University of Essex

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Digital Border Governance: A Human Rights Based Approach

September 2023

Acknowledgments

This study is the product of a collaboration between the University of Essex and the Office of the United Nations High Commissioner for Human Rights (OHCHR), generously funded and supported by the Federal Department of Foreign Affairs of Switzerland, without necessarily reflecting the views or position of the donor.

The study was written by Lorna McGregor, the principal investigator, professor of international human rights law and director of the Human Rights, Big Data and Technology Project at the University of Essex, and Petra Molnar, consultant to the project and the Associate Director of the Refugee Law Lab, York University and Faculty Associate at Harvard's Berkman Klein Center. It was developed in close consultation and collaboration with OHCHR's Migration Unit and the Rule of Law and Democracy Section of the Office of the High Commissioner for Human Rights. Buddhadeb Halder provided background research and materials for the report and Penny Castagnino organised the in-person expert meeting in Geneva.

This study has been shaped by critical contributions and insights from civil society, academia, and international organisations who participated in one-to-one meetings and interviews as well as online and in-person expert meetings throughout 2022 and 2023. As these meetings were held under the Chatham House Rule, we do not name these participants. However, we express our sincere gratitude for their time and generosity in sharing their knowledge and expertise with us in addition to the experts who carefully and critically reviewed earlier versions of the document. The study has also been shaped by the contributions of panellists, presenters, and participants at a Human Rights Council side-event held as part of the project.

Finally, the authors and OHCHR wish to recognise and thank all the survivors of human rights violations and abuses at borders whose experience, activism, and contributions have informed the development of an understanding of the impacts of digital border technologies and shaped the content of this study. The legal standards, analysis, and approach that we set out here are the product of their struggle and we dedicate the study to them.

Methodology

This study represents an initial mapping and identifies areas in need of further consideration through consultations with Member States and other stakeholders. It is based on research and information available in the public domain, as well as interviews and expert gatherings in 2022 and 2023 with representatives from civil society, academia, and international organizations. Further research is needed to fully assess practices across a broader range of countries and regions.

Contents

1. Introduction

In an age in which digital technologies are rapidly reshaping the dynamics of border governance, it is crucial to reflect on the timeless phenomenon of migration and the fact that people who embark on these journeys often find themselves in precarious and vulnerable situations. This vulnerability is further compounded by the unacceptable reality that human rights violations and abuses are regularly part of many people's journey. The human stories that underlie this complex landscape must be at the heart of any analysis into digital border technologies.

Many actors have repeatedly raised concerns about the dangers people on the move face at borders, which continue to be sites of systemic racism, discrimination, and human rights violations.[1] International borders are increasingly securitised and even militarised, with many States constructing expansive physical infrastructures to prevent migration. Some States embed digital technologies within their border governance infrastructure,[2] working with private actors to access and operate new and emerging digital technologies. For example, some States use drones and infrared cameras to detect movement near and at physical borders. When migrants and refugees arrive at border crossings, States and international organisations routinely employ biometric technologies, such as fingerprint and iris scanners and facial recognition technologies, with some reportedly testing new systems such as so-called lie detectors,[3] robo-dogs,[4] and GPS tagging.[5]

Additionally, the concepts of borders and border governance have expanded beyond the physical border. This expansion includes the internalisation or 'insourcing' of border governance through the 'policing… and enforcement controls within the interior, such as the detection, detention, and deportation' of people on the move.[6] It also involves the externalisation or 'outsourcing' of border governance, including practices such as remotely collecting biometric data and monitoring social media to gather information prior to individuals physically crossing the borders.[7] These practices raise risks that migrants and refugees are subjected to scrutiny, profiling, risk categorisation, and surveillance even before they leave their country of origin. Some States have also begun to incorporate new and emerging digital technologies, such as algorithmic risk assessments, into such processes alongside widescale data collection, including through large-scale and interoperable databases, which may collect, process, analyse, and share much wider forms of data than were previously collected within border governance. These processes can be underpinned by an opaque and discretionary ecosystem of decision-making, raising due process concerns.

Only partial information is publicly available on the full extent of current and proposed uses of digital technologies in border governance and the reasons States employ them.[8] Technological advancements can help speed up processes at borders. They could be used to prevent and address human rights violations and abuses against migrants and refugees at borders, and ensure accountability by enhancing human rights monitoring. However, a growing body of research by migrants' organisations, refugee-led organisations, civil society, UN entities and independent experts, think tanks, and academics demonstrates the numerous ways in which the use of digital technologies can negatively impact human rights and place people on the move in vulnerable situations, exacerbating power differentials already inherent throughout migration processes.[9] Depending on factors such as the type of technology, the reason for its use, the context in which it is deployed, and legal framework and procedural safeguards in place, a range of human rights can be at risk, including human dignity and the rights to non-discrimination, to privacy, to freedom of movement, to claim asylum, to an individual assessment of human rights protection needs, to liberty, and even to life. In addition, the use of new and emerging digital technologies within border governance can have a chilling effect on the exercise of rights such as to freedom of expression, association and religion, and the rights to education, housing and health.[10] These risks are exacerbated by people's intersecting vulnerabilities along the lines of race, ethnicity, gender identity, sex, age, disability, nationality, migration status and other factors.

The growing body of research on digital border technologies highlights the lack of a dedicated regulatory framework at the national, regional, and international level for the use of new and emerging digital technologies generally, and in border contexts specifically. Researchers have also outlined the gaps within efforts by States to uphold their human rights obligations and by private actors to respect their human rights responsibilities in the conception, design, development, deployment,[11] ongoing monitoring and oversight of the use of such technologies.[12] These failures also relate to decisions on whether to use such technologies at all, in the establishment, adequacy and effectiveness of accountability mechanisms and in access to justice and remedies and reparation for individuals and groups whose rights have been violated.

This study builds on this growing body of research. The analysis has been constrained by limited transparency relating to where technologies are used within border governance, details on the technologies themselves and the reasons for their deployment; whether human rights impact assessments were carried out prior to deployment; data sharing arrangements with private actors providing or operating the technology; and the nature of safeguards in place. Nevertheless, the study provides examples of specific technologies reported to be in use in parts of the world and their potential effects on human rights to illustrate possible human rights protection gaps and the importance of robust legal and policy frameworks to close these gaps and prevent the future materialisation of human rights harm.

