United Nations A/75/590

General Assembly

Distr.: General
10 November 2020

Original: English

Seventy-fifth session
Agenda item 70 (b)
Elimination of racism, racial discrimination, xenophobia and related intolerance: comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action

Contemporary forms of racism, racial discrimination, xenophobia and related intolerance*

Note by the Secretary-General

The Secretariat has the honour to transmit to the General Assembly the report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, prepared pursuant to General Assembly resolution 74/137.

* The present report was submitted after the deadline owing to circumstances beyond the submitter's control.

Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance

Summary

Governments and United Nations agencies are developing and using emerging digital technologies in ways that are uniquely experimental, dangerous and discriminatory in the border and immigration enforcement context. By so doing, they are subjecting refugees, migrants, stateless persons and others to human rights violations, and extracting large quantities of data from them on exploitative terms that strip these groups of fundamental human agency and dignity.

The present report highlights how digital technologies are being deployed to advance the xenophobic and racially discriminatory ideologies that have become so prevalent, in part due to widespread perceptions of refugees and migrants as per se threats to national security. In other cases, discrimination and exclusion occur in the absence of explicit animus, but as a result of the pursuit of bureaucratic and humanitarian efficiency without the necessary human rights safeguards. The report also notes that vast economic profits associated with border securitization and digitization are a significant part of the problem.

Contents

I. Introduction

1. The present report continues the analysis initiated by the Special Rapporteur in her most recent report to the Human Rights Council, entitled "Racial discrimination and emerging digital technologies: a human rights analysis".[1] In that report, the Special Rapporteur introduced an equality-based approach to human rights governance of emerging digital technologies, with a focus on racial discrimination resulting from the design and use of these technologies. She urged State and non-State actors to move beyond "colour-blind" or "race-neutral" strategies that ignore the racialized and ethnic impact of emerging digital technologies, and instead to confront directly the intersectional forms of discrimination that result from and are exacerbated by the widespread adoption of these technologies. That report focused on those subject to discrimination primarily on the basis of race and ethnicity (including indigeneity), and drew attention to the effects of gender, religion, and disability status. The present report to the General Assembly brings additional nuance by focusing on the xenophobic and racially discriminatory impacts of emerging digital technologies on migrants, stateless persons, refugees and other non-citizens, as well as on nomadic and other peoples for whom migratory traditions are central. The term "refugees" includes asylum seekers who meet the refugee definition but whose status as refugees has not yet been formally recognized by any State.

2. Although emerging digital technologies are now prevalent in the governance of all aspects of society, unique concerns exist in the border and immigration context for at least two reasons. Under most if not all national governance frameworks:

(a) Non-citizens, stateless persons and related groups have fewer rights and legal protections from abuse of State power, and may be the targets of unique forms of xenophobic private violence;

(b) Executive and other branches of government retain expansive discretionary, unreviewable powers in the realm of border and immigration enforcement that are not subject to the typical substantive and procedural constraints, constitutionally and otherwise guaranteed to citizens.

3. As highlighted in the present report, governments and non-State actors are developing and deploying emerging digital technologies in ways that are uniquely experimental, dangerous and discriminatory in the border and immigration enforcement context. By so doing, they are subjecting refugees, migrants, stateless persons and others to human rights violations, and extracting large quantities of data from them on exploitative terms that strip these groups of fundamental human agency and dignity. Although the focus of the present report is relatively recent technological innovations, many of these technologies have historical antecedents in colonial technologies of racialized governance, including through migration controls. Not only is technology not neutral, but its design and use typically reinforce dominant social, political and economic trends. As highlighted in previous reports, the resurgence of ethnonationalist populism globally has had serious xenophobic and racially discriminatory consequences for refugees, migrants and stateless persons.[2] The present report highlights how digital technologies are being deployed to advance the xenophobic and racially discriminatory ideologies that have become so prevalent, in part due to widespread perceptions of refugees and migrants as per se threats to national security. In other cases, discrimination and exclusion occur in the absence of explicit animus, but as a result of the pursuit of bureaucratic and humanitarian efficiency without the necessary human rights safeguards. The report also highlights

[1] A/HRC/44/57.

[2] See, for example, A/73/312.

how ongoing securitization of borders, and related massive economic profits, are a significant part of the problem.

4. Refugees, migrants and stateless persons are subject to the violations enumerated in the present report on account of their national origin, race, ethnicity and religion and other impermissible grounds. These violations cannot be dismissed as permissible distinctions between citizens and non-citizens. In this regard, the Special Rapporteur calls attention to her prior report on racial discrimination on the basis of citizenship, nationality and immigration status, in which she highlights discriminatory trends and the application of international human rights law where such violations are concerned.[3]

5. Many of the same factors highlighted in the Special Rapporteur's report to the Human Rights Council[4] are essential background for the present report, and she recommends that the present report be read in conjunction with that prior report. Her prior report is especially helpful, among other reasons, for explaining the mechanisms that cause racial discrimination through emerging digital technologies, and for highlighting the economic, political and other societal forces driving the expansion in the discriminatory use of these technologies. Here, she reiterates that, notwithstanding widespread perceptions of emerging digital technologies as neutral and objective in their operation, race, ethnicity, national origin and citizenship status shape access to and enjoyment of human rights in all of the fields in which these technologies are now pervasive. States have obligations to prevent, combat and remediate this racial discrimination, and private actors, such as corporations, have related responsibilities to do the same. In the context of border and immigration enforcement (as in other contexts), preventing human rights violations may require outright bans or abolition of technologies due to a failure to control or mitigate their effects.

6. In the preparation of the report, the Special Rapporteur benefited from valuable input from: expert group meetings hosted by the Promise Institute for Human Rights at the University of California, Los Angeles (UCLA) School of Law, the UCLA Center for Critical Internet Inquiry, the Institute on Statelessness and Inclusion, and the Migration and Technology Monitor; interviews with researchers, including stateless persons, migrants and refugees; and submissions received from a range of stakeholders in response to a public call for submissions. Non-confidential submissions will be available on the webpage of the mandate.

II. The rise of digital borders

7. Technology has always been a part of border and immigration enforcement, and instruments ranging from passports and even physical border walls are all properly understood as features of this technology. The specific focus of the present report is the growing prevalence of digital technologies in immigration and border enforcement, such that some commentators appropriately refer to the rise of "digital borders"[5] – which in the present report refers to borders whose infrastructure and processes increasingly rely on machine learning, automated algorithmic decision-making systems, predictive analytics and related digital technologies. These technologies are integrated into identification documents, facial recognition systems, ground sensors, aerial video surveillance drones, biometric databases, asylum

[3] A/HRC/38/52.

[4] A/HRC/44/57.

[5] See, for example, Dennis Broeders, "The new digital borders of Europe: EU databases and the surveillance of irregular migrants", *International Sociology*, vol. 22, No. 1 (January 2007), pp. 71–92.

decision-making processes and many other facets of border and immigration enforcement.

8. As a general matter, digital border technologies are reinforcing parallel border regimes that segregate the mobility and migration of different groups on the basis of national origin and class, among other things. Automated border controls are one example of these parallel border regimes in action. One submission offered the example of the introduction of "eGates" at Irish ports of entry, such as Dublin Airport, where e-passport holders from the European Union/European Economic Area and Switzerland can go through eGates on a "self-service" basis to clear immigration control.[6] The submission notes that "only certain nationalities can adopt the 'self-service' approach, and the nationalities included are affluent and white nations (with the exception of Japan)". Non-nationals of the European Union/European Economic Area or Switzerland travelling from outside Ireland by air or sea must present themselves to an immigration officer upon arrival.

