United Nations A/HRC/48/76

General Assembly

Distr.: General
17 December 2021

Original: English

Human Rights Council
Forty-eighth session
13 September–1 October 2021
Agenda item 9
Racism, racial discrimination, xenophobia and related forms of intolerance: follow-up to and implementation of the Durban Declaration and Programme of Action

Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement

Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume*

Summary

The present report complements the report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, submitted to the Human Rights Council at its forty-fourth session, entitled "Racial discrimination and emerging digital technologies: a human rights analysis". In the present report, the Special Rapporteur highlights how digital technologies are being deployed in the xenophobic and racially discriminatory treatment and exclusion of migrants, refugees and stateless persons. In some 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. Furthermore, the Special Rapporteur underscores that the vast economic profits associated with border securitization and digitization are a significant part of the problem.

* The present report was submitted after the deadline so as to include the most recent information.

Contents

I. Introduction

1. In the present report, the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, develops the analysis she initiated in the report she submitted to the Human Rights Council at its forty-fourth session, entitled "Racial discrimination and emerging digital technologies: a human rights analysis".[1] In that report, the Special Rapporteur introduced an equality-based approach to the human rights governance of emerging digital technologies, with a focus on the intersection of these technologies with racial equality and non-discrimination principles under international human rights law. She urged State and non-State actors to move beyond "colour-blind" or "race neutral" strategies, which 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. This approach further entails moving beyond the tendencies of human rights and regulatory frameworks to focus only on explicit prejudice in efforts to prohibit racial discrimination. In her previous report, the Special Rapporteur examined discrimination on the grounds of race, ethnicity and indigeneity, and drew attention to the effects of gender, religion and disability status. In the present report, she brings additional nuance by focusing on the xenophobic and racially discriminatory impacts of emerging digital technologies on migrants, stateless persons, refugees and non-citizens, as well as on nomadic and other peoples with migratory traditions. In this analysis, the term "refugees" includes asylum seekers who meet the refugee definition but whose status as refugees has not been formally recognized by any State. Furthermore, the Special Rapporteur addresses how the deployment of emerging digital technologies to contain the coronavirus disease (COVID-19) pandemic has accelerated these discriminatory trends.

2. Digital technologies now play a central role in mediating the enjoyment of fundamental rights, with States and private corporations relying upon these technologies to deliver essential goods and services.[2] Experts have usefully coined the term "digital borders"[3] to speak of borders whose infrastructure increasingly relies upon machine learning, big data, automated algorithmic decision-making systems, predictive analytics and related digital technologies. These technologies form part of identification documents and systems, facial recognition systems, ground sensors, aerial video surveillance drones, biometric databases and even visa and asylum decision-making processes. Recently, border and immigration enforcement has experienced accelerated digitization in response to the COVID-19 pandemic.

3. 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 targeted by 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 substantive and procedural constraints typically guaranteed to citizens.

4. Refugees, migrants and stateless persons are subject to the violations enumerated in the present report on account of their national origin, race, ethnicity, 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 report on racial discrimination in the context of laws, policies and practices concerning citizenship, nationality and immigration status.[4]

[1] A/HRC/44/57.

[2] See, e.g., A/74/493, A/73/348 and A/HRC/44/57.

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

[4] A/HRC/38/52.

5. Digital borders enhance the scope and precision of the racially discriminatory operation of borders. Governments and non-State actors are developing and deploying emerging digital technologies in ways that are uniquely experimental and dangerous 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 these groups on exploitative terms that strip them of fundamental human agency and dignity. Although the Special Rapporteur focuses in the present report on recent technological innovations, many of these technologies have historical antecedents in colonial technologies of racialized governance.

6. The analysis contained in the Special Rapporteur's previous report on racial discrimination and emerging digital technologies provides essential background information. That report is especially helpful for explaining the mechanisms that make it possible for emerging digital technologies to result in racial discrimination and for highlighting the economic, political and other societal forces driving the expansion of the discriminatory use of these technologies. In the present report, 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 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, preventing human rights violations may require outright bans on or the abolition of technologies due to a failure to control or mitigate their effects.

7. 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.[5] In the present report, the Special Rapporteur highlights how digital technologies are being deployed to advance the xenophobic and racially discriminatory ideologies that have proliferated in part due to widespread perceptions of refugees and migrants as per se threats to national security. In other cases, discrimination and exclusion occur not due to explicit animus, but because of the pursuit of bureaucratic and humanitarian efficiency without the necessary human rights safeguards. The ongoing securitization of borders and the related massive economic profits are a significant part of the problem.

8. The present report has benefited from the valuable contributions of experts at 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 are available online.[6]

II. Rise of digital borders

9. 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 examples of such technology. In the present report, the Special Rapporteur focuses specifically on the growing prevalence of digital technologies in border and immigration enforcement. The COVID-19 pandemic has accelerated this trend by encouraging the reliance on technological solutions to migration challenges. The "border industry" has begun advocating for "contactless biometrics" technology to combat the spread

[5] See, e.g., A/73/312.

[6] See https://www.ohchr.org/EN/Issues/Racism/SRRacism/Pages/CallRaceBordersDigitalTechnologies.aspx.

of the virus,[7] and public health and national security concerns are used to justify an increase in tracking and collecting data on migrants.[8]

10. In general, 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 grounds. Automated border controls are one example of parallel border regimes in action. At Irish ports of entry, such as Dublin airport, e-passport holders from the European Union, the European Economic Area and Switzerland can go through e-gates on a self-service basis to clear immigration control.[9] Only persons of certain nationalities – in other words, nationals of predominantly white, affluent countries (and of Japan) – can use the self-service option; others travelling to Ireland by air or sea must present themselves to an immigration officer upon arrival.

11. Digital borders make expansive use of biometrics, which is defined as the "automated recognition of individuals based on their biological and behavioural characteristics".[10] Biometrics can make use of fingerprints, retinal scans and facial recognition, as well as the recognition of a person's vein and blood vessel patterns, ear shapes and gait. Biometrics is used to establish, record and verify the identity of migrants and refugees. For example, the United Nations has collected the biometric data of over 8 million people, most of them fleeing conflict or needing humanitarian assistance.[11] Researchers have documented the racialized origins of biometric technologies,[12] as well as their contemporary use, which is discriminatory on the basis of race, ethnicity and gender.[13] In a report on facial recognition technology deployed in border crossing contexts such as airports, it has been noted that, although the best algorithms misrecognize Black women 20 times more often than they misrecognize White men, the use of these technologies is increasing globally.[14] Accordingly, "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)".[15] This differential treatment frequently perpetuates negative stereotypes and may even entail prohibited discrimination that could lead to refoulement.