This study and its findings have been informed by interviews with experts in the field, a series of collaborative bilateral and group meetings with more than 70 experts working in the fields of human rights, refugee protection, digital technologies, migration and border governance conducted from March to October 2022 and an online side event at the Human Rights Council in September 2022.[13] The recommendations in this study have been constructed through an iterative dialogue with key stakeholders, engaging a diversity of perspectives across geographies, disciplines, and lived experiences of migration. Examples in this study draw from this collective body of expertise, research, and evidence.

Building on this introduction, Part 2 sets out key definitions used in this study and provides further context to the use of new and emerging digital technologies in border governance. It highlights the expansion of where and how border control and border governance are taking place; the role of state and private actors; transparency barriers to mapping and assessing the human rights impact of digital border technologies; the factors that may influence the uptake of such technologies; and the frequent failures to operationalise human rights obligations and responsibilities in the context of digital border technologies.

Against this contextual background, Part 3 analyses the human rights impacts of particular digital border technology practices. This part does not seek to provide a comprehensive mapping or analysis of human rights harm but rather selects specific technologies to highlight the potential for serious and wide-ranging risks to human rights. By identifying these potential risks, the study underscores the need to ensure that robust protection frameworks are in place in order to prevent human rights harm materialising.

Part 4 advances the study's findings on minimum requirements to ensure that any uptake of new and emerging digital technologies at borders complies with international human rights standards and norms.

Endnotes

[1] UN OHCHR, *Recommended Principles and Guidelines on Human Rights at International Borders* (2014); UNGA, 'Promotion and protection of human rights, including ways and means to protect the human rights of migrants: Report of the Secretary-General' A/69/277 (7 August 2014); UNGA, 'Promotion and protection of human rights, including ways and means to protect the human rights of migrants: Report of the Secretary-General' A/68/292 (9 August 2013); OHCHR, 'Promotion and protection of the human rights and fundamental freedoms of Africans and of people of African descent against excessive use of force and other human rights violations by law enforcement officers through transformative change for racial justice and equality: Report of the UN High Commissioner for Human Rights' A/HRC/51/53 (2 August 2022); OHCHR, 'Promotion and protection of the human rights and fundamental freedoms of people of African descent against excessive use of force and other human rights violations by law enforcement officers: Report of the United Nations High Commissioner for Human Rights' A/HRC/47/53 (1 June 2021).

[2] The different reasons States may employ such technologies is discussed in Part 2(E) below.

[3] *See*, Parts 3(B) and (C) below.

[4] *See*, Part 3(A) below.

[5] Privacy International, 'Stop GPS tagging migrants'; Privacy International, 'Privacy International files complaints against GPS tagging of migrants in the UK' (17 August 2022).

[6] *See*, Cecilia Menjívar, 'Immigration Law Beyond Borders: Externalizing and Internalizing Border Controls in an Era of Securitization' 10 *Annual Review of Law and Social Science* 353 (2014), abstract.

[7] UK Home Office, 'Biometric self-enrolment feasibility trials' (4 July 2022); *See also*, Faiza Patel, Rachel Levinson-Waldman, Sophia DenUyl, and Raya Koreh, 'Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security', *Brennan Center for Justice at New York University School of Law* (22 May 2019).

[8] *See*, for example, UN Working Group on the use of mercenaries, 'Impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants: Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination' A/HRC/45/9 (9 July 2020), at §17.

[9] OHCHR and Global Migration Group, *Principles and Guidelines, Supported by Practical Guidance, on the Human Rights Protection of Migrants in Vulnerable Situations* (2018) at 5-7.

[10] *See,* Part 3 below.

[11] UNGA, 'Resolution adopted by the Human Rights Council on 13 July 2021: 47/23 new and emerging digital technologies and human rights, A/HRC/RES/47/23 (16 July 2021).

[12] *See*, Parts 3(D) and 4(A)(2) below.

[13] *See* acknowledgments section.

2. Definitions and context

This part sets out definitions of key terms used in the study, as per established OHCHR guidelines. Building on the introduction, it also provides a contextual analysis of the border governance systems into which new and emerging digital technologies are often introduced; transparency barriers to mapping the deployment of new and emerging digital technologies; and the factors which may influence the uptake of such technologies.

A. Borders and Border Governance

In its 2014 *Recommended Principles and Guidelines on Human Rights at International Borders*, OHCHR defines '[i]nternational borders' as

> the politically defined boundaries separating territory or maritime zones between political entities and to the areas where political entities exercise border governance measures on their territory or extraterritorially (such areas include land checkpoints, border posts at train stations, ports and airports, immigration and transit zones, the high seas and so-called "no-man's land" between border posts, as well as embassies and consulates).[14]

It explains that border governance 'measures' include

> legislation, policies, plans, strategies action plans and activities related to the entry into and exit of persons from the territory of the State, including detection, rescue, interception, screening, interviewing, identification, reception, detention, removal or return, as well as related activities such as training, technical, financial and other assistance, including that provided to other States.[15]

Since the adoption of these standards, researchers have pointed to 'the global spread of legal techniques that strive… to "push the border out" as far away from the actual territorial border as possible… [P]rosperous nations increasingly rely on sophisticated legal tools to expand the reach of border control.'[16] As noted above, border controls can also be pushed inwards into the interior of a State through a process of 'internalisation.'[17] Therefore, border governance should be understood as much wider in application than acts at a physical border. New and emerging digital technologies are increasingly deployed as central tools in this expanded form of border governance.[18] As such, this study examines the use of new and emerging digital technologies at physical international borders and also within States of intended departure, and after people on the move have crossed borders, including many years later.