9. One facet of the digital border is the expansive use of biometrics or the "automated recognition of individuals based on their biological and behavioural characteristics".[7] Biometrics can include fingerprint data, retinal scans, and facial recognition, as well as less well-known methods such as the recognition of a person's vein and blood vessel patterns, ear shape, and gait, among others. Biometrics are used to establish, record and verify the identity of migrants and refugees. The United Nations, for example, has collected the biometric data of over 8 million people, most of them fleeing conflict or needing humanitarian assistance.[8] Researchers have documented the racialized origins of biometric technologies,[9] as well as their contemporary discriminatory operation on the basis of race, ethnicity and gender.[10] A recent report on facial recognition technology deployed in border crossing contexts, such as airports, notes that despite the fact that even the best algorithms misrecognize black women twenty times more often than white men, the use of these technologies is increasing globally.[11] As that report notes, "where facial recognition is applied as a gate-keeping technology, travellers are excluded from border control mechanisms on the basis of race, gender and other demographic characteristics (e.g. country of origin)". The frequent results of this differential treatment include perpetuation of negative stereotypes, and even prohibited discrimination which for asylum seekers might lead to refoulement.

10. Examples below show that governmental and humanitarian biometric data collection from refugees and migrants has been linked to severe human rights violations against these groups, notwithstanding the bureaucratic and humanitarian justifications behind the collection of this data. Furthermore, it is unclear what happens to this collected biometric data and whether affected groups have access to their own data. The World Food Programme (WFP), for example, has been criticized for partnering with data mining company Palantir Technologies for a $45 million contract, raising risks around data processing, security and responsibility regarding the 92 million aid recipients' data managed by WFP.[12] Private corporations such as

[6] Submission by the Immigrant Council of Ireland.

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

[8] These enormous data sets are notoriously hard to track and can also include the retrofitting of old data with newly collected biometrics. See, for example, http://humanitarian-congress-berlin.org/2018/.

[9] See, for example, Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Duke University Press, 2015).

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

[11] Tamir Israel, "Facial recognition at a crossroads: transformation at our borders and beyond" (September 2020).

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

Palantir have proved essential in providing the technology that supports the detention and deportation programmes run by United States Immigration and Customs Enforcement and the Department of Homeland Security,[13] raising justified concerns of corporate complicity in human rights violations associated with these programmes. It is not yet clear what data-sharing accountability mechanism will be in place during the World Food Programme–Palantir partnership or whether data subjects will be able to opt out.[14] Data collection is not an apolitical exercise, especially when powerful Global North actors collect information on vulnerable populations with no regulated methods of oversight and accountability.[15] The increasingly fervent collection of data on migrant populations has been criticized for its potential to cause significant privacy breaches and human rights concerns.[16]

11. History provides many examples of the discriminatory and even deadly use of data collection from marginalized groups. Nazi Germany strategically collected vast amounts of data on Jewish communities to facilitate the Holocaust, largely in partnership with a private corporation: IBM.[17] Other genocides also relied on systematic tracking of groups, such as the Tutsi registries based on ethnicity identity cards, which facilitated the magnitude of the Rwandan genocide in 1994.[18] Post 9–11, the United States experimented with various modes of data collection on marginalized populations through the Department of Homeland Security's National Security Entry-Exit Registration System, which collected photographs, biometrics, and even first-person interview data from over 84,000 flagged individuals coming from mostly Arab States.[19] In all of these cases, different actors, including governments, exploited ideas about the neutrality or non-prejudicial necessity of data collection from marginalized groups to then target those groups on a discriminatory basis.

12. Autonomous technologies are also increasingly used in monitoring and securing border spaces. For example, the European Border and Coast Guard Agency (Frontex) has been testing various unpiloted military-grade drones in the Mediterranean and Aegean Seas for the surveillance and interdiction of vessels of migrants and refugees hoping to reach European shores.[20] A joint investigation by Bellingcat, *Lighthouse Reports, Der Spiegel*, TV Asahi and Report Mainz produced credible evidence in October 2020 that Frontex had been complicit in pushbacks,[21] or the forced returns of refugees and migrants over a border without consideration of individual circumstances and without the possibility to apply for asylum or appeal. Such pushbacks likely violate non-refoulement obligations under international law, and are aided by surveillance technologies. One submission highlighted legal developments in Greece that permit the police to use drone surveillance to monitor irregular

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

[14] See 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 (May 2019), available at www.cigionline.org/publications/data-protection-and-digital-agency-refugees.

[16] See 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* (Dialog Press, 2012).

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

[19] See 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" (November 2020).

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

migration in border regions, but that do so without ensuring the requisite legal protections for the human rights of those subject to this surveillance.[22]

13. The usage of military, or quasi-military, autonomous technology bolsters the nexus between immigration, national security, and the increasing push towards the criminalization of migration and using risk-based taxonomies to demarcate and flag cases.[23] States, particularly those on the frontiers of large numbers of refugee and migrant arrivals, have been using various ways to pre-empt and deter those seeking to legally apply for asylum. This normative shift towards criminalization of asylum and migration works to justify increasingly hardline and intrusive technologies such as drones and various border enforcement mechanisms like remote sensors and integrated fixed towers with infrared cameras (so-called autonomous surveillance towers) to mitigate the "threat environment" at the border.[24] These technologies can have drastic results. While so-called "smart-border" technologies have been called a more humane alternative to other border enforcement regimes, studies have documented that such technologies along the United States-Mexico border, for example, have actually increased numbers of migrant deaths and pushed migration routes towards more dangerous terrains through the Arizona desert.[25] Samuel Chambers and others have found that migrant deaths have more than doubled since these new technologies have been introduced,[26] creating a "land of open graves".[27]

14. The use of these technologies by border enforcement authorities is only likely to increase in the "militarized technological regime"[28] of border spaces, without appropriate public consultation, accountability frameworks and oversight mechanisms. One submission provided an example of the Korean Peninsula's demilitarized zone where the Republic of Korea had deployed stationary, remote-operated semi-autonomous weapons.[29] The Government of the Republic of Korea stated that it had no intent to develop or acquire lethal autonomous weapons systems.[30] Due to a lack of transparency, often the status of autonomous weapons systems' deployment on borders is difficult to determine. In anticipation of such systems being under way, it is crucial that States account for and combat the disproportionate racial, ethnic and national origin impacts that fully autonomous weapons would have on vulnerable groups, especially refugees, migrants, asylum seekers, stateless persons, and related groups.

15. United Nations member States and numerous organs of the United Nations are increasingly relying on big data analytics to inform their policies. For example, the International Organization for Migration (IOM) Displacement Tracking Matrix[31] monitors populations on the move to better predict the needs of displaced people, using mobile phone call records and geotagging, as well as analyses of social media activity. In the United States of America, big data analytics are also being used to predict likely successful outcomes of resettled refugees based on pre-existing

[22] Submission by Homo Digitalis.
[23] Submission by 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), pp. 175–200.
[25] 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", *Journal of Borderlands Studies* (2019).
[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] Submission by Campaign to Stop Killer Robots.
[30] Ibid.
[31] See https://dtm.iom.int/about.

community links.[32] In an increasingly anti-immigrant global landscape, criticisms have surfaced that migration data has also been misinterpreted and misrepresented for political ends, for example to affect the distribution of aid. Inaccurate data can also be used to stoke fear and xenophobia, as seen in the characterization of the group of migrants attempting to claim asylum at the United States-Mexico border,[33] or the galvanization of anti-migrant sentiments in the Mediterranean area, including the recently proposed floating barrier walls.[34] Societal fear is then used to justify increasingly hardline responses that contravene international human rights law.[35] As one submission notes, in polarized, anti-immigrant and even xenophobic political contexts, "the data used to inform machine learning algorithms at borders or used in political campaigns or legislation can be flawed, and in an environment of structural bias against minorities such misrepresentation of data can fuel disinformation, hate speech and violence".[36]