12. 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 such data. Furthermore, it is unclear what happens to the data and whether affected groups have access to their own data. The World Food Programme (WFP), for example, has been criticized for concluding a $45 million contract with the data-mining company Palantir Technologies and for sharing data on 92 million aid recipients.[16] Private corporations such as Palantir have proved essential in providing the technology that supports the detention and deportation programmes run by the Immigration and Customs Enforcement of the United States Department of Homeland Security,[17] 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 put in place for the WFP-Palantir partnership or whether data subjects

[7] See https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf.

[8] See https://www.opendemocracy.net/en/pandemic-border/covid-19-can-technology-become-tool-oppression-and-surveillance/.

[9] Submission by the Immigrant Council of Ireland.

[10] See https://www.biometricsinstitute.org/what-is-biometrics/.

[11] These enormous data sets are notoriously hard to track and can also include the retrofitting of old data with newly collected data. See, e.g., youtube.com/watch?v=7qt4U7elpiA and youtube.com/watch?v=DgYs1scVHYM.

[12] See, e.g., Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Duke University Press, 2015).

[13] A/HRC/44/57.

[14] Tamir Israel, *Facial Recognition at a Crossroads: Transformation at our Borders and Beyond* (2020).

[15] Ibid., p. 158.

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

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

will be able to opt out.[18] Data collection is not an apolitical exercise, especially when powerful entities in the global North collect information on vulnerable populations without being subject to regulated methods of oversight and accountability.[19] The increasingly fervent collection of data on migrant populations has been criticized for its potential to lead to significant privacy breaches and human rights concerns.[20]

13. History provides many examples of the discriminatory and even deadly results of efforts to collect data on 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.[21] Other genocides too have relied on the systematic tracking of groups: the Rwandan genocide, for example, was facilitated by the registries of identity cards identifying Tutsis by ethnicity.[22] Since 11 September 2001, the United States of America has experimented with various modes of collecting data on marginalized populations, including photographs, biometric information and even first-person interviews in respect of over 84,000 flagged individuals coming from mostly Arab States.[23] In all of these cases, different actors, including Governments, have exploited ideas about the neutrality or non-prejudicial necessity of data collection to target marginalized groups on a discriminatory basis.

14. Autonomous technologies are also increasingly being used in monitoring and securing border spaces. For example, the European Border and Coast Guard Agency (Frontex), has been testing unpiloted military-grade drones in the Mediterranean and Aegean Seas for the surveillance and interdiction of vessels containing migrants and refugees hoping to reach European shores.[24] In October 2020, an investigation produced credible evidence that Frontex had been complicit in "pushbacks"[25] (i.e. the forced return of refugees and migrants over a border without consideration being given to the individuals' circumstances and without allowing them to apply for asylum or submit an appeal). It is likely that pushbacks violate the non-refoulement obligations of States under international law; yet, they are carried out with the aid of surveillance technologies. Legal developments in Greece have permitted the police to use drones to monitor irregular migration in border regions, but without ensuring the requisite legal protections for the human rights of the subjects of this surveillance.[26]

15. The use of military, or quasi-military, autonomous technology bolsters the nexus between immigration, national security, the increasing criminalization of migration and the use of risk-based taxonomies to demarcate and flag cases.[27] States, particularly those experiencing large numbers of refugee and migrant arrivals, have been using various methods to pre-empt and deter those seeking to legally apply for asylum. This normative shift towards the criminalization of asylum and migration works to justify increasingly hard-line 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.[28] These technologies can have drastic results. While so-called "smart-border" technologies have been called a more humane alternative to other border enforcement regimes, the use of such technologies along the United States-Mexico border have actually increased migrant deaths and pushed

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

[19] See https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees/.

[20] See https://www.chathamhouse.org/2018/03/beware-notion-better-data-lead-better-outcomes-refugees-and-migrants.

[21] Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, 2nd ed. (Dialog Press, 2012).

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

[23] See http://www.aaiusa.org/nseers.

[24] See https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf.

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

[26] Submission by Homo Digitalis.

[27] Submission by Dimitri Van Den Meerssche.

[28] 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.

migration routes towards more dangerous terrains.[29] In fact, migrant deaths have more than doubled since these new technologies have been introduced,[30] creating a "land of open graves".[31]

16. The use of these technologies by border enforcement agencies is only likely to increase in the "militarized technological regime"[32] of border spaces, without appropriate public consultation, accountability frameworks or oversight mechanisms. In the demilitarized zone on the Korean peninsula, the Republic of Korea has deployed stationary, remotely operated semi-autonomous weapons.[33] The Government of the Republic of Korea has stated that it has no intention to develop or acquire lethal autonomous weapons systems.[34] Due to a lack of transparency, however, the status of autonomous weapons systems' deployment on borders is often difficult to determine. Ahead of any such deployment, 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 and stateless persons.

17. Member States and entities of the United Nations are increasingly relying on big data analytics to inform their policies. For example, the Displacement Tracking Matrix of the International Organization for Migration (IOM)[35] monitors populations on the move to better predict the needs of displaced people, using mobile telephone records and geotagging, as well as analyses of social media activity. In the United States, big data analytics are also being used to predict the likelihood of a successful outcome for resettled refugees based on pre-existing community links.[36] In an increasingly anti-immigrant global landscape, criticisms have surfaced that migration-related 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[37] or the galvanization of anti-migrant sentiments in the Mediterranean region, including the recently proposed floating barrier walls.[38] Societal fear is then used to justify increasingly hard-line responses that contravene international human rights law.[39] As has been noted, 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.[40]

18. 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 border and immigration 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,[41] as Governments increasingly turn to the private sector to manage migration through new technologies, predominately

[29] Samuel Norton Chambers and others, "Mortality, surveillance and the tertiary 'funnel effect' on the US-Mexico border: a geospatial modeling of the geography of deterrence", *Journal of Borderland Studies*, vol. 36, No. 3 (2019), pp. 443–468.

[30] Ibid.