B. Actors Involved in Border Governance

Key standards such as OHCHR's *Principles and Guidelines on the human rights protection of migrants in vulnerable situations* refer to actors involved in border governance as 'border guards, consular and immigration officials, border police, staff at border detention facilities, immigration and airport liaison officers, coast guard officials, and other front line officers and staff performing border governance roles.'[19] With the increasing securitisation of borders and their internalisation and externalisation, the profile of State, non-State armed groups and private actors, such as private military and security companies, involved in border governance has expanded significantly.[20] As highlighted by the UN Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination (UN Working Group on the use of mercenaries), 'immigration and border management has become a multibillion-dollar business, with global border security identified as a potential market for further growth in the coming years.'[21] International organisations are also playing a part in the development and deployment of technologies used for border governance.[22]

C. Digital Border Technologies

This study employs the term 'digital border technologies'[23] to refer to the wide range of technologies from basic internet-enabled devices to more advanced forms of technologies, including those enabled by algorithms, automated decision-making, and artificial intelligence, which States and private actors already use or plan to use in border governance in the future. The UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance has noted that infrastructure at borders '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.'[24]

The term 'digital border technologies' includes technologies which are often characterised as 'artificial intelligence' (AI) but is not confined to them. This is because not all digital technologies employed in border governance would constitute a form of 'AI.' Moreover, 'AI' is itself a contested term[25] which is frequently employed by policy-makers and the wider public without an agreed definition. Even where technologies are employed which would fall within a definition of 'AI,' it is not possible to discuss 'AI' technologies without also assessing the role of data which both feeds and is the product of such technologies. Digital border technologies also include some surveillance technologies, such as drones, towers, and vehicles, which are equipped with infrared cameras and night vision, and which in some instances may simply operate digitally but in others may already, or in the near future, be 'AI-enabled,' for example, with the capacity to make distinctions between humans and animals.[26] This study also recognizes the growing use of tools reliant on generative AI, including for border enforcement and migration management.[27]

D. Transparency Barriers in Mapping the Use of Digital Border Technologies

Despite the growing body of research into digital border technologies, a lack of transparency presents a major barrier to the mapping of such technologies and to the assessment and operationalisation of human rights protection in the use of digital border technologies. Only partial information is publicly available on the full extent of current and future uses of digital technologies in border governance.[28] States often link border enforcement and security concerns[29] as well as use justifications of national sovereign control over border enforcement, creating grey zones of accountability and oversight.[30]

Such opacity can deepen where private actors are involved,[31] consolidating knowledge and power within the private sector.[32] Full details on the use of digital technologies often only come to light after-the-fact, typically through the work of civil society organisations, human rights monitors, investigative journalists, and academics. Even then, researchers have pointed to significant obstacles to transparency which can prove difficult to overcome, including, for example, freedom of information requests which have in some instances not resulted in a response or have been rejected on the basis of national security or the 'commercial interests' of technology developers or providers.[33]

Where a response is received, it may also be incomplete or contain extensive redactions. Increased targeting of civil society, monitors, and journalists, who endeavour to bring these issues to light, including through social media surveillance, has also been documented, potentially creating a chilling effect on the investigation and reporting on the impacts of digital border governance technologies.[34]

As a result, there is insufficient policy and regulatory information available documenting the reasons for integrating technology into border governance strategies. There is a similar lack of information regarding how States assess the lawfulness, necessity and proportionality of such deployment, particularly against the potential impacts on human rights, and the availability of less intrusive alternatives, both technological and non-technological. There are also few publicly available human rights impact assessments of digital border technologies, meaning there is little information regarding the perceived need to deploy digital border technologies (individually or collectively); consideration of non-technological approaches; justifications for the selection of particular technological models and private contractors to supply and/or operate the technology; assessments of the potential human rights impact of technological deployment; applicable legal frameworks; and the safeguards to mitigate harm. States also rarely provide public information regarding the reasoning underlying their use of digital border technologies and their prominence within border governance. Where information is available, it is often limited to broad explanations of the centrality of technology in overarching policy documents, such as border strategies. The layered opacity accompanying the use of digital border technologies therefore presents obstacles to capturing the full extent of human rights harm.

E. Factors Potentially Influencing the Adoption of Digital Border Technologies

Some documentation exists which indicates the types of practical, policy, legal, and economic factors that, individually or collectively, could account for States' decisions to employ digital border technologies. For instance, some border governance strategies emphasise the efficiency gains of digital border technologies, both for the actors governing borders[35] and through the offer of 'seamless' travel for certain individuals.[36] Other documents, such as the legal instruments underpinning the European Union's interoperable databases on border governance, refer to objectives such as to 'contribute to a high level of security,'[37] to prevent irregular migration,[38] to identify migrants with irregular status, such as 'overstayers,'[39] to combat fraud,[40] as part of strategies on 'the prevention, detection and investigation of terrorist offences or of other serious criminal offences,'[41] to contribute to the 'protection of public health,'[42] or to facilitate search and rescue at sea but 'taking place in situations which may arise during border surveillance operations.'[43]

In addition, during the Covid-19 pandemic, research points to an increased normalisation of surveillance and automated technologies originally justified as necessary to respond to a public health emergency, including but not limited to border governance.[44] Moreover, resolutions from the UN Security Council have imposed on States a series of 'border security and information sharing' requirements related to counterterrorism.[45] States may also deploy digital border technologies as part of bilateral agreements[46] as conditions for funding[47] or technical assistance[48] from other States. These technologies can become embedded and further normalised in border governance not only through formal procurement processes[49] but also through the 'donation' of digital border technologies to States.[50] Finally, the political economy of border governance and securitisation agendas may drive and incentivise the development, deployment, and adoption of digital border technologies, prioritising and normalising technical solutions to border governance.[51]

As digital border technologies increasingly become part of border governance, private actors not only provide and operate digital border technologies but also contribute to their proactive design and development, thus becoming central shapers of how borders are governed.[52] The UN Working Group on the use of mercenaries has observed that 'the considerable and growing corporate involvement in this sector has led to a commodification of immigration and border management services, with such services being seen primarily as economic, profitmaking activities rather than as an essential function of the State to ensure security and appropriate protection, as guaranteed by international law, for all those on its territory.'[53]

Endnotes

[14] *Recommended Principles and Guidelines on Human Rights at International Borders* (n1), at §10(b).

[15] Ibid at §10(e).

[16] Ayelet Schachar, 'Instruments of Invasion: The Global Dispersing of Rights-Restricting Migration Policies' 110 *California Law Review* 967 (2022), at 969. *See also*, Ayelet Schachar, *The Shifting Border* (2020).

[17] *See*, introduction.

[18] For example, Marie McAuliffe, Jenna Blower, and Ana Beduschi, 'Digitalization and Artificial Intelligence in Migration and Mobility: Transnational Implications of the COVID-19 Pandemic' 11 Societies 135 (2021) (noting that, '[t]o situate the analysis of digitalization and AI in migration, we apply the analytical framework of the "Migration Cycle" to demonstrate its broader applicability that is much wider than the more obvious areas of border management and visa processing. The increase in digital capture means that AI has been used throughout the Migration Cycle at all stages: pre-departure, entry, stay and return.')