16. Central to assessing the human rights landscape of digital borders is the role of private corporations whose pursuit of profit has played an important role in driving the expansion of digital technology in immigration and border enforcement, often in partnerships that allow governments to abdicate responsibility for violations that may result from the use of these technologies. The term "border industrial complex" has been used to describe "the nexus between border policing, militarization and financial interest",[37] as governments increasingly turn to the private sector to manage migration through new technologies predominately through a national security lens that neglects fundamental human rights.[38] Trends that fuel the border industrial complex include the externalization, militarization and automation of borders.[39] In the United States, the budget for border and immigration enforcement has increased by more than 6,000 per cent since 1980.[40] The European Union budget for the management of external borders, migration and asylum for 2021–2027 will increase by 2.6 times, amounting to more than €34.9 billion, compared to €13 billion for 2014–2020.[41] Recent market research reports project the compound annual growth rate for this global border security market to be between 7.2 and 8.6 per cent (US$65 to 68 billion) by 2025.[42]

17. Among the emerging digital technologies that drive the border industrial complex, drones that service border monitoring, and biometrics that help build "smart borders",[43] play a key role. The big corporate players and beneficiaries in the border monitoring service sector are largely Global North military companies, some of which, like Lockheed Martin, are the largest arms sellers in the world.[44] Information technology companies such as IBM are also major players, including in data gathering and processing roles.[45] Many of these corporate actors exert great influence in

[32] See https://news.stanford.edu/2018/01/18/algorithm-improves-integration-refugees/.
[33] Submission by the Center on Race, Inequality and the Law, at the New York University School of Law.
[34] See www.dezeen.com/2020/02/10/greece-floating-sea-border-wall-news/.
[35] See also Ana Beduschi, "International migration management in the age of artificial intelligence", *Migration Studies* (2020); and the submission from Ana Beduschi.
[36] Submission by Minority Rights Group International.
[37] See www.aljazeera.com/opinions/2019/11/1/why-climate-action-needs-to-target-the-border-industrial-complex/.
[38] Submission by Dhakshayini Sooriyakumaran and Brami Jegan.
[39] Ibid.
[40] Ibid.
[41] See https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4106.
[42] See www.issuewire.com/border-security-system-industry-projected-to-garner-usd-6781-billion-by-2025-flir-systems-lockhee-1631530966252699 and www.marketresearchfuture.com/reports/border-security-market-1662.
[43] Submission by Dhakshayini Sooriyakumaran and Brami Jegan.
[44] Ibid.
[45] Ibid.

domestic and international decision-making related to the governance of the digital border industry.[46] The "revolving door" between public office and private companies further tightens and blurs the line between government (border control, military) and industry (security and consulting companies).[47] Corporations are also linked with governments through joint ventures. According to one submission, for example, in 2016, French public-private company Civipol set up fingerprint databases for Mali and Senegal.[48] Financed with €53 million from the European Union Emergency Trust Fund for stability and addressing root causes of irregular migration and displaced persons in Africa, these projects are aimed at identifying refugees arriving in Europe from both countries and deporting them.[49] France owns 40 per cent of Civipol, while arms producers Airbus, Safran and Thales each own more than 10 per cent of the shares.[50] This further illustrates the manner in which Global North countries use international aid to advance their border agendas in the Global South.

18. One researcher has pointed out the pressing concern of the rise of "technocolonialism" which highlights "the constitutive role that data and digital innovation play in entrenching inequalities between refugees and humanitarian agencies and, ultimately, inequalities in the global context",[51] fuelled in part by corporate profit and government abdication of human rights responsibility. These inequalities are entrenched through forms of technological experimentation, data and value extraction, and direct and indirect forms of discrimination described in section III below.

19. In short, many digital border technologies substitute or aid human decision-making processes, sometimes in ways that raise serious human rights concerns. These technologies also expand the power and control that governments and private actors can exert over migrants, refugees, stateless persons and others, while simultaneously shielding this power from legal and judicial constraints. In other words, they magnify the potential for grave human rights abuses, and do so in ways that circumvent substantive and procedural protections that have otherwise been essential in the border enforcement context. Section III below highlights the range of discriminatory human rights violations enabled by digital border machinery and infrastructure, calling attention to these expansions of power and the contraction of constraints.

III. Mapping racial and xenophobic discrimination in digital border and immigration enforcement

A. Direct and indirect discrimination

1. Online platforms

20. Consultations with migrants, refugees and stateless persons highlighted the use of social media platforms such as Facebook, Twitter and WhatsApp to spread racist and xenophobic hatred, and some reported having been targeted directly through personal messages on these platforms. Participants in Malaysia, for example, reported

[46] Ibid., citing www.escr-net.org/corporateaccountability/corporatecapture.

[47] Submission by Dhakshayini Sooriyakumaran and Brami Jegan.

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

[49] Ibid., citing https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/eutf_2016_annual_report_final_en.pdf.

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

[51] Mirca Madianou, "Technocolonialism: digital innovation and data practices in the humanitarian response to refugee crises", *Social Media + Society* (April 2019).

the rise of racist and xenophobic advocacy on social media platforms in the wake of the coronavirus disease (COVID-19) pandemic. In some cases, users had posted photographs of migrants and refugees whom they perceived to be "illegal", raising serious concerns of subsequent real-world targeting of individuals, in addition to online abuse.

21. One submission called attention to an anonymously run blacklisting website, Canary Mission, that prejudicially targets students, professors and activists who have publicly advocated for Palestinian rights and disproportionately targets people of Arab descent. According to the submission, information published on Canary Mission has been used by Israeli immigration officials in the context of administration and enforcement of Israeli borders, and the borders of the occupied Palestinian territory, including to deny entry.[52] Such practices violate equality and non-discrimination rights, as well as freedom of expression protections, and leave those whose rights are violated with limited avenues of redress.

2. Racial profiling

22. Consultations with migrants, refugees and stateless persons also highlighted the role of digital technologies in racial and ethnic profiling in border enforcement. Participants raised concerns with ethnic profiling of Roma at the borders of North Macedonia. A 2017 case of racial profiling of Roma revealed that officials stored biometric data of individuals prevented from crossing these borders, on a "stop list".[53] Advocates raised valid concerns that these sorts of lists are disproportionately populated by Roma, who are subject to ethnic profiling and have limited means of challenging their presence on these lists.