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

[32] Raluca Csernatoni, "Constructing the EU's high-tech borders".

[33] Submission by the Campaign to Stop Killer Robots.

[34] Ibid.

[35] See https://dtm.iom.int/about.

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

[37] Submission by the New York University School of Law Center on Race, Inequality and the Law.

[38] See https://www.dezeen.com/2020/02/10/greece-floating-sea-border-wall-news/.

[39] See, e.g., Ana Beduschi, "International migration management in the age of artificial intelligence", *Migration Studies* (2020). See also the submission by Ana Beduschi.

[40] Submission by Minority Rights Group International.

[41] See https://www.aljazeera.com/opinions/2019/11/1/why-climate-action-needs-to-target-the-border-industrial-complex/.

through a national security lens that neglects fundamental human rights.[42] The externalization, militarization and automation of borders fuel the border industrial-complex.[43] In the United States, the budget for border and immigration enforcement has increased by more than 6,000 per cent since 1980.[44] The European Union budget for the management of external borders, migration and asylum will increase by 2.6 times, amounting to more than 34.9 billion euros for the period 2021–2027 compared to 13 billion euros for the period 2014–2020.[45] Recent research estimates that the compound annual growth rate for this global border security market will reach 7.2–8.6 per cent (65–68 million United States dollars) in 2025.[46]

19. Among the emerging digital technologies that drive the border industrial complex and the creation of "smart borders", drones play a key role by monitoring borders and collecting biometric data.[47] The big corporate players and beneficiaries in the border monitoring service sector are largely military companies in the global North, some of which, like Lockheed Martin, are also among the largest arms sellers in the world.[48] Information technology companies such as IBM are also major players, including in data gathering and processing.[49] Many of these corporate actors exert great influence in domestic and international decision-making related to the governance of the digital border industry.[50] Corporations are also linked with Governments through joint ventures. For example, in 2016, the French public-private company Civipol set up databases of fingerprints in Mali and Senegal.[51] Financed with 53 million euros from the European Union Emergency Trust Fund for stability and addressing root causes of irregular migration and displaced persons in Africa, the project aims to identify refugees arriving in Europe from those two countries and to deport them.[52] France owns 40 per cent of Civipol, while arms producers Airbus, Safran and Thales each own more than 10 per cent of its shares.[53] This further illustrates the manner in which countries in the global North use international aid to advance their border agendas in the global South.

20. One researcher has highlighted the rise of "technocolonialism", highlighting that "technocolonialism shifts the attention to the constitutive role that data and digital innovation play in entrenching inequalities between refugees and humanitarian agencies and, ultimately, inequalities in the global context",[54] which are fuelled in part by corporate profit and Governments' abdication of their human rights responsibilities. These inequalities are entrenched through forms of technological experimentation, data and value extraction, and direct and indirect forms of discrimination (see sect. III below).

21. In short, many digital border technologies replace 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 context of border and immigration enforcement. Section III highlights the range of discriminatory human rights violations enabled by digital border machinery and infrastructure.

[42] Submission by Dhakshayini Sooriyakumaran and Brami Jegan.
[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] Mirca Madianou, "Technocolonialism: digital innovation and data practices in the humanitarian response to the refugee crisis", *Social Media + Society* (2019).

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

A. Direct and indirect discrimination

1. Online platforms

22. Migrants, refugees and stateless persons have reported that social media platforms such as Facebook, Twitter and WhatsApp are often used to spread racist and xenophobic hatred, and some have reported being targeted directly through personal messages posted on these platforms. In Malaysia, for example, migrants reported increasing racist and xenophobic advocacy on social media platforms during the COVID-19 pandemic. In some cases, users posted photographs of migrants and refugees they perceived to be "illegal", raising serious concerns that this would encourage the subsequent targeting of individuals both in the real world and online.

23. One anonymously-run blacklisting website, Canary Mission, prejudicially identifies students, professors and activists who have publicly advocated in favour of Palestinian rights, primarily targeting people of Arab descent. It has been reported that information published on Canary Mission has been used by Israeli immigration officials in the context of the administration and enforcement of the borders of Israel and the occupied Palestinian territory, including to deny entry.[55] Such practices violate the rights to equality and non-discrimination, as well as to freedom of expression, and leave those whose rights have been violated with limited avenues for redress.

2. Racial profiling

24. Consultations with migrants, refugees and stateless persons also highlighted the role of digital technologies in racial and ethnic profiling in border enforcement. In November 2020, the Committee on the Elimination of Racial Discrimination adopted its general recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials, in which the Committee recognized that migrants, refugees, asylum seekers, people of African descent, indigenous peoples and national and ethnic minorities, including Roma, are the groups most vulnerable to racial profiling. In the same general recommendation, the Committee also observed that the increasing use of new technological tools, including artificial intelligence, in areas such as security, border control and access to social services, has the potential to deepen racism, racial discrimination, xenophobia and other forms of exclusion.

25. In consultations, participants raised concerns about the ethnic profiling of Roma at the borders of North Macedonia. In 2017, it was revealed that officials stored the biometric data of individuals prevented from crossing that borders on a "stop list".[56] Advocates have raised valid concerns that these sorts of lists are disproportionately populated by Roma individuals, who are subject to ethnic profiling and have limited means of redress.

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

26. States are increasingly mandating extensive biometric data collection from non-citizens. The collection and use of such data raise concerns of direct and indirect forms of discrimination on the basis of race, ethnicity, national origin, descent and religion. In most cases, refugees, migrants and stateless persons have no control over how their data are shared. India, for example, requires biometric data to be collected from non-citizens; that data is primarily used to make decisions about detention and deportation, including of Rohingya refugees.[57] Another concern raised in the context of India is the use of identification numbers

[55] Submission by Palestine Legal.