[19] OHCHR and Global Migration Group (n9) at 11.

[20] Report of the Working Group on the use of mercenaries (n8), at §17. See also, Mark Akkerman, 'Financing Border Wars: The border industry, its financiers and human rights' *Transnational Institute* (April 2021).

[21] Report of the Working Group on the use of mercenaries (n8), at §21.

[22] *See*, for example, UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, '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' A/HRC/48/76 (22 September 2021) (including at §§63-67 a dedicated set of recommendations to international organisations dealing with migration management and their own use of border technologies, such as the UNHCR and IOM).

[23] The definition of digital border technologies – and for reasons of space, this study – does not cover the use of digital technologies by migrants and refugees themselves. However, the report acknowledges the critical role these technologies can play, including for those embarking on dangerous journeys, both for navigating the journey and keeping in touch with families and friends and how they can become part of digital border technologies if migrants and refugees are compelled to hand them over or enable others to access them at borders.

[24] Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance' (n22), at §2.

[25] *See*, for example, UNGA, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', A/73/348 (29 August 2018), at §3.

[26] Mijente, Just Futures Law & No Border Wall Coalition, *The Deadly Digital Border Wall* (2021) at 12. The definition above also fits with wider definitions such as that employed by the Human Rights Council Advisory Committee, see, Human Rights Council Advisory Committee, 'Possible impacts, opportunities and challenges of new and emerging digital technologies with regard to the promotion and protection of human rights: Report of the Human Rights Council Advisory Committee' A/HRC/47/52 (19 May 2021) at §3. For further definitions, *see* UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (23 November 2022) at 10; UN Chief Executives Board for Coordination, High-Level Committee on Programmes (HLCP) Inter-Agency Working Group on Artificial Intelligence, *Principles for the Ethical Use of Artificial Intelligence in the United Nations System* (20 September 2022) at §2.

[27] *See* for example, Andy J. Semotiuk, '12 Ways Chat GPT Will Change U.S. Immigration Forever', Forbes (16 December 2022), see also Petra Molnar, *Generative AI or Generative Discrimination? Border Surveillance at the Sharpest Edges*, Harvard Law School's Berkman Klein Center for Internet and Society (forthcoming September 2023).

[28] *See*, for example, Report of the Working Group on the use of mercenaries (n8), at §17.

[29] Gavin Sullivan, *The Law of the List: UN Counterterrorism Sanctions and the Politics of Global Security* (2020).

[30] Petra Molnar, 'Surveillance sovereignty: migration management technologies and the politics of privatization' in Idil Atak and Graham Hudson (eds), *Migration, Security, and Resistance: Global and Local Perspectives* (2021) 66-82, at 70.

[31] *See*, Business & Human Rights Resource Centre, Scrutinising Migration Surveillance: human rights responsibilities of tech companies operating in MENA (September 2022), at 6.

[32] Petra Molnar, 'Technology at the Margins: The Human Rights Impacts of AI in Migration Management' 8(2) *Cambridge Journal of International Law* (2019), at 77.

[33] Derya Ozkul, Automating Immigration and Asylum: New Technologies in Migration and Asylum Governance in Europe' Oxford: *Refugee Studies Centre, and* AFAR (2023) at 27; University of Essex and OHCHR Online Expert Meeting 1 (8 March 2022).

[34] *See also*, Special Rapporteur on the situation of human rights defenders, 'Greece migration policy having a "suffocating effect" on human rights defenders says UN expert' (22 June 2022); Daniel Ghezelbash, 'Technology and countersurveillance: holding governments accountable for refugee externalization policies' *Globalizations* (2022), at 10.

[35] European Union, Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 [hereinafter 'EES Regulation'], Article 6(1)(a); Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, Article 4(d) [hereinafter 'ETIAS Regulation'].

[36] *See*, for example, 'The Republic of Seychelles deploys Travizory technology to streamline travel authorization'; HM Government, '2025 UK Border Strategy' (December 2020); Australia's Department of Immigration and Border Protection, Technology Strategy 2020.

[37] ETIAS Regulation (n35), Article 4(a); Regulation 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas' (9 July 2008), Article 2(g) [hereinafter 'VIS Regulation'].

[38] ETIAS Regulation (n35), Article 4(b).

[39] EES Regulation (n35), Article 6(1)(b) and (c) – 2017/2226; VIS Regulation (n37), Article 2(e).

[40] EES Regulation (n35), Article 6(1)(i); VIS Regulation (n37), Article 2(c).

[41] EES Regulation (n35), Article 6(2)(a) ; ETIAS Regulation (n35), Article 4(e) and (f).

[42] Ibid. Article 4(c). *See,* for example, Australia Department of Immigration and Border Protection (n36) at 6 (stating that, '[t]he Department's technology will need to adapt to the changing global threat environment to protect Australia and its interests from terrorism, illicit materials, illegal migration and organised crime. Real-time data matching, intelligence, identity and biometrics, operational capability technologies that support functions such as scanning and surveillance, and automated decision making systems will be fundamental to managing and adapting to the contemporary and complex threats across the border continuum').

[43] European Union, Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, Article 3(1)(b).

[44] Petra Molnar, 'Territorial and Digital Borders and Migrant Vulnerability Under a Pandemic Crisis' in Anna Triandafyllidou (ed), *Migration and Pandemics Spaces of Solidarity and Spaces of Exception*. IMISCOE Springer (2022) 44-64, at 48; European Centre for Not-for-Profit Law (ECNL), International Network of Civil Liberties Organisations (INCLO) and Privacy International, 'Under Surveillance: (Mis)use of Technologies in Emergency Responses Global lessons from the Covid-19 pandemic' (14 December 2022).

[45] UNSC, Resolution 2396 (2017) S/RES/2396 (21 December 2017) (providing that obligations include 'collect[ing], process[ing], analys[ing]' and sharing passenger name records, the 'develop[ment of] watch lists or databases of known and suspected terrorists, including foreign terrorist fighters, for use by law enforcement, border security, military, and intelligence agencies to screen travelers and conduct risk assessments and investigations'; and the 'develop[ment] and implement[ation of] systems to collect biometric data'.)