3. Mandatory biometric data collection, digital identification systems, and exclusion from basic services

23. States are increasingly mandating extensive biometric data collection from non-citizens, where the collection and use of this data raise concerns of direct and indirect forms of discrimination on the basis of race, ethnicity, national origin, descent and even religion. As mentioned above, in most cases refugees, migrants and stateless persons have no control over how the data collected from them are shared. According to one submission, India requires mandatory biometric data collection from non-citizens, with a discriminatory use of this data being targeted detention and deportation even for refugees such as Rohingya.[54] Another concern raised in the context of India is the use of Aadhaar as de facto exclusion from vital basic services which rely on automated systems from which non-citizens are excluded entirely[55] Because refugees without residency permits are prohibited from holding Aadhaar cards, they are discriminated against and excluded from access to basic services and enjoyment of "rights that ensure a dignified refuge in India".[56] According to this submission, even refugee children have been denied primary education on the basis of not having Aadhaar.[57]

24. Regarding stateless persons in particular, participants in consultations reported that the expansion of digital identification systems was destroying the informal means of survival that these groups had developed in the absence of proper documentation

[52] Submission by Palestine Legal.
[53] See www.errc.org/uploads/upload_en/file/5209_file1_third-party-intervention-kham-delchevo-and-others-v-north-macedonia-5-february-2020.pdf.
[54] Submission by Anubhav Dutt Tiwari and Jessica Field.
[55] Ibid.
[56] Ibid.
[57] Ibid.

and recognition by the States in which they resided. Stateless persons, who are predominantly from racial and ethnic minorities, are systematically excluded from digital identity databases and documentation. Centralized biometric identification systems challenge the internationally recognized framework of nationality and citizenship in multiple ways. Key problems include algorithmic decision-making, and taking decisions on legal status out of the hands of government officials and placing them in the hands of machines or registrars administering biometric data kits. This can have the effect of de facto denaturalization without due process or safeguards. The same key considerations that must flow into every nationality deprivation decision, including non-discrimination, avoidance of statelessness, prohibition of arbitrariness, proportionality, necessity and legality,[58] must also be present when considering the introduction of centralized biometric identification systems. The introduction of digital governance structures risks deprivation of nationality by proxy measures, without due process – both intentionally and as a result of incomplete or flawed civil registration systems.[59] During consultations, participants from Kenyan Nubian and Somali communities, and Rohingya communities, for example, reported systematic difficulties securing digital identification, which then threatened their ability to access formal employment and other basic needs. In some cases, digital identification regimes seemed to exacerbate statelessness by resulting in complete exclusion and non-recognition of ethnic minority groups.

4. Language recognition

25. Although automated registration systems may be adopted for the purpose of enhancing bureaucratic efficiency, their technology can produce discriminatory outcomes. According to one submission, the Federal Office for Migration and Refugees, of Germany,[60] uses TraLitA, an automatic transliteration programme, to register Arabic names in the Latin alphabet. However, the system is more error-prone for applicants whose names originate from the Maghreb region, giving a success rate of 35 per cent in contrast to 85 to 90 per cent for names of Iraqi or Syrian applicants. Arabic-speaking applicants may also be subject to a dialect analysis upon registration. The Federal Office for Migration and Refugees uses software to analyse the applicant's spoken language sample to determine the plausibility of the stated national origin. This software relies on the Levantine dialect of Arabic,[61] and the submission raises the serious concern that the software's "susceptibility to errors has never been checked by a specialist supervisory control and cannot be understood by external actors with no recourse to the algorithms used".[62] The obvious risk is that speakers of Arabic dialects not represented by the software may erroneously be deemed non-credible, and therefore excluded from legal and other protections on a discriminatory basis.

5. Mobile data extraction and social media intelligence on migrant and refugee populations

26. Governments are increasingly targeting the electronic devices of migrants and refugees as a means to verify the information they provide to border and immigration authorities. Officials are able to do so using mobile extraction tools that download data from smartphones – including contacts, call data, text messages, stored files,

[58] Institute on Statelessness and Inclusion et al., Principles on Deprivation of Nationality as a National Security Measure (2020), available at https://files.institutesi.org/PRINCIPLES.pdf.
[59] Ibid., principle 10.
[60] Submission by Geselleschaft für Freiheitsrechte.
[61] Ibid.
[62] Ibid.

location information, and more.[63] In some cases, officials go so far as to deprive migrants and refugees of their personal devices. One submission reported that "intercepted migrants are regularly stripped of their belongings by Croatian authorities, particularly passports and other forms of ID, cell phones and power banks, and are summarily expelled to Bosnia and Herzegovina".[64]

27. In Austria, Belgium, Denmark, Germany, Norway and the United Kingdom of Great Britain and Northern Ireland, laws allow for the seizure of mobile phones from asylum or migration applicants, from which data are then extracted and used as part of asylum procedures.[65] These practices constitute a serious, disproportionate interference with migrants' and refugees' right to privacy, on the basis of immigration status and, in effect, national origin. Furthermore, the presumption that data obtained from digital devices necessarily leads to reliable evidence is flawed.[66] Governments have also resorted to social media intelligence – the techniques and technologies that allow companies or governments to monitor social media networking sites, such as Facebook or Twitter.[67] Some of these activities are undertaken directly by government officials themselves, but in some instances, governments call on companies to provide them with the tools and/or know-how to undertake this surveillance.[68]

28. One submission detailed concerning practices in Germany.[69] Pursuant to section 15 of the amended Asylum Act (Asylgesetz), asylum seekers unable to produce a valid passport or equivalent document must surrender all data carriers – not only mobile phones, but also laptops, USB sticks, and even fitness wristbands – along with login information to be "read out" by the Federal Office for Migration and Refugees to confirm identity or nationality.[70] The Law on Better Enforcement of the Obligation to Leave the Country (Gesetz zur besseren Durchsetzung der Ausreisepflicht) also empowers the Federal Office for Migration and Refugees to share the data with other government agencies, such as security authorities and intelligence services.[71] If determined necessary, the readout takes place before the asylum hearing upon the request of the Asylum Procedures Secretariat with the asylum applicant's signed consent,[72] although it is noted in the submission that applicants are "under exceptional pressure to follow governmental requests" for fear of negative consequences that could result from their asylum procedure.[73] This routine practice affected more than half of all first-time asylum applicants in the past two years,[74] and with regard to certain nationalities more than others raised serious concerns of de facto national origin discrimination.

29. This invasive data extraction from personal devices in Germany is unprecedented, and targets only asylum seekers, and the legalization of these measures was based on racist and xenophobic assumptions in political discourse.[75] The submission further emphasizes that data carrier evaluations have proven unsuitable to verify the identity or national origin of the asylum seeker with any degree of certainty, or to prevent abuse of asylum procedures.[76] Approximately a

[63] Ibid.; and submission by Privacy International et al.
[64] Submission by Border Violence Monitoring Network.
[65] Submission by Privacy International et al.
[66] Submission by Geselleschaft für Freiheitsrechte.
[67] Submission by Privacy International et al.
[68] Ibid.
[69] Submission by Geselleschaft für Freiheitsrechte.
[70] Ibid.
[71] Ibid.
[72] Ibid.
[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] Ibid.

quarter of attempted readouts fail technically, and even if readouts are successful, most of the evaluation reports are unusable because the set of data reviewed is too small or otherwise inconclusive.[77] Among 21,505 mobile phones successfully read out in 2018 and 2019, only about 118 cases, or 0.55 per cent, indicated a contradiction.[78] Furthermore, since neither the algorithms nor the training data are known to the public, judges and other decision makers cannot properly assess their reliability.[79]

30. Although regulations such as the European Union's General Data Protection Regulation seek to protect data and privacy, some States create exemptions in the immigration enforcement context. Two submissions noted relevant exemptions from the General Data Protection Regulation in the Data Protection Act 2018, of the United Kingdom.[80] Under this "immigration exemption", an entity with the power to process data, known as a "data controller", may circumvent core rights of an individual around data access if to do otherwise would "prejudice effective immigration control".[81] These rights include the rights to object to and restrict the processing of one's data and the right to have one's personal data deleted.[82] The exemption also frees data controllers from their responsibility to provide information to the individuals concerned when their data are collected, including from other sources, like a school, employer or local authority.[83] In the United Kingdom, the amended Police Act empowers not only police but also immigration officers to interfere with mobile phones and other electronic devices belonging to asylum seekers.[84] Going far beyond even the data carrier evaluation permitted in Germany, the Crime and Courts Act 2013, of the United Kingdom, enables police and immigration officers to carry out secret surveillance measures, place bugging devices, and hack and search mobile phones and computers.[85] The individuals affected will disproportionately be targeted on national origin grounds when national origin should never be a basis for diminished privacy and other rights.

