rapporteuse spéciale formule les recommandations ci-dessous.

62. **Le HCR devrait :**

a) mettre en place des politiques et des pratiques obligatoires pour l'analyse systémique des conséquences nuisibles et discriminatoires possibles des technologies frontalières numériques avant d'adopter ces technologies, et interdire l'adoption de technologies dont il ne peut être démontré qu'elles répondent aux exigences d'égalité et de non-discrimination ; fournir également des lignes directrices plus claires et plus concrètes, fondées sur les droits humains, concernant les critères de désignation des technologies numériques « option zéro », et veiller à ce que ces directives soient appliquées ;

b) adopter des protocoles obligatoires d'évaluation continue des droits humains pour les technologies frontalières numériques une fois qu'elles ont été déployées ;

c) créer des mécanismes de contrôle indépendant en matière de droits humains concernant l'utilisation par l'OIM des technologies frontalières numériques et mettre en œuvre des réformes visant à rendre plus transparente la manière dont les décisions sont prises concernant l'adoption de ces technologies ;

d) fournir aux migrants, réfugiés, apatrides et groupes apparentés des mécanismes obligeant l'OIM à répondre directement des violations de leurs droits humains découlant de l'utilisation des technologies numériques aux frontières.

63. **Tous les organismes humanitaires et apparentés des Nations Unies devraient mettre en œuvre les recommandations énoncées ci-dessus à l'intention de l'OIM et du HCR.**