[46] Alex Perala, 'Canadian Authorities to Track Unverified Refugees with Voice Recognition' (26 July 2018) (discussing biometric tracking of refugee claimants).

[47] University of Essex and OHCHR Online Expert meeting 4 (25 July 2022).

[48] Ibid.

[49] *See* Chris Burt, 'Zimbabwe to use Hikvision facial recognition technology for border control' *Biometric update.com* (14 June 2018).

[50] University of Essex and OHCHR Online Expert Meeting 1 (8 March 2022).

[51] Petra Molnar, *The Walls Have Eyes: Surviving Migration in the Age of Artificial Intelligence*, The New Press (2024), at chapters 7 and 8.

[52] See Dimitri Van Den Meerssche, 'Virtual Borders: International Law and the Elusive Inequalities of Algorithmic Association', 33(1) *European Journal of International Law* 171 (2022).

[53] UN Working Group on the use of mercenaries (n8), at §23.

3. The human rights impact of digital border technologies

Nearly every part of a person's migration journey is now impacted by digital border governance. For those who do not qualify for the benefits of 'seamless' international travel and mobility, due to various factors such as race, ethnicity, national origin, gender identity, sex, prior travel history, protection needs, migration status, and others, borders can be sites of exclusion, violence and discrimination.[54]

Increasing securitisation[55] and even militarisation[56] of borders and border governance can also fuel anti-migrant sentiments, particularly of a racist and xenophobic nature, and entail the pursuit of strategies and practices that are either inherently incompatible with human rights or put many human rights at risk, such as push and pullbacks,[57] wide-scale and prolonged detention, and refoulment.

Extensive documentation already exists, including by UN entities, of the serious inequality and threats to human rights faced by many migrants and refugees before, at and after international borders, including the rights to non-discrimination, liberty and security, freedom of movement and prohibition of refoulment and collective expulsion, and the right to seek asylum, among many others.[58]

In such contexts, digital border technologies that inevitably become harnessed to achieve security objectives both accentuate existing human rights concerns and enable these concerns to manifest in new ways.[59] A human rights-based approach to border governance and migration has to be the priority. This approach should be grounded in first trying to first understand how ill-conceived approaches to border governance and management of population movements may lead to deficits in human rights protection, and second, to assess how technologies that are introduced, may accentuate existing concerns.

While a growing body of research has increased the public information available on the deployment of digital border technologies,[60] it is not currently possible to present a comprehensive picture due to significant deficits in transparency as noted in the previous part of this study.[61] Accordingly, this part provides selected examples of new and emerging digital technologies that are already employed by certain States and private actors within border governance with serious consequences for human rights.[62] These examples are non-exhaustive and are not the only instances of digital technologies resulting in human rights harm.

A. Technologies Used to Detect People on the Move at Physical Borders

As part of securitised border policies, many States and transnational entities employ new and emerging digital technologies near and at land and sea borders (including at external frontiers, such as the external borders of the European Union and Schengen zone) as a means to detect people on the move. These technologies are used together with physical barriers designed to prevent people from crossing international borders.[63] They can include remote and mobile video surveillance systems which may employ colour and infrared cameras with video analytics,[64] surveillance towers, ground sensors, and both manned and unmanned aerial systems, including drones.[65] Some of these technologies are now enabled by artificial intelligence designed to not only detect movement but also to 'distinguish between people and livestock' among others.[66] New projects introduced for border governance also repurpose technology developed for law enforcement or military operations, such as quadruped or biped autonomous robots, colloquially referred to as 'robo-dogs.'[67]

Some States and regional organisations, are now not only using technologies in real time at, and close to, international borders (for example, at sea) but also harnessing technologies in an attempt to predict migration trends.[68] Research suggests that these efforts often employ data from a wide range of sources including social media, internet searches and mobile phone data extraction for the purposes of monitoring and predicting people's behaviour.[69] Civil society organisations, academics and international organisations have expressed concern that attempts at prediction are focused on preventing border crossings, rather than supporting migrants and potential asylum seekers.

When these technologies are used as part of a securitised approach to border governance, they can put many human rights at risk, including by preventing people from leaving their country of origin or claiming asylum. For example, some of these systems are used in conducting search and rescue or interceptions operations, including as part of push and pullbacks and border interdiction operations.[70] The UN Working Group on the use of mercenaries has reported that the use of drones in maritime surveillance enables States and regional organizations to focus on detection and to distance themselves from search and rescue operations[71] that may result in migrants reaching safe harbours. Reports suggest that information gathered by drones and other air assets used in surveillance operations by countries of destination has been sent to coastguards in countries of transit so that the latter conducts the rescue operations in lieu of the former, resulting in returns of migrants to the country of transit. This has included return to a country of transit where migrants are at serious risk of arbitrary detention, torture, ill-treatment and other forms of abuse.[72]

In 2021, the UN Special Rapporteur on the human rights of migrants also issued a report on pushbacks, noting that, '[p]ushbacks are often carried out as a measure of deterrence, punishment, or targeting migrants as part of wider strategies. Pushback policies and practices, together with the deployment of physical barriers and advanced surveillance and deterrence equipment at borders, carry life-threatening risks for migrants.'[73]

In addition, recent research has highlighted that where people on the move are aware of the use of surveillance systems at physical borders, such as surveillance towers and mobile monitoring devices, they may pursue 'less direct and more dangerous routes' in order to avoid such systems[74] due to a fear of being detected and penalised, their chance of seeking asylum or other human rights protections jeopardised, or being subject to increased human rights risks, including loss of life.[75]

B. Polygraphs

Other digital border technologies tested for use at international borders include so-called lie-detection systems.[76] Such systems have been described as a 'virtual border agent kiosk developed to interview travelers at airports and border crossings' that can 'detect deception to flag to human security agents.'[77] EU-funded pilot projects such as iBorder Control have sought to develop an automated deception detection system, 'a 'face-matching tool' that gathers images for facial recognition, a 'biometrics tool' that collects iris and palm vein scans and a 'document authentication tool,' Tresspass, provides the capacity for 'real-time behaviour analytics' that could detect 'hidden aspects' of 'intent' and 'attitude' through 'on-site observations' as well as 'open source web intelligence and mining.''[78]

Attempts to determine what people are thinking and the veracity of what they say are likely to be highly susceptible to bias, stereotypes, and discrimination.[79] Indeed, the project iBorderCtrl itself concluded 'there is always a risk of false positives (people being falsely identified as deceptive) and false negatives (criminals being falsely identified as truthful)… lead[ing] to stigmatization and or prejudice against affected persons' and presenting human rights risks.[80] In addition to the inherent risks to the rights to non-discrimination and freedom of thought, in a border governance context, the use of such technologies could result in the unjustified denial of an asylum claim or visa, detention, prosecution, refoulement, or violation of the right to family life through separation or denial of family reunification.