B. Discriminatory structures

31. In her report to the Human Rights Council, the Special Rapporteur provided examples of how the design and use of different emerging digital technologies could be combined intentionally and unintentionally to produce racially discriminatory structures that holistically or systematically undermined enjoyment of human rights for certain groups, on account of their race, ethnicity or national origin, in combination with other characteristics. In other words, rather than only viewing emerging digital technologies as capable of undercutting access to and enjoyment of discrete human rights, she urged that they should also be understood as capable of creating and sustaining racial and ethnic exclusion in systemic or structural terms. In this subsection, the Special Rapporteur highlights ways in which migrants, refugees, stateless persons and related groups are being subjected to technological interventions that expose them to a broad range of actual and potential rights violations on the basis of actual or perceived national origin or immigration status.

[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Ibid.; and submission by Platform for International Cooperation on Undocumented Migrants.
[81] Submission by Platform for International Cooperation on Undocumented Migrants.
[82] Ibid.
[83] Ibid.
[84] Submission by Geselleschaft für Freiheitsrechte.
[85] Ibid.

1. Surveillance humanitarianism and surveillance asylum

32. Commentators have cautioned against the rise of "surveillance humanitarianism",[86] whereby increased reliance on digital technologies in service provision and other bureaucratic processes perversely results in the exclusion of refugees and asylum seekers from essential basic necessities such as access to food.[87] Surveillance humanitarianism refers to "enormous data collection systems deployed by aid organizations that inadvertently increase the vulnerability of people in urgent need".[88] Even a misspelled name can result in "bureaucratic chaos" and accusations of providing false information, slowing down what is already a slow asylum process.[89] Potential harms around data privacy are often latent and violent in conflict zones, where data compromised or leaked to a warring faction could result in retribution for those perceived to be on the wrong side of the conflict.[90]

33. In this regard, one submission highlights the dangers associated with the growing use by the Office of the United Nations High Commissioner for Refugees (UNHCR) of digital technologies to manage aid distribution.[91] In refugee camps in Afghanistan, UNHCR mandated iris registration for returning Afghan refugees as a prerequisite for receiving assistance.[92] Though UNHCR justifies collecting, digitizing and storing refugees' iris images in the Biometric Identity Management System as a means of detecting and preventing fraud,[93] the impact of processing such sensitive data can be grave when systems are flawed or abused.[94] It has also been documented that such biometric surveillance tools have led to system aversion and loss of access to goods and services for survival.[95] This submission noted, for example, the failure of technology in Rohingya refugee camps in Bangladesh, which resulted in the denial of food rations to refugees.[96]

34. Collection of vast amounts of data on migrants and refugees creates serious issues and possible human rights violations related to data sharing and access, particularly in settings such as refugee camps where power differentials between United Nations agencies, international non-governmental organizations and the affected communities are already stark. Although exchanging data on humanitarian crises or biometric identification is often presented as a way to increase efficiency and inter-agency and inter-State cooperation, benefits from the collection do not accrue equally. Data collection and the use of new technologies, particularly in contexts characterized by steep power differentials, raise issues of informed consent and the ability to opt out. In various forced migration and humanitarian aid settings, such as Mafraq, Jordan, biometric technologies are being used in the form of iris scanning in lieu of identity cards in exchange for food rations.[97] However, conditioning food access on data collection removes any semblance of choice or autonomy on the part of refugees – consent cannot freely be given where the

[86] See www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
[87] Submission by Ana Beduschi.
[88] See 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, April 2019).
[90] See www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
[91] Submission by Amnesty International.
[92] Ibid.
[93] Ibid.
[94] Ibid., citing A/HRC/39/29.
[95] Submission by 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). See also https://medium.com/unhcr-innovation-service/managing-risk-to-innovate-in-unhcr-91fe9294755b.

alternative is starvation. Indeed, an investigation in the Azraq refugee camp[98] revealed that most refugees interviewed were uncomfortable with such technological experiments but felt that they could not refuse if they wanted to eat. The goal or promise of improved service delivery cannot justify the levels of implicit coercion underlying regimes such as these.[99]

35. Consultations highlighted concerns among Rohingya refugees in Bangladesh and India that their data may be shared in ways that increased their risk of refoulement, or be shared with the Government of Myanmar, increasing their vulnerability to human rights violations in the event of forcible and other forms of return of these groups to their country of origin. A serious concern in this context is that of "function creep", where data collected in one context (e.g. monitoring low-level fraud) is shared and reused for different purposes (e.g. to populate registries of potential terror suspects),[100] with no procedural and substantive protections for the individuals whose data are being shared and repurposed.

36. In some cases, the very nature of data collection can produce profoundly discriminatory outcomes. Fleeing genocide in Myanmar, more than 742,000 stateless Rohingya refugees have crossed to Bangladesh since August 2017.[101] The UNHCR and Government of Bangladesh registration system did not offer "Rohingya" as an ethnic identity option, instead using "Myanmar nationals", a term that Myanmar does not recognize, and which does not capture the reality that Rohingya are stateless due to having been arbitrarily deprived of their right to nationality of Myanmar.[102] As one submission notes, categorization using this unrecognizable term on their digital identity cards amounts to a form of "symbolic annihilation of the Rohingya" required to carry and use these cards.[103]

37. Exclusion of refugees and asylum seekers from essential basic services through digital technology systems also occurs outside of refugee camp settings. One submission provides an example from Germany. In Germany, under the Asylum Seekers' Benefits Act, undocumented persons have the same right to health care as asylum seekers.[104] However, the social welfare office that administers health care for the undocumented has a duty to report their personal data to immigration authorities under section 87 of the Residence Act, which governs the "transfer of data and information for foreign authorities" by all public authorities.[105] This means that legally accessing health care may result in immigration enforcement, which likely has a chilling effect on migrant and refugees' use of even emergency health care.

2. Technological experimentation

38. Submissions received for the present report raise serious concerns with the widespread technological experimentation conducted by State and non-State actors on refugees, migrants and stateless persons. This experimentation involves testing of various technological products under circumstances where targeted groups have limited or no means of providing informed consent, and where the human rights consequences of the testing and experimentation are negative or unknown. Typically,

[98] See www.irinnews.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan.
[99] See www.unhcr.org/innovation/wp-content/uploads/2020/04/Space-and-imagination-rethinking-refugees%E2%80%99-digital-access_WEB042020.pdf; and Dragana Kaurin, "Data protection and digital agency for refugees".
[100] Submission by Mirca Madianou.
[101] See 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] Submission by Mirca Madianou.
[104] Submission by Platform for International Cooperation on Undocumented Migrants.
[105] Ibid.

refugees, migrants and stateless persons have no or very limited recourse for challenging this technological experimentation, and the human rights violations that may be associated with it. Furthermore, it is national origin and citizenship/immigration status that exposes refugees, migrants and stateless persons to this experimentation, raising serious concerns about discriminatory structures of vulnerability.