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

[57] Submission by Anubhav Dutt Tiwari and Jessica Field.

for the de facto exclusion of migrants from vital basic services, the provision of which relies on automated systems.[58] Because refugees without a residence permit are prohibited from holding the relevant identification documents, they are discriminated against, cannot gain access to basic services and are therefore denied enjoyment of rights that ensure a dignified refuge in India.[59] Even refugee children have reportedly been denied primary education because they do not have the appropriate document.[60]

27. The expansion of digital identification systems is destroying the informal means of survival that stateless persons have developed in the absence of proper documentation and recognition by the States in which they reside. Stateless persons, most of whom are members of 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, which means that decisions about legal status are no longer taken by government officials but, rather, by machines or registrars administering biometric data kits. This can result in de facto denaturalization without due process or safeguards. The key considerations that must guide every nationality deprivation decision – including non-discrimination, avoidance of statelessness, prohibition of arbitrariness, proportionality, necessity and legality[61] – must also be considered when introducing centralized biometric identification systems. The introduction of digital governance structures risks depriving individuals of a nationality by proxy, without due process, whether intentionally or as a result of incomplete or flawed civil registration systems.[62] Nubian and Rohingya communities have reported systematic difficulties in securing digital identification, which has in turn threatened their ability to gain formal employment and satisfy other basic requirements. In some cases, digital identification regimes seem to exacerbate statelessness by excluding and not recognizing ethnic minority groups.

4. Language recognition

28. Although automated registration systems may be adopted to enhance bureaucratic efficiency, their technology can produce discriminatory outcomes. The Federal Office for Migration and Refugees of Germany uses an automatic program to transliterate Arabic names into Latin script.[63] However, the system is more error-prone for applicants whose names originate from the Maghreb region, at a success rate of 35 per cent in contrast to the 85–90 per cent success rate for names of Iraqi or Syrian applicants. Arabic-speaking applicants may also be subjected to a dialect analysis upon registration. Furthermore, the Federal Office for Migration and Refugees uses software to analyse applicants' spoken language to determine the plausibility of their stated national origin. The software relies on the Levantine Arabic dialect,[64] raising serious concerns that the software's susceptibility to errors has never been checked by a specialist and cannot be understood by external actors with no recourse to the algorithms used.[65] The obvious risk is that speakers of Arabic dialects not represented by the software may erroneously be deemed not credible and may therefore be excluded from legal and other protections on a discriminatory basis.

5. Mobile data extraction and social media intelligence on migrants and refugees

29. Governments are increasingly targeting the electronic devices of migrants and refugees to verify the information they provide to border and immigration authorities. Officials are able to do so using tools that download data from smartphones, including contacts, call data, text messages, stored files and location information.[66] In some cases,

[58] Ibid.
[59] Ibid.
[60] Ibid.
[61] See https://files.institutesi.org/PRINCIPLES.pdf.
[62] Ibid., principle 10.
[63] Submission by Gesellschaft für Freiheitsrechte.
[64] Ibid.
[65] Ibid.
[66] Ibid. See also the joint submission by Privacy International and others.

officials go so far as to deprive migrants and refugees of their personal devices. It has been reported, for example, that intercepted migrants are regularly stripped by the Croatian authorities of their belongings, particularly their passports and other forms of identification, their mobile telephones and power banks, and are summarily expelled to Bosnia and Herzegovina.[67]

30. In Austria, Belgium, Denmark, Germany, Norway and the United Kingdom of Great Britain and Northern Ireland, laws allow for the seizure of mobile telephones from asylum seekers and migrants and for the use of the extracted data in asylum procedures.[68] 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.[69] Governments have also resorted to social media intelligence, the techniques and technologies that allow companies and Governments to monitor social media networking websites. [70] Some of these activities are undertaken directly by government officials themselves but, in some instances, Governments call upon companies to provide them with the tools and the know-how to undertake such surveillance.[71]

31. During the COVID-19 pandemic, the proliferation of contact-tracing applications has raised concerns that sharing information about areas with high concentrations of infections could reinforce the existing social stigmatization of disproportionately infected groups and communities, with a particular disparate impact on the basis of race, ethnicity, national origin and citizenship status.[72]

32. Concerns have been raised about practices regarding the seizure of digital data in Germany.[73] Pursuant to the amended Asylum Act, asylum seekers unable to produce a valid passport or equivalent document must surrender all data carriers, not only mobile telephones but also laptops, USB sticks and even fitness wristbands, along with the relevant login information, which is then read out by the Federal Office for Migration and Refugees to confirm identity or nationality.[74] The Act also empowers the Federal Office to share the data with other government agencies, such as security authorities and intelligence services.[75] If deemed necessary, the information is read out before the asylum hearing, upon request by the Secretariat for the Digitalization of the Asylum Procedure and with the asylum applicant's signed consent,[76] even though it is recognized that applicants are under exceptional pressure to follow governmental requests, as they fear that not doing so would have negative consequences for their request for asylum.[77] This routine practice has affected more than half of all first-time asylum applicants during the past two years,[78] and certain nationalities more than others, raising serious concerns of de facto discrimination on the basis of national origin.

33. This invasive data extraction from personal devices is unprecedented, targets only asylum seekers and is justified by racist and xenophobic political discourse.[79] Furthermore, evaluations of data carriers have proved that the extracted data are unsuitable for the purposes of verifying the identity or national origin of asylum seekers with any degree of certainty or of preventing abuse of the asylum procedures.[80] Approximately a quarter of attempts to read out the extracted data fail technically; even when they are successful, most of the evaluation

[67] Submission by the Border Violence Monitoring Network.
[68] Joint submission by Privacy International and others.
[69] Submission by Gesellschaft für Freiheitsrechte.
[70] Joint submission by Privacy International and others.
[71] Ibid.
[72] See https://policyoptions.irpp.org/magazines/april-2020/five-ways-a-covid-19-contact-tracing-app-could-make-things-worse/.
[73] Submission by Gesellschaft für Freiheitsrechte.
[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Ibid.

reports are unusable because the set of data reviewed is too small or otherwise inconclusive.[81] Of the 21,505 mobile telephones from which data were extracted and successfully read out in 2018 and 2019, only about 118, or 0.55 per cent, indicated a matter of concern.[82] Furthermore, since neither the algorithms used nor training information are known to the public, judges and other decision makers cannot properly assess the reliability of the data collected from mobile telephones.[83]

34. Although regulations such as the General Data Protection Regulation[84] seek to protect data and privacy, some States create exemptions in the immigration enforcement context, as illustrated by the United Kingdom Data Protection Act of 2018.[85] Under the Act, an entity with the power to process data, known as a "data controller", may circumvent the obligation to respect an individual's core rights on data access if upholding those rights would prejudice effective immigration control.[86] 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.[87] The United Kingdom amended Police Act empowers not only police officers but also immigration officers to interfere with mobile telephones and other electronic devices belonging to asylum seekers.[88] Going far beyond what is permitted in Germany, the United Kingdom Crime and Courts Act of 2013 enables police and immigration officers to take secret surveillance measures, place bugging devices and hack and search mobile telephones and computers.[89] It is likely that the individuals affected will be disproportionately targeted on the grounds of their national origin, when national origin should never be a basis for diminished privacy and other rights.