C. Technologies aimed at identifying people with irregular status for removal

As part of the internalisation of borders, some States are employing new and emerging digital technologies to try to detect people with irregular status, including taking these steps years after the person first arrived in the country.[81] Civil society organisations and investigative journalists have documented that some immigration enforcement agencies have accessed other State agencies' databases which are usually firewalled from law enforcement to try to detect individuals with irregular status, risking detention and deportation. Some States have reportedly used data brokers to access data such as 'financial records, property records, past jobs, former marriages, phone subscriptions, cable TV bills, car registrations.'[82]

Given the severe consequences that may flow from detection, academics and civil society organisations have documented the chilling effect the use digital border technologies can have on the exercise of people's rights, such as to education, health, and housing. Reports have highlighted that migrants often fear engaging with 'record-keeping institutions that are critical to the well-being of themselves and their family' such as 'child welfare, healthcare, and access to legal systems' out of fear that law enforcement agencies may be able to access their data and eventually detain, prosecute and remove them from the country.[83]

D. Use of Digital Border Technologies in Decisions to Detain and as 'Alternatives' to Detention

Researchers have documented the use of algorithmic risk assessments in different areas of border governance, for example, to sort visa applicants into different levels of risk, diverting those deemed higher risk to a human decision maker. Some States also use algorithmic risk assessments in decisions on whether to detain migrants.[84]

As with the wider use of algorithmic risk assessments elsewhere, the use of algorithmic risk assessments in decisions to detain poses significant human rights risks.[85] Algorithms require vast datasets on which to learn. However, these datasets can be replete with biased and discriminatory data, both through the over or underrepresentation of particular groups, particularly in areas of historical discrimination such as gender, race, and ethnicity.[86] In the border governance context, these categories can include proxies for discrimination such as country of origin. Discrimination may also result from how the algorithm weighs the data it is fed and the outcomes it produces.[87] In research on the use of algorithms in decisions to detain, researchers in the US have highlighted the potential for certain algorithms to be designed to tip in favour of a high-risk classification, noting that manipulating the weight of different factors could mean that some 'low-risk' migrants are subject to blanket detention.[88]

Even if only presented as an evidentiary tool, human decision-makers may defer to the findings of an algorithmic risk assessment due to the perceived objectivity and scientific nature of algorithms, which may trigger confirmation and automation biases held by human officers.[89] Such exercises may discriminate among different groups and may result in presumptions of risk and stereotypes including about 'entire groups or communities' by human decision-makers.[90]

States may also employ surveillance technologies ostensibly as an 'alternative' to traditional forms of detention, such as electronic monitoring, digital ankle shackles and voice and facial recognition reporting software.[91] However, the UN Committee on the Protection of the Rights of All Migrant Workers and Members of their Families has noted that these measures can exacerbate the stigmatization of migrants, generate excessively onerous requirements, and may amount to de facto detention even if characterised as an 'alternative,' resulting in the expansion of detention regimes. Even if specific measures are not deemed to constitute a form of detention, they increase surveillance and restrict freedom of movement of people on the move.[92]

E. Role of Data

Data is central to the technologies discussed above and those used more broadly within the border governance context, both as input data and as a product of their deployment, thus generating more data. Many States have expanded the types of data they collect, process, store and share, including fingerprints and facial images collected as part of visa and travel authorisation applications[93] and through automated border control technologies such as e-gates and smart tunnels,[94] monitoring health data,[95] data from social media accounts,[96] information on a person's educational attainment[97] and whether they are in employment.[98] Data is not only collected from people on the move by migration authorities but may also be gathered by private companies, international organisations, and other States and shared not only regionally but also globally.[99] The European Union's draft Act to Regulate Artificial Intelligence proposes to exclude existing interoperable migration, and asylum, and criminal records databases from the protections the Act would normally provide for high risk uses of AI.[100] Access to interoperable databases supports the conflation of data collected for criminal proceedings with immigration databases, presenting various potential human rights risks, including infringements on the rights to privacy, equality and freedom from discrimination, as well as the rights to life, liberty, and security of the person if indiscriminate data sharing results in detention and deportation.

In addition to expanding the types of data collected, States and organisations increasingly store some or all this data within large-scale and/or interoperable databases. In the USA, for example, recent reports suggest that the Department of Homeland Security is developing a large-scale database creating digital profiles of individuals, linking biometric information, political affiliation, location, relationship patterns, and religious affiliations, among other factors.[101] The aim of this database is reportedly to share personal data from federal agencies such as Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), the Federal Bureau of Investigation (FBI), and the Department of Defense as well as from local and state enforcement, and from dozens of foreign governments and international agencies, including the United Nations.[102]

Where data is collected within the context of border governance, there is the increasing possibility that it may be accessed by other actors. First, law enforcement agencies may be able to access data due to an absence of firewalls. For example, the European Union has adopted a framework for the interoperability of its databases, which 'allows authorised actors to search across all six databases depending on their access rights.'[103] In contrast to its previous 'compartmentalisation' of migration-related databases,[104] this new framework has been described by the European Union Agency for Fundamental Rights as creating 'a database of identities.'[105]

Second, even where data is collected for a specific purpose, such as to process a visa application or to claim asylum, it is possible that the purpose changes later, enabling other actors – including law enforcement – to access the data.[106] For example, within the European Union, at least with regard to one of the new systems (ECRIS-TCN)), the relevant regulation foresees the possibility of including additional (and as of yet undefined) purposes in the future.[107]

Researchers have raised similar concerns that data may be collected for humanitarian purposes, including in refugee camps[108] and conflict settings,[109] but then shared with States that may then use it for immigration enforcement purposes, without the knowledge of the person concerned.[110] Researchers also note that interoperability may expand to encompass further information systems, including commercial systems, and new and emerging digital technologies as they are introduced.[111]