39. One submission drew attention to iBorderCtrl (the Intelligent Portable Border Control System), part of the European Union's Horizon 2020 Programme, which "aims to enable faster and thorough border control for third-country nationals crossing the land borders of European Union member States".[106] iBorderCtrl uses hardware and software technologies that seek to automate border surveillance.[107] Among its features, the system undertakes automated deception detection.[108] The European Union has piloted this lie detector at airports in Greece, Hungary and Latvia.[109] Reportedly, in 2019 iBorderCtrl was tested at the Serbian-Hungarian border and failed.[110] iBorderCtrl exemplifies the trend of experimenting surveillance and other technologies on asylum seekers, based on scientifically dubious grounds.[111] Drawing upon the contested theory of "affect recognition science", iBorderCtrl replaces human border guards with a facial recognition system that scans for facial anomalies while travellers answer a series of questions.[112] Other countries such as New Zealand are also experimenting with using automated facial recognition technology to identify so-called future "troublemakers", which has prompted civil society organizations to mount legal challenges on grounds of discrimination and racial profiling.[113]

40. States are currently experimenting with automating various facets of immigration and asylum decision-making. For example, since at least 2014, Canada has used some form of automated decision-making in its immigration and refugee system.[114] A 2018 University of Toronto report examined the human rights risks of using artificial intelligence (AI) to replace or augment immigration decisions, noting that these processes created a laboratory for high-risk experiments within an already highly discretionary and opaque system.[115] The ramifications of using automated decision-making in the immigration and refugee context are far-reaching. Although the Government of Canada has confirmed that this type of technology is confined only to augmenting human decision-making and is reserved for certain immigration applications only, there is no legal mechanism in place protecting non-citizens' procedural rights and preventing human rights abuses from occurring. Similar visa algorithms are currently in use in the United Kingdom and have been challenged in

[106] Submission by Privacy International et al.

[107] For general information about the project, see European Commission, "Smart lie-detection system to tighten EU's busy borders" (24 October 2018), available at https://ec.europa.eu/research/infocentre/. =49726.

[108] Submission by Privacy International et al.

[109] Submission by Maat for Peace, Development and Human Rights. See also Petra Molnar, "Technology on the margins: AI and global migration management from a human rights perspective" (2019); and submission by Minority Rights Group International.

[110] Submission by Privacy International et al.

[111] Ibid.

[112] Submission by Minority Rights Group International.

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

[114] Petra Molnar and Lex Gill, "Bots at the gate: a human rights analysis of automated decision-making in Canada's immigration and refugee system", Citizen Lab and International Human Rights Program, Faculty of Law, University of Toronto, Research Report No. 114 (September 2018).

[115] Ibid.

court for their discriminatory potential.[116] Canada, Switzerland and the United Kingdom also use automated or algorithmic decision-making "for selecting refugees and resettling them".[117] The introduction of new technologies impacts both the processes and outcomes associated with decisions that would otherwise be made by administrative tribunals, immigration officers, border agents, legal analysts and other officials responsible for the administration of immigration and refugee systems, border enforcement and refugee response management. There is a serious lack of clarity surrounding how courts will interpret administrative law principles such as natural justice, procedural fairness and standard of review where an automated decision system is concerned or where an opaque use of technology operates.

41. In some contexts, the nature of technological experimentation relates to the collection of genetic data, whose purposes are justified on tenuous grounds, but raise serious and concrete human rights concerns. One submission described the Combined DNA Index System (CODIS), a forensic DNA database in the United States through which individual states and the federal Government collect, store and share genetic information.[118] Since January 2020, the federal Government has been collecting DNA from any person in immigration custody.[119] What this means is that "for the first time, CODIS will warehouse the genetic data of people who have not been accused of any crime, for crime detection purposes", severing the long-standing prerequisite of prior alleged criminal conduct to compel DNA collection.[120] Non-citizens in immigration custody are not criminals as a rule.[121] In fact, the vast majority of immigration infractions for which an immigrant is detained are civil in nature.[122] As regards asylum seekers, who form an increasingly large proportion of the detained non-citizen population, both international and domestic laws expressly allow them to enter the United States to claim the right to refuge.[123] The submission rightly points out that the new immigration policy expanding CODIS moves the United States towards constructing a "genetic panopticon", whose purposes and effects may well be discriminatory. CODIS risks turning into a dystopian tool of genetic surveillance that will "encompass anyone within United States borders, including ordinary Americans neither convicted nor even suspected of criminal conduct", threatening democracy and human rights,[124] including on the basis of national origin.

42. As COVID-19 has further incentivized and legitimized surveillance and other technologies targeting refugees and migrants, these groups have been subjected to further experimentation.[125] One example is the experimental deployment of an immunity passport called "COVI-Pass" in West Africa.[126] A product of partnership between Mastercard and the Gavi Alliance, a private-public alliance for vaccination, this digital initiative combines biometrics, contact tracing, cashless payments, national identification and law enforcement.[127] Not only do such technologies operate outside human rights impact assessments and regulations, they also risk threatening

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

[117] Submission by Maat for Peace, Development and Human Rights; and submission by Ana Beduschi, citing Petra Molnar and Lex Gill, "Bots at the gate: a human rights analysis of automated decision-making in Canada's immigration and refugee system".

[118] Submission by Daniel I. Morales, Natalie Ram and Jessica L. Roberts.

[119] Ibid.

[120] Ibid.

[121] Ibid.

[122] Ibid.

[123] Ibid.

[124] Ibid.

[125] Submission by Amnesty International.

[126] Ibid.

[127] Ibid.

human rights, including freedom of movement, the right to privacy, the right to bodily autonomy and the right to equality and non-discrimination, especially for refugees and migrants.[128]

3. Border externalization

43. Border externalization – the extraterritorialization of national and regional borders to other geographic regions in order to prevent migrant and refugee arrivals – has become a standard border enforcement tool for many countries and regions. The human rights violations associated with border externalization are well documented.[129] Border externalization does not affect all nationality or national origin groups equally. It has a disproportionate impact on persons from Africa, Central and South America and South Asia, and in many regions is fuelled by racialized, xenophobic, ethnonationalist politics that seek to exclude certain national and ethnic groups from regions on discriminatory bases. States and regional blocs have increasingly relied on digital technologies to achieve this border externalization, thereby consolidating and expanding discriminatory, exclusionary regimes.

44. One submission highlighted the European Border Surveillance System (EUROSUR) as a programme that uses big data technologies to predict, control and monitor traffic across European Union borders.[130] It deploys surveillance drones in the Mediterranean Sea, in order to notify the Libyan coastguard to intercept refugee and migrant boats and return migrants to Libya.[131] Although the European Commission insists that the drones are only for civil surveillance purposes,[132] the Office of the United Nations High Commissioner for Human Rights has spoken out against coordinated pushbacks and failures to assist migrants and refugees in the Mediterranean, making it one of the deadliest migration routes in the world.[133] Surveillance technologies are essential for coordination in this context.

45. Another submission reported the participation of 13 European nations in the ROBORDER project, a "fully functional, autonomous border surveillance system".[134] ROBORDER consists of unpiloted mobile robots capable of functioning on a stand-alone basis or in swarms, in a range of environments – aerial, water surface, underwater, and ground.[135] This proposed increased use of drones to police Europe's borders exacerbates the decentralization of the border zone into various vertical and horizontal layers of surveillance, suspending State power from the skies, and extends the border visually and virtually, turning people into security objects and data points to be analysed, stored, collected and rendered intelligible.[136] The usage of military, or quasi-military, autonomous technology also bolsters the connection between immigration, national security, and the increasing push towards the criminalization of

[128] Ibid.

[129] See, for example, A/HRC/23/46, A/HRC/29/36 and A/72/335.

[130] Submission by Maat for Peace, Development and Human Rights, citing Btihaj Ajana, "Augmented borders: big data and the ethics of immigration control", *Journal of Information, Communication and Ethics in Society*, vol. 13, issue 1 (2015).

[131] Submission by Franciscans International, citing www.middleeastmonitor.com/20190819-eu-using-israel-drones-to-track-migrant-boats-in-the-med/.