B. Discriminatory structures

35. The Special Rapporteur has already shown how the design and use of different emerging digital technologies can produce racially discriminatory structures that undermine the enjoyment of human rights by certain groups on account of their race, ethnicity or national origin, in combination with other characteristics. She has called for emerging digital technologies to be understood as capable of creating and sustaining racial and ethnic exclusion in systemic or structural terms.[90] The Special Rapporteur now 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.

1. Surveillance humanitarianism and surveillance asylum

36. Commentators have cautioned about the rise of "surveillance humanitarianism",[91] whereby increased reliance on digital technologies in service provision and other bureaucratic processes perversely result in the exclusion of refugees and asylum seekers from gaining access to essential basic necessities such as food.[92] Even a misspelled name can result in bureaucratic chaos and in accusations of providing false information, slowing down further the asylum process.[93] The potential harms linked to breaches of data privacy are often latent;

[81] Ibid.
[82] Ibid.
[83] Ibid.
[84] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[85] Submissions by Gesellschaft für Freiheitsrechte and the Platform for International Cooperation on Undocumented Migrants.
[86] Submission by the Platform for International Cooperation on Undocumented Migrants.
[87] Ibid.
[88] Submission by Gesellschaft für Freiheitsrechte.
[89] Ibid.
[90] A/HRC/44/57, para. 38.
[91] See https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.
[92] Submission by Ana Beduschi.
[93] Mark Latonero and others, "Digital identity in the migration and refugee context: Italy case study", *Data and Society* (April 2019).

in conflict zones, they may flare up into violence, as the leaking of data to one of the warring factions could result in retribution against those perceived to be on the wrong side of the conflict.[94]

37. In this regard, there are dangers associated with the growing use of digital technologies to manage aid distribution.[95] In refugee camps in Afghanistan, for example, returning Afghan refugees are reportedly required to have their irises registered in order to receive assistance.[96] Collecting, digitizing and storing information on refugees' irises can be problematic when systems are flawed or abused.[97] It has also been documented that such biometric surveillance tools have led to system aversion and loss of access to goods and services necessary for survival.[98] For example, the failure of technology in Rohingya refugee camps in Bangladesh has resulted in the denial of food rations to refugees.[99] The Office of the United Nations High Commissioner for Refugees (UNHCR), in turn, has reported to the Special Rapporteur that its policy is that safeguards should be in place to ensure that refugees can gain access to assistance and protection services without the use of biometric technology, where necessary, and to address the risk of error or failure in its use.

38. The 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 there are stark power differentials between United Nations agencies, international non-governmental organizations and the affected communities. 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, not everyone benefits from the collection equally. Data collection and the use of new technologies, particularly in contexts characterized by marked power differentials, raise issues of informed consent and the ability to opt out. In various forced migration and humanitarian aid settings, such as in Mafraq, Jordan, biometric technologies are being used in the form of iris scanning in lieu of identity cards in exchange for food rations.[100] However, conditioning access to food on data collection removes any semblance of choice or autonomy on the part of refugees, as consent cannot be given freely when the alternative is starvation. Indeed, an investigation in the Azraq refugee camp[101] has revealed that most refugees interviewed were uncomfortable with such technological experiments but felt that they could not refuse them 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.[102]

39. Rohingya refugees in Bangladesh and India have expressed concern that their data may be shared in ways that increase their risk of refoulement, for example with the Government of Myanmar, increasing their vulnerability to human rights violations in the event of forcible and other forms of return to their country of origin. A serious concern in this context is that of "function creep", where data collected in one context (e.g. for monitoring low-level fraud) is shared and reused for different purposes (e.g. to populate registries of potential terror suspects),[103] with no procedural or substantive protections for the individuals whose data are being shared and repurposed. UNHCR says that it has not collected information that could be interpreted as consent to repatriation, and that it has secured consent from refugees to share their data with the Government of Myanmar in order to verify their right of return.

---

94 See https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.

95 Submission by Amnesty International.

96 Ibid.

97 Ibid., citing A/HRC/39/29.

98 Submission by Amnesty International.

99 Ibid.

100 See Fleur Johns, "Data, detection and the redistribution of the sensible in international law", *Cambridge University Press*, vol. 111, No. 1 (2017). See also https://medium.com/unhcr-innovation-service/managing-risk-to-innovate-in-unhcr-91fe9294755b.

101 See http://www.irinnews.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan.

102 See https://www.unhcr.org/innovation/wp-content/uploads/2020/04/Space-and-imagination-rethinking-refugees%E2%80%99-digital-access_WEB042020.pdf; https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees.

103 Submission by Mirca Madianou.

40. In some cases, the way in which data are collected can produce profoundly discriminatory outcomes. One example concerns the more than 742,000 stateless Rohingya refugees who fled genocide in Myanmar and arrived in Bangladesh between August 2017 and July 2019.[104] The registration system used by UNHCR and the Government of Bangladesh did not offer "Rohingya" as an ethnic identity option, only "Myanmar national", a term that Myanmar does not recognize and that does not capture the fact that Rohingya individuals are stateless because they have been arbitrarily deprived of their right to Myanmar nationality.[105] The categorization of individuals through the use of an unrecognizable term on digital identity cards amounts, in this case, to a form of symbolic annihilation of the Rohingya required to carry and use such cards.[106] UNHCR has reported that Rohingya refugees accepted this approach and were consulted on its adoption.

41. Refugees and asylum seekers are also excluded from gaining access to essential basic services through digital technology systems outside of refugee camps. For example, under the German Asylum Seekers' Benefit Act, although undocumented persons have the same right to health care as asylum seekers,[107] the social welfare office that administers health care for the undocumented has a duty – under section 87 of the Residence Act, which governs the transfer by all public authorities of data and information for foreign authorities – to report the personal data of such persons to the immigration authorities.[108] This means that legally accessing health care may result in the enforcement of immigration provision that are likely to have a chilling effect on migrants' and refugees' desire to use even emergency health care.