Expansions in the types of data collected by States within a border governance context raises questions as to the adequacy and effectiveness of data protection regimes in place. The establishment of large scale and interoperable databases and the potential for the repurposing of data originally collected for a specific purpose on its face appears to conflict with core data protection principles such as purpose limitation and data minimisation as well as the maintenance of firewalls.[112] These minimum safeguards are critical for the protection of human rights. Their absence can lead to unlawful and discriminatory surveillance and profiling (including the use of biometrics); an increase in stop and search of already discriminated against, and overpoliced, groups;[113] arbitrary arrest and detention; refoulement;[114] and the sharing of information with the very States from which individuals have fled.[115] As discussed above, the potential for the repurposing of data now or in the future can result in 'system avoidance' and thus have a chilling effect on people on the move accessing services and enjoying their human rights. For example, some may feel compelled to participate in data collection, such as iris scanning, in exchange for services in refugee camps such as food rations, or to be allowed to exercise their rights to seek asylum and other human rights protection. Or they may forego these rights out of fear of immigration enforcement related to data collection and repurposing, due to power differentials, language issues, and questions about consent.

Endnotes

[54] *See,* for example the work of Harsha Walia, *Border and Rule: Global Migration, Capitalism, and the Rise of Racist Nationalism* (2021), see also Human Rights Council, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (n22), at §2.

[55] University of Essex and OHCHR Online Expert Meeting 2 (2 June 2022).

[56] University of Essex and OHCHR Online Expert Meetings 2 (2 June 2022) and 3 (15 June 2022).

[57] OHCHR, *Manual on Human Rights Monitoring: Chapter 26, Monitoring and protecting human rights in the context of migration* (2021) at 41 (explaining that '[p]ullback operations are designed to physically prevent people from leaving the territory of any given State, or to forcibly return them to that territory, before they can reach the jurisdiction of their destination State. Pullbacks could happen at the instigation and on behalf of destination States desiring to prevent arrivals without having to engage their own border authorities in unlawful pushback operations. Pushback operations are proactive operations that physically prevent people from reaching, entering or remaining within the territorial jurisdiction of the destination State. They can take place at sea, where they involve the interception of vessels carrying migrants inside or outside territorial waters. They may be followed by immediate return to their port of origin, or they may leave migrants and refugees adrift. They can also happen on land at or close to an international border. Pushbacks usually involve the threat or use of force by border officials to prevent people on the move from approaching or crossing the border, or to intimidate those who have successfully crossed the border, before returning them to the country of departure. Pushbacks render individual assessments summary or undermine them altogether'). See also, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (n22); Report of the Working Group on the use of mercenaries (n8), at §43.

[58] This study endeavours to be as fulsome as possible regarding the many different contexts but some additional examples of human right infringements that can occur include: securitisation and policies leading to raids, pushbacks, pullbacks, lack of individual assessment, criminalization of irregular migration, criminalization of human rights defenders in the context of migration and search-and-rescue, use of detention (separation of children and families in some cases), deportations, exacerbation of xenophobia, lack of protection against third actors such as transnational trafficking operations, lack of effective search and rescue operations, lack of de-embarkation mechanisms, prioritising voluntary returns and normalizing forced returns, externalization agreements and off-shoring practices, among others.

[59] *See*, Human Rights Council, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (n22).

[60] *See,* for example the work of Mijente, Just Futures Law, Immigrant defence Project, R3D, Derechos Digitales, EDRi, Access Now, PICUM, Equinox Racial Justice Collective, Statewatch, Transnational Institute, Refugee Law Lab, Border Violence Monitoring Network, Forensic Architecture, Lighthouse Reports, Privacy International, Homo Digitalis, Article 19, Digital Rights Foundation, 7amleh, Josoor, Haki na Sheria, Namati, Nubian Rights Forum, and others.

[61] Report of the Working Group on the use of mercenaries (n8), at §62.

[62] Many of the examples relied upon within this part of the study are drawn from destination countries. No conclusions can easily be drawn from this imbalance due to ongoing transparency obstacles. However, within the expert meetings arranged as part of the research for this project, some participants observed that some States and international organisations within destination countries appear to be incentivising other States to use and emerging technologies within their governance of borders.

[63] Jane Kilpatrick and Chris Jones, 'A clear and present danger: Missing safeguards on migration and asylum in the EU's AI Act' (12 May 2022).

[64] Mijente, Just Futures Law & No Border Wall Coalition (n26) at 11.

[65] *See* more: https://roborder.eu/; Statewatch, 'Drones for Frontex: unmanned migration control at Europe's borders' (27 February 2020); Algorithm Watch, *Greece plans automated drones to spot people crossing border*, (23 September 2022).

[66] Mijente, Just Futures Law & No Border Wall Coalition (n26), at 12; *see also*, Report of the Working Group on the use of mercenaries (n8), at §22: 240, Sarah Léonard, 'EU border security and migration into the European Union: FRONTEX and securitisation through practices,' 19(2) European Security 231 (2010).

[67] Petra Molnar and Todd Miller, 'Robo Dogs and Refugees: The Future of the Global Border Industrial Complex' *The Border Chronicle* (17 February 2022).

[68] See for instance, 'Artificial Intelligence – based capabilities for European Border and Coast Guard' (26 March 2021).

[69] Disclose, 'Predicting migration flows with artificial intelligence – the European Union's risky gamble' (26 July 2022); see also, EDRi, *Regulating Migration Tech: How the EU's AI Act can better protect people on the move* (9 May 2022); Petra Molnar (n44); Marcelo Carammia, Stefano Maria Iacus & Teddy Wilkin, 'Forecasting asylum-related migration flows with machine learning and data at scale', 12 *Nature Scientific Reports* 1457 (2022).

[70] See, Raluca Csernatoni, 'Constructing the EU's High-Tech Borders: FRONTEX and Dual-Use Drones for Border Management' 27 *European Security* 175 (2018); Petra Molnar (n30), at 314.

[71] See, for example, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (n22); at 6; Petra Molnar (n32) at 19; Matthias Monroy, 'Border surveillance: Frontex installs cameras in the stratosphere' (4 October 2022).

[72] Report of the Working Group on the use of mercenaries (n8), at §44.

[73] UN Special Rapporteur on the human rights of migrants 'Report on means to address the human rights impact of pushbacks of migrants on land and at sea: Report of the Special Rapporteur on the human rights of migrants, Felipe González Morales' A/HRC/47/30 (12 May 2021) at § 54.