[132] Submission by Franciscans International, citing www.europarl.europa.eu/doceo/document/E-9-2019-003257-ASW_EN.pdf.

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

[134] Submission by Homo Digitalis. See also https://roborder.eu/. The participating States are Belgium, Bulgaria, Estonia, Finland, Germany, Greece, Hungary, Italy, Portugal, Romania, Spain, Switzerland and the United Kingdom of Great Britain and Northern Ireland.

[135] Ibid.

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

migration and using risk-based taxonomies to demarcate and flag cases.[137] Globally, States, particularly those on the frontiers of large numbers of migrant arrivals, have been using various ways to pre-empt and deter those seeking to legally apply for asylum. This type of deterrence policy is very evident in Greece, Italy and Spain,[138] countries which are on the geographic frontiers of Europe, which increasingly rely on violent deterrence and "pushback" policies.

46. One submission highlighted the use by Croatia of European Union-funded technologies to detect, apprehend and return refugees and migrants along the Balkan route, travelling from Bosnia and Herzegovina and Serbia through Croatia to reach the Schengen border.[139] This submission alleges hundreds of human rights abuses in the past three years, including "illegal pushbacks" that reflect "inherently racist cleavages".[140] Surveillance technologies such as drones and helicopters with automated searchlights "have been weaponized against people on the move, making them easier to detect and thus compounding their vulnerability and the dangers they face".[141]

47. Discriminatory border externalization is also achieved through transnational biometric data-sharing programmes across multiple countries. One submission reported a biometric data-sharing programme between the Governments of Mexico and the United States.[142] As at August 2018, Mexico had deployed the United States-funded programme in all 52 migration processing stations.[143] This bilateral programme uses biometric data to screen detained migrants in Mexico who allegedly have tried to cross the United States border or are members of a criminal gang.[144] However, Mexico's National Institute of Migration has denied having processed biometric data in answer to freedom of access to information requests.[145]

4. Immigration surveillance[146]

48. One submission reported on the ongoing construction at the United States-Mexico border of "a network of 55 towers equipped with cameras, heat sensors, motion sensors, radar systems and a GPS system".[147] This border enforcement system also surveils the Tohono O'odham Nation reservation, located in Arizona approximately one mile from the border.[148] This "smart" border surveillance system replaces a prior one, which research showed had failed to prevent undocumented border crossings, but instead had shifted migrants' routes, thereby increasing their vulnerability to injury, isolation, dehydration, hyperthermia and exhaustion – and deaths.[149] Another submission notes that researchers and civil society organizations

[137] Submission by Dimitri van den Meerssche.

[138] See 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/ and www.efadrones.org/countries/italy/.

[139] Submission by Border Violence Monitoring Network.

[140] Ibid.

[141] Ibid.

[142] Submission by Privacy International et al.

[143] Ibid.

[144] Ibid.

[145] Ibid.

[146] Anil Kalhan, "Immigration surveillance", *Maryland Law Review*, vol. 74, No. 1 (2014) (defining immigration surveillance as the product of dramatically expanded identification, mobility tracking and control, and information-sharing, and evasion of the traditional substantive and procedural legal protections that have typically been relied upon to protect non-citizens from a host of human rights abuses).

[147] Submission by 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".

have opposed these border technologies because "they would exacerbate racial and ethnic inequality in policing and immigration enforcement, as well as curbing freedom of expression and the right to privacy".[150] Other submissions also highlighted the operation of other autonomous surveillance AI infrastructure at the United States-Mexico border, including drones designed to detect human presence and alert border enforcement officials.[151] The Committee on the Elimination of Racial Discrimination has expressed its concern to the General Assembly over the "ever more precarious journeys being taken by asylum seekers, refugees and migrants in search of safety and dignity resulting in unnecessary deaths and suffering".[152,153] As mentioned above, the current evidence is that so-called "smart" border technology forces these ever more precarious journeys, with a disproportionate impact on certain national origin, ethnic and racial groups.

49. In the United States, the communications of detained immigrants and their families and friends are surveilled.[154] The business model of the corporate providers of the technology is one whereby detained immigrants and their families "get convenience in the form of calls, video chats, voice mail messages, photo sharing and text messaging, while its real clients," immigration officials, get user data.[155] The web-based surveillance software, promoted as free to government officials with every installation, "includes call-pattern analysis, relationship analysis and tools for data visualization".[156]

50. Yet another facet of immigration surveillance involves social media screening. As of April 2019, the United States Department of State requires visa applicants to disclose their social media account information in the past five years from the time of application.[157] In September 2019, the Department of Homeland Security proposed to compel such disclosures from non-citizens already present and even residing in the country who apply for immigration benefits, including naturalization, permanent residence and asylum.[158] As the submission highlights, this expansive approach to social media screening is especially troubling because of United States immigration enforcement's demonstrated track record of utilizing social media information in a manner that disproportionately harms members of minority racial, ethnic and religious groups.[159] The Department of Homeland Security has already falsely accused black and Latinx youth of gang membership by exploiting social media connections, resulting in their detention, deportation, and/or denial of immigration benefits.[160] United States Immigration and Customs Enforcement, a constituent agency of the Department of Homeland Security, frequently combs social media to support gang membership allegations.[161] In one case, the Department of Homeland Security evidenced its allegation with a Facebook photo of the immigrant youth wearing a Chicago Bulls hat. The immigration court denied him bond and rejected both his application for asylum and for permanent residence, deporting him to a

[150] Submission by Minority Rights Group International.
[151] Submission by Mijente and submission by Iván Chaar-López.
[152] Submission by Franciscans International.
[153] See A/72/18.
[154] Submission by Mijente, citing www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.
[155] Ibid.
[156] Ibid.
[157] Submission by Harvard Immigration and Refugee Clinical Program.
[158] Ibid., citing www.govinfo.gov/content/pkg/FR-2019-09-04/pdf/2019-19021.pdf.
[159] Submission by Harvard Immigration and Refugee Clinical Program.
[160] Ibid., citing www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-20180521.pdf.
[161] Submission by Harvard Immigration and Refugee Clinical Program.

country where he feared for his life,[162] in violation of non-refoulement prohibitions under international law.

51. Moreover, social media screening has compounded the disproportionate risk affecting people belonging to or presumed to be of the Muslim faith or Arab descent "by creating an infrastructure rife with mistaken inference and guilt by association".[163] For example, in 2019, United States Customs and Border Protection, another constituent agency of the Department of Homeland Security, denied a Palestinian college student entry to the country based on his friends' Facebook posts expressing political views against the United States, even though he did not post such views of his own.[164] In addition to the direct burdens they place on non-citizens, the expanded social media disclosure requirements of the Government of the United States foreseeably affect freedoms of speech and association.

52. Homeland Security Investigations, the investigative arm of United States Immigration and Customs Enforcement, had already been testing automated social media profiling as early as 2016,[165] strengthening its open source social media exploitation capabilities for the purposes of scrutinizing visa applicants and visa holders before and after they arrived in the United States.[166] Submissions also raised concerns about consideration by the Government of the United States of technologies whose goal was "determinations via automation" regarding whether an individual applying for or holding a United States visa was likely to become a "positively contributing member of society" or intended "to commit criminal or terrorist attacks".[167] One submission noted in particular the use in the United States of risk assessments tools in immigration detention decisions, including one using an algorithm that was set to always recommend immigration detention, regardless of an individual's criminal history.[168] This example is one in which technology has been tailored to pursue punitive immigration enforcement measures rooted in the racist, xenophobic and ethnonationalist vision of immigration that has been advanced by the Administration of President Donald Trump.