2. Technological experimentation

42. Serious concerns have been raised about the widespread technological experimentation conducted by State and non-State actors on refugees, migrants and stateless persons. This experimentation involves testing various technological products on groups with limited or no means of providing informed consent and without there being sufficient knowledge about the human rights consequences of such testing and experimentation. Furthermore, it is their national origin, citizenship and immigration status that exposes refugees, migrants and stateless persons to technological experimentation, raising serious concerns about discriminatory structures of vulnerability.

43. Another example is the European Union iBorderCtrl project, an "intelligent portable control system" that aims to enable faster and thorough border control for third country nationals crossing the land borders of European Union member States.[109] iBorderCtrl uses hardware and software technologies that seek to automate border surveillance,[110] including through automated deception detection.[111] The European Union has piloted this lie detector at airports in Greece, Hungary and Latvia.[112] Reportedly, in 2019 iBorderCtrl was tested at the Serbian-Hungarian border and failed.[113] iBorderCtrl exemplifies the trend of experimenting surveillance and other technologies on asylum seekers based on scientifically dubious grounds.[114] Drawing upon the contested discipline 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.[115] New Zealand too is experimenting with automated facial recognition technology in order to identify future

[104] See https://www.unhcr.org/en-us/rohingya-emergency.html.
[105] Mirca Madianou, "Technocolonialism".
[106] Submission by Mirca Madianou.
[107] Submission by the Platform for International Cooperation on Undocumented Migrants.
[108] Ibid.
[109] Joint submission by Privacy International and others. See also https://www.iborderctrl.eu/The-project.
[110] See https://www.iborderctrl.eu/The-project.
[111] Ibid. See also the joint submission by Privacy International and others.
[112] Submission by the Maat for Peace, Development and Human Rights Association. See also Petra Molnar, "Technology on the margins: AI and global migration management from a human rights perspective", *Cambridge International Law Journal*, vol. 8, No. 2 (2019); and the submission by Minority Rights Group International.
[113] Joint submission by Privacy International and others.
[114] Ibid.
[115] Submission by Minority Rights Group International.

"troublemakers", prompting civil society organizations to mount legal challenges on grounds of discrimination and racial profiling.[116] Canada and Romania have also experimented with similar "emotion recognition" projects for border screening.[117]

44. 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.[118] In 2018, it was found that these processes "create a laboratory for high-risk experiments within an already highly discretionary system".[119] 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 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 court for their discriminatory potential.[120] Canada, Switzerland and the United Kingdom also use automated or algorithmic decision-making for selecting and resettling refugees.[121] The introduction of new technologies affects 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 immigration and refugee administration systems, border enforcement and refugee response management. It is unclear how the courts will interpret administrative law principles like natural justice, procedural fairness and standard of review in respect of automated decision-making systems or where technologies are used opaquely.

45. Some technological experimentation relates to the collection of genetic data, which is justified on tenuous grounds. For example, in the United States there is the Combined DNA Index System (CODIS), a forensic DNA database used by states and the federal Government to collect, store and share genetic information.[122] Since January 2020, the Government of the United States has been collecting DNA from all persons in immigration custody.[123] This means 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 practice of collecting DNA only from individuals alleged to have engaged in criminal conduct.[124] In general, non-citizens in immigration custody are not criminals.[125] In fact, the vast majority of immigration infractions for which immigrants are detained are civil in nature.[126] In the case of 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.[127] The new immigration policy risks turning CODIS into a "genetic panopticon" that will encompass anyone within United States borders, including ordinary citizens who have been neither convicted nor even suspected of criminal conduct, threatening democracy and human rights.[128]

46. As COVID-19 has further incentivized and legitimized surveillance and other technologies targeting refugees and migrants, these groups have been subjected to further experimentation.[129] One example is the experimental deployment of an immunity passport

116 See https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12026585.

117 See https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf.

118 Petra Molnar and Lex Gill, *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System* (2018).

119 Ibid.

120 Joint Council for the Welfare of Immigrants v. Secretary of State for the Home Department CO/2057/2020.

121 Submissions by the Maat for Peace, Development and Human Rights Association and Ana Beduschi (citing Petra Molnar and Lex Gill, *Bots at the Gate*).

122 Joint submission by Daniel I. Morales, Natalie Ram and Jessica L. Roberts.

123 Ibid.

124 Ibid.

125 Ibid.

126 Ibid.

127 Ibid.

128 Ibid.

129 Submission by Amnesty International.

called “COVI-Pass” in West Africa.[130] The result of a partnership between Mastercard and the Gavi Alliance, this digital initiative combines biometrics, contact tracing, cashless payments, national identification and law enforcement.[131] Not only do such technologies operate outside human rights impact assessments and regulations, they also risk threatening human rights, including the right to 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.[132]

47. In the United Kingdom, concerns have been raised about the fact that contact-tracing applications and other data-collection technologies employed to combat the COVID-19 pandemic could eventually be used for immigration enforcement, undermining trust in contact-tracing technologies among immigrant communities and leading to their exclusion from effective health policies.[133] The United States Customs and Border Protection recently launched the CBP One application, which uses facial recognition and GPS technologies, as well as cloud storage, to collect data on asylum seekers before they enter the United States.[134] This application raises serious privacy and non-discrimination concerns.[135]

48. States and international organizations have promoted the creation of “immunity” or “health” passports that condition international travel and mobility on bearers’ vaccination status.[136] However, because of the unequal distribution of access to vaccines, such requirements will further exacerbate inequality in immigration and mobility opportunities. As vaccines become available, States and international organizations are turning to new technologies to facilitate the mobility of the vaccinated.[137] Organizations such as the World Health Organization, the International Air Transport Association, the World Economic Forum and the Gavi Alliance are actively developing digital systems that can track vaccination data and facilitate travel. Private technology companies are also working to provide seamless digital access to vaccination records.[138] IOM and the Migration Policy Institute have called for these efforts to be particularly sensitive to pre-existing inequalities, which are worsened by digitization, including to the impacts on “those in vulnerable situations or unable to access the relevant technology”.[139]

3. Border externalization

49. 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 have been well documented.[140] Border externalization does not affect all nationalities 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 and 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.