53. All this points to a trend in immigration surveillance where predictive models use artificial intelligence to forecast whether people with no ties to criminal activity will nonetheless commit crimes in the future. Yet, these predictive models are prone to creating and reproducing racially discriminatory feedback loops.[169] Furthermore, racial bias is already present in the datasets on which these models rely.[170] When discriminatory datasets are treated as neutral inputs, they lead to inaccurate models of criminality which then "perpetuate racial inequality and contribute to the targeting and overpolicing of non-citizens".[171]

[162] Ibid.
[163] Ibid.
[164] Ibid.
[165] Submission by Mijente, citing 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] Submission by Mijente, citing www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.
[167] Ibid.
[168] Submission by Minority Rights Group International.
[169] Submission by Mijente.
[170] Ibid.
[171] Ibid.

IV. Recommendations

54. **In her report to the Human Rights Council, the Special Rapporteur provided States with a structural and intersectional human rights law approach to racial discrimination in the design and use of emerging digital technologies. The report explained the applicable international human rights obligations, highlighting:**

(a) **The scope of legally prohibited racial discrimination in the design and use of emerging digital technologies;**

(b) **Obligations to prevent and combat racial discrimination in the design and use of emerging digital technologies;**

(c) **Obligations to provide effective remedies for racial discrimination in the design and use of emerging digital technologies.**

55. **The Special Rapporteur explained the concepts and doctrines of direct, indirect and structural racial discrimination under international human rights law and outlined the obligations that these imposed on States with regard to emerging digital technologies. She noted that these obligations also had implications for non-State actors, including corporations, which in many respects exert more control over these technologies than States do. She reiterates her analysis and recommendations in that report and urges States to consider them alongside the recommendations included in the present report. The focus of this recommendations section is implementing the human rights equality and non-discrimination obligations highlighted in the Human Rights Council report in the specific context of border and immigration enforcement.**

56. **Member States must address the racist and xenophobic ideologies and structures that have increasingly shaped border and immigration enforcement and administration. The effects of technology are in significant part a product of the underlying social, political and economic forces driving the design and use of technology. Without a fundamental shift away from racist, xenophobic, anti-migrant, anti-stateless and anti-refugee political approaches to border governance, the discriminatory effects of digital borders highlighted in the present report cannot be redressed. States must comply with international human rights obligations to prevent racial discrimination in border and immigration enforcement and implement the recommendations provided in the report of the Special Rapporteur entitled "Racial discrimination and emerging digital technologies: a human rights analysis" (A/HRC/44/57). States should also follow the guidance provided by interventions such as the Principles on Deprivation of Nationality as a National Security Measure[172] and the Principles of Protection for Migrants, Refugees and Other Displaced Persons During COVID-19,[173] which articulate the existing obligations States have, including with respect to equality and non-discrimination, to ensure the human rights of migrants, refugees, stateless persons and related groups.**

57. **Member States must adopt and strengthen human rights-based racial equality and non-discrimination legal and policy approaches to the use of digital technologies in border and immigration enforcement and administration. There currently exists no integrated regulatory global governance framework for the use of automated and other digital technologies, which only raises the**

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

[173] Zolberg Institute on Migration and Mobility et al., Principles of Protection for Migrants, Refugees and Other Displaced Persons During COVID-19 (2020).

importance of existing international human rights legal obligations in the regulation of the design and use of these technologies.

58. **At both the domestic and international levels, Member States must ensure that border and immigration enforcement and administration are subject to binding legal obligations to prevent, combat and remedy racial and xenophobic discrimination in the design and use of digital border technologies. These obligations include but are not limited to:**

(a) **Swift and effective action to prevent and mitigate the risk of the racially discriminatory use and design of digital border technologies, including by making racial equality and non-discrimination human rights impact assessments a prerequisite for the adoption of systems before they can be publicly deployed. These impact assessments must incorporate meaningful opportunity for co-design and co-implementation with representatives of racially or ethnically marginalized groups, including refugees, migrants, stateless persons and related groups. A purely or even mainly voluntary approach to equality impact assessments will not suffice; a mandatory approach is essential;**

(b) **An immediate moratorium on the procurement, sale, transfer and use of surveillance technology, until robust human rights safeguards are in place to regulate such practices. These safeguards include human rights due diligence that complies with international human rights law prohibitions on racial discrimination, independent oversight, strict privacy and data protection laws, and full transparency about the use of surveillance tools such as image recordings and facial recognition technology. In some cases, it will be necessary to impose outright bans on technology that cannot meet the standards enshrined in international human rights legal frameworks prohibiting racial discrimination;**

(c) **Ensuring transparency and accountability for private and public sector use of digital border technologies, and enabling independent analysis and oversight, including by only using systems that are auditable;**

(d) **Imposing legal obligations on private corporations to prevent, combat and remedy racial and xenophobic discrimination due to digital border technologies;**

(e) **Ensuring that public-private partnerships in the provision and use of digital border technologies are transparent and subject to independent human rights oversight, and do not result in abdication of government accountability for human rights.**

59. **The Special Rapporteur had the opportunity to consult with representatives of UNHCR and IOM on their use of different digital border technologies. Based on those consultations, she recommends that both bodies adopt and implement mechanisms for sustained and meaningful participation and decision-making by migrants, refugees and stateless persons in the adoption, use and review of digital border technologies. She makes the recommendations set out below.**

60. **IOM should:**

(a) **Mainstream and strengthen international human rights obligations and principles, especially relating to equality and non-discrimination in its use and oversight of digital border technologies, including in all its partnerships with private and public entities. This requires moving beyond a narrow focus on privacy concerns relating to data sharing and data protection, and mandating rather than recommending equality and non-discrimination protections;**

(b) **Adopt mandatory policies and practices for systemic analysis of potential harmful and discriminatory impacts of digital border technologies prior to the adoption of these technologies, and prohibit adoption of technologies that cannot be shown to meet equality and non-discrimination requirements. Provide clearer, more concrete human rights-based guidelines on the criteria for the designation of "zero option" digital technologies, and ensure the implementation of these guidelines;**

(c) **Adopt mandatory ongoing human rights assessment protocols for digital border technologies once deployed;**

(d) **Create mechanisms for independent human rights oversight of use by IOM of digital border technologies and implement reforms to ensure greater transparency in how decisions are made to adopt these technologies;**

(e) **Provide migrants, refugees, stateless persons and related groups with mechanisms for holding IOM directly accountable for violations of their human rights resulting from the use of digital border technologies.**

61. **Relative to IOM, UNHCR has taken greater steps to engage with equality and non-discrimination norms in its guidance frameworks relating to digital border technologies, but it too has significant additional work to do to ensure that those norms are realized in its practice. In this regard, the Special Rapporteur makes the recommendations set out below.**

62. **UNHCR should:**

(a) **Adopt mandatory policies and practices for systemic analysis of potential harmful and discriminatory impacts of digital border technologies prior to the adoption of these technologies, and prohibit adoption of technologies that cannot be shown to meet equality and non-discrimination requirements. Provide clearer, more concrete human rights-based guidelines on the criteria for the designation of "zero option" digital technologies, and ensure the implementation of these guidelines;**

(b) **Adopt mandatory ongoing human rights assessment protocols for digital border technologies once deployed;**

(c) **Create mechanisms for independent human rights oversight of the use by UNHCR of digital border technologies and implement reforms to ensure greater transparency in how decisions are made to adopt these technologies;**

(d) **Provide migrants, refugees, stateless persons and related groups with mechanisms for holding UNHCR directly accountable for violations of their human rights resulting from the use of digital border technologies.**

63. **All United Nations humanitarian and related bodies should implement the recommendations above addressed to IOM and UNHCR.**