130 Ibid.
131 Ibid.
132 Ibid.
133 See https://www.openrightsgroup.org/blog/contact-tracing-apps-vulnerable-migrants-key-concerns/.
134 See https://www.latimes.com/politics/story/2021-06-04/asylum-bidens-got-an-app-for-that-with-privacy-risks-and-surveillance-beyond-border.
135 See https://www.americanimmigrationcouncil.org/FOIA/investigating-cbp%E2%80%99s-use-mobile-application-cbp-one.
136 International Organization for Migration and Migration Policy Institute, *COVID-19 and the State of Global Mobility in 2020* (2021), p. 51.
137 Ibid., pp. 51–52.
138 Ibid.
139 Ibid., p. 52.
140 See, e.g., A/HRC/23/46, A/HRC/29/36 and A/72/335.

50. The European Border Surveillance System, for example, uses big data technologies to predict, control and monitor traffic across European Union borders.[141] 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.[142] Although the European Commission insists that the drones are only for civilian surveillance purposes,[143] 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 Sea, one of the deadliest migration routes in the world.[144]

51. Another example is the participation of 13 European States in the ROBORDER project, a fully functional, autonomous border surveillance system consisting of unpiloted mobile robots capable of functioning on a standalone basis or in swarms, in a range of environments: aerial, water surface, underwater and ground.[145] 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, turning people into security objects and data points to be analysed, stored, collected and rendered intelligible.[146] The use of military, or quasi-military, autonomous technology also bolsters the connection between immigration, national security and the increasing criminalization of migration and use of risk-based taxonomies to flag cases.[147] Globally, States have been using various methods 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,[148] countries that are at the geographic frontiers of Europe and that increasingly rely on violent deterrence and pushback policies.

52. According to the Border Violence Monitoring Network, Croatia uses of European Union-funded technologies to detect, apprehend and return refugees and migrants travelling along the Balkan route, from Bosnia and Herzegovina and Serbia, through Croatia, to the Schengen border.[149] The Network alleges that hundreds of human rights abuses have been committed during the past three years, including illegal pushbacks that reflect inherently racist "cleavages".[150] Surveillance technologies such as drones and helicopters with automated searchlights have been weaponized and used against people on the move, making them easier to detect and thus compounding their vulnerability and the dangers they face.[151]

53. Discriminatory border externalization is also achieved through transnational biometric data-sharing programmes. One such program has reportedly allowed the Governments of Mexico and the United States to share biometric data.[152] As of August 2018, Mexico had deployed the United States-funded program, in all 52 migration processing stations.[153] The program uses biometric data to screen migrants detained in Mexico on suspicion of having tried to cross the border into the United States or of being members of

[141] Submission by Maat for Peace, Development and Human Rights Association, citing 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).

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

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

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

[145] Submission by Homo Digitalis. See also https://roborder.eu/.

[146] Raluca Csernatoni, "Constructing the EU's high-tech borders".

[147] Submission by Dimitri Van Den Meerssche.

[148] See https://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/.

[149] Submission by the Border Violence Monitoring Network.

[150] Ibid.

[151] Ibid.

[152] Joint submission by Privacy International and others.

[153] Ibid.

criminal gangs.[154] However, the National Institute of Migration of Mexico has denied, in answers to freedom of access to information requests, processing biometric data.[155]

4. Immigration surveillance[156]

54. A network of 55 towers equipped with cameras, heat sensors, motion sensors, radar systems and a GPS system is being constructed at the United States-Mexico border.[157] This border enforcement system, which also surveils the Tohono O'odham Nation's reservation, located in Arizona approximately one mile from the border,[158] has shifted the routes used by migrants, thereby increasing their vulnerability to injury, isolation, dehydration, hyperthermia and exhaustion and to death.[159] Researchers and civil society organizations have opposed these border technologies because they would exacerbate racial and ethnic inequality in policing and immigration enforcement, as well as curb freedom of expression and the right to privacy.[160] Others have highlighted the use of other autonomous surveillance artificial intelligence infrastructure at the United States-Mexico border, including drones designed to detect humans and alert border enforcement officials.[161] As mentioned above, the current evidence is that so-called "smart" border technologies force migrants to undertake ever more precarious journeys[162] and have a disproportionate impact on individuals from certain national origin, ethnic and racial groups.

55. In the United States, the communications of detained immigrants and their families and friends are surveilled.[163] The corporate providers of the technologies used for such communications claim to provide detained immigrants and their families with convenience in the form of calls, video chats, voicemail messages, photographs and text messages, while the company's real clients – the immigration officials – get data on users.[164] The web-based surveillance software offers government officials free "call-pattern analysis, relationship analysis and tools for data visualization".[165]

56. Yet another facet of immigration surveillance involves social media screening. Since April 2019, the United States State Department has required visa applicants to disclose information on social media accounts they have had during the five years prior to the time of application.[166] This expansive approach to social media screening is especially troubling because of the United States immigration enforcement's demonstrated track record of utilizing social media information in a manner that disproportionately harms members of racial, ethnic and religious minority groups.[167] The Department of Homeland Security has already falsely accused young Black and Latinx individuals of being members of gangs by exploiting social media connections, which has resulted in their detention, deportation and/or denial of immigration benefits.[168] Immigration and Customs Enforcement, an agency of the Department of Homeland Security, frequently combs social media to support gang

---

154 Ibid.

155 Ibid.

156 Anil Kalhan, "Immigration surveillance", *Maryland Law Review*, vol. 74, No. 1 (2014), wherein immigration surveillance is defined as the product of dramatically expanded capabilities for identifying individuals, tracking and controlling mobility and sharing information and of a weakening 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.

157 Submission by the Stop Killer Robots coalition.

158 Ibid.

159 Samuel Norton Chambers and others, "Mortality, surveillance and the tertiary 'funnel effect' on the US-Mexico border".

160 Submission by Minority Rights Group International.

161 Submissions by Mijente and Iván Chaar-López.

162 Submission by Franciscans International.

163 Submission by Mijente, citing https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

164 Ibid.

165 Ibid.

166 Submission by the Harvard Immigration and Refugee Clinical Program.

167 Ibid.

168 Ibid., citing https://www.ilrc.org/sites/default/files/resources/deport_by_any_means_nec-20180521.pdf.

membership allegations.[169] In one case, the Department of Homeland Security backed its allegation with a Facebook photograph of an immigrant youth wearing a Chicago Bulls hat. The immigration court denied him bond and rejected both his applications for asylum and permanent residence, deporting him to a country where he feared for his life,[170] in violation of non-refoulement obligations under international law.

57. Moreover, social media screening has compounded the disproportionate risk of people belonging to or presumed to be of Muslim faith or Arab descent by creating an infrastructure rife with mistaken inference and guilt-by-association.[171] For example, Customs and Border Protection, another agency of the Department of Homeland Security, denied a Palestinian college student entry to the United States based on his friends' Facebook posts expressing political views against the United States, even though he did not post such views himself.[172] In addition to the direct burden they place on non-citizens, the expanded social media disclosure requirements imposed by the Government of the United States foreseeably affect the rights to freedom of speech and of association.

58. Homeland Security Investigations, the principal investigative arm of Immigration and Customs Enforcement, was already testing automated social media profiling as early as 2016,[173] 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.[174] Concerns have also been raised about the use by the Government of the United States of technologies with the goal of making determinations through automation, in other words its use of technologies to determine whether an individual applying for or holding a United States visa was likely to become a positively contributing member of society or someone who intended to commit criminal or terrorist attacks.[175] Of particular concern has been the use in the United States of risk assessments tools in immigration detention decisions, including one that uses an algorithm set to always recommend immigration detention regardless of an individual's criminal history.[176]

59. All this points to a trend in immigration surveillance whereby predictive models use artificial intelligence to predict whether people with no history of criminal activity will nonetheless commit crimes in the future. These predictive models are prone to creating and reproducing racially discriminatory feedback loops.[177] Furthermore, racial bias is already present in the datasets on which these models rely.[178] When discriminatory datasets are treated as neutral inputs, they lead to inaccurate models of criminality that then perpetuate racial inequality and contribute to the targeting and over-policing of non-citizens.[179]

60. The response to the COVID-19 pandemic has led to the rapid increase in "bio-surveillance" – the monitoring of an entire population's health and behaviour on an unprecedented scale, facilitated by emerging digital technologies.[180] As States increasingly move towards a bio-surveillance system to combat the pandemic, there has been an increase in the use of digital tracking, automated drones and other technologies "purporting to help manage migration and stop the spread of the virus".[181] There is an outsize risk that these

169 Submission by the Harvard Immigration and Refugee Clinical Program.
170 Ibid.
171 Ibid.
172 Ibid.
173 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, No. 2 (2019).
174 Submission by Mijente, citing https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.
175 Ibid.
176 Submission by Minority Rights Group International.
177 Submission by Mijente.
178 Ibid.
179 Ibid.
180 See https://www.newstatesman.com/science-tech/2020/03/rise-bio-surveillance-state.
181 See https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf.

technologies will enable further discrimination on the basis of race, ethnicity and citizenship status.[182]

IV. Recommendations

61. **The Special Rapporteur recalls her previous report to the Human Rights Council and reminds States of their applicable international human rights obligations, in particular:**

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

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

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

62. **The Special Rapporteur reiterates the analysis and recommendations contained in her previous report regarding the obligations of States and non-State actors and urges States to consider them alongside the recommendations included in the present report. In the specific context of border and immigration enforcement, she recommends that Member States:**

(a) **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 person and anti-refugee political approaches to border governance, there can be no redress for the discriminatory effects of digital borders highlighted in the present report. States must comply with the international human rights obligation to prevent racial discrimination in border and immigration enforcement and implement the recommendations contained in the Special Rapporteur's previous report. States should also follow the guidance provided by the Principles on Deprivation of Nationality as a National Security Measure [183] and the Principles of Protection for Migrants, Refugees and Displaced People during COVID-19, [184] which articulate existing State obligations, including with respect to equality and non-discrimination, to ensure respect for the human rights of migrants, refugees and stateless persons, among others;**

(b) **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 highlights the importance of respecting existing international human rights legal obligations in the regulation of the design and use of these technologies;**

(c) **Take the steps recommended by the Committee on the Elimination of Racial Discrimination in its general recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials, particularly those recommendations on aligning the use of artificial intelligence with international human rights law;**

(d) **Ensure, at both the domestic and international levels, that border and immigration enforcement and administration are subject to binding legal obligations to**

[182] Ibid.

[183] See https://files.institutesi.org/PRINCIPLES.pdf.

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

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:

(i) **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 public deployment of systems. Such impact assessments must incorporate meaningful opportunities for representatives of racially or ethnically marginalized groups, including refugees, migrants, stateless persons and others, to co-design and co-implement the technologies. A purely or even mainly voluntary approach to equality impact assessments will not suffice – a mandatory approach is essential;**

(ii) **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. Such 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 video recordings and facial recognition technology. In some cases, it will be necessary to impose outright bans on technologies that cannot meet the standards enshrined in international human rights legal frameworks prohibiting racial discrimination;**

(iii) **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;**

(iv) **Legal obligations on private corporations to prevent, combat and provide remedies for racial and xenophobic discrimination resulting from the use of digital border technologies;**

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

63. **The Special Rapporteur had the opportunity to consult with representatives of UNHCR and IOM on their use of digital border technologies. Based on those consultations, she recommends that both entities adopt and implement mechanisms for the sustained and meaningful participation and decision-making of migrants, refugees and stateless persons in the adoption, use and review of digital border technologies.**

64. **Moreover, she recommends that IOM:**

(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 the systemic analysis of the potentially harmful and discriminatory impacts of digital border technologies prior to the adoption of these technologies, and prohibit the adoption of technologies that cannot be shown to meet equality and non-discrimination requirements. It should provide clearer, more concrete human rights-based guidelines on the criteria for the designation of "zero option" digital technologies and ensure the implementation of those guidelines;**

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

65. **Compared with 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 practice. In this regard, the Special Rapporteur recommends that UNHCR:

(a) **Ensure the effective implementation of its policies and practices for systemic analysis of the potentially harmful and discriminatory impacts of digital border technologies prior to their adoption and prohibit the adoption of technologies that cannot be shown to meet equality and non-discrimination requirements. It should provide clearer, more concrete human rights-based guidelines on the criteria for the designation of "zero option" digital technologies and ensure the implementation of those guidelines;**

(b) **Ensure the use and implementation of mandatory ongoing human rights assessment protocols for digital border technologies once deployed.**

66. **The Special Rapporteur recommends that IOM and UNHCR:**

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

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

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