[74] Report of the Working Group on the use of mercenaries (n8), at §45.

[75] *See,* for example Geoffrey Allan Boyce, Samuel N. Chambers and Sarah Launis, 'Democrats' 'smart border' technology is not a 'humane' alternative to Trump's wall', The Hill (11 February 2019).

[76] *See,* for example Statewatch (n63).

[77] Daniels, J. 'Lie-detecting computer kiosks equipped with artificial intelligence look like the future of border security' CNBC (15 May 2018, updated on 15 May 2018). For discussion of EU iBorderCtrl, *See*, Dimitri van den Meerssche (n52).

[78] Dimitri van den Meerssche (n52) at 12 (also noting that 'These systems further trade technologies of facial recognition (cross-matching images with databases) for forms of biophysiological reading – in 'analysing non-verbal micro-expressions' to 'quantif[y] the probability of deceit', iBorderCtrl claims to have moved 'beyond biometrics and onto biomarkers'.')

[79] UNGA, 'Freedom of religion or belief: Interim report of the Special Rapporteur on freedom of religion or belief, Ahmed Shaheed: Freedom of thought' A/76/380 (5 October 2021) at §§68-72.

[80] *See,* for example, iBorderCTRL, 'Frequently Asked Questions'.

[81] Nicholas Keung, 'Did Canada use facial-recognition software to strip two refugees of their status? A court wants better answers' *Toronto Star* (19 September 2022).

[82] Sam Biddle, 'ICE Searched LexisNexis Database Over 1 Million Times in Just Seven Months' *The Intercept* (9 June 2022) (discussing the US Immigration and Customs Enforcement Agency).

[83] Nina Wang, Allison McDonald, Daniel Bateyko & Emily Tucker, *American Dragnet: Data-Driven Deportation in the 21st Century*, Center on Privacy & Technology at Georgetown Law (2022) at 62.

[84] For a discussion on such practices, see Robert Koulish & Kate Evans, 'Injustice and the Disappearance of Discretionary Detention under Trump: Detaining Low Risk Immigrants without Bond', ILCSS Working Paper # 5 (22 May 2020); Lorna McGregor, *Detention and its Alternatives under International Law* (forthcoming OUP 2023), chapter 6.

[85] OHCHR, 'The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights' A/HRC/48/31 (13 September 2021); Niovi Vavoula, 'Artificial Intelligence (AI) at EU Borders: From Automated Processing to Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism' 31(4) *European Journal of Migration and Law* (2021) 457; Lorna McGregor, Daragh Murray and Vivian Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability' 68 *International and Comparative Law Quarterly* 309 (2019) at 338.

[86] Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (n22); Ruha Benjamin, *Race After Technology* (2019); Safiya Noble, *Algorithms of Oppression* (2018), Nanjala Nyabola, *Travelling While Black: Essays Inspired by a Life on the Move* (2021)

[87] *See,* for example, McGregor et al (n85).

[88] Robert Koulish & Kate Evans, 'Injustice and the Disappearance of Discretionary Detention under Trump: Detaining Low Risk Immigrants without Bond', *ILCSS Working Paper* # 5 (May 22, 2020).

[89] Ibid.

[90] ODIHR, *Policy Brief: Border Management and Human Rights Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context* (2021), at 24.

[91] Jordana Signer, Bill Frelick and Clara Long, 'Dismantling Detention: International Alternatives to Detaining Immigrants', *Human Rights Watch* (3 November 2021); Tosca Giustini, Sarah Greisman, Peter Markowitz, Ariel Rosen, Zachary Ross, and Alisa Whitfield, *Immigration Cyber Prisons: Ending the Use of Electronic Ankle Shackles*, Benjamin N. Cardozo School of Law, Kathryn O. Greenberg *Immigrant Justice Clinic*; Christina Fialho of Freedom for Immigrants; and Brittany Castle and Leila Kang of the Immigrant Defense Project (July 2021); Petra Molnar (n32); Lorna McGregor (n84); Nicola Kelly, 'Facial recognition smart watches to be used to monitor foreign offenders in UK' *The Guardian* (5 August 2022).

[92] UN Committee on the Protection of the Rights of All Migrant Workers and their Families, 'General Comment No. 5 (2021) on migrants' rights to liberty and freedom from arbitrary detention and their connection with other human rights', CMW/C/GC/5 (21 July 2022), at §48.

[93] *See*, for example, the six information systems already in operation or shortly to be introduced within the EU (discussed further below).

[94] *See*, for example iBorder control (discussed below). See, PERSONA Project, *D2.1: A study of latest and new generation no-gate crossing point solutions* (30 June 2021) (providing a range of examples of States' piloting of ABC technologies as well as forecasting the future development of smart technologies in this space).

[95] Marie McAuliffe, Jenna Blower, and Ana Beduschi (n18).

[96] Mark Latonero and Paula Kift, 'On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control' *Social Media + Society* (2018).

[97] Once operational ETIAS (discussed further below) will require applicants to provide information on educational attainment (Article 17).

[98] Ibid.

[99] Petra Molnar (n44); Mizue Aizeki and Paromita Shah, 'HART Attack: How DHS's massive biometrics database will supercharge surveillance and threaten rights' *Immigrant Defense Project, Just Futures Law and Mijente* (2022); See also Mizue Aizeki, Laura Bingham, Santiago Narváez, 'The Everywhere Border: Digital Migration Control Infrastructure in the Americas,' R3D, Immigration Defence Project, and Temple Law School.

[100] See draft Annex III (Art 7), Article 9, Article 83 and Annex IX.

[101] Mizue Aizeki and Paromita Shah (n99), at 8.

[102] Ibid, at 4.

[103] Regulation 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, Article 1; Regulation 2019/817 on establishing a framework for the interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861. See also, 2017/2226 (Article 8, Interoperability with VIS), (building in interoperability); ETIAS Regulation (n35), Article 11. Within the UN, there is also an increased focus on the interoperability of databases and information systems within particular agencies (for example UNHCR's Population and Identity Management System (PRIMES) and between different UN agencies.

[104] Chris Jones, '*Data Protection, Immigration, Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status*' *Statewatch and Picum* (2019), at 14.

[105] Fundamental Rights Agency, 'Interoperability and fundamental rights implications Opinion of the European Union Agency for Fundamental Rights' FRA Opinion 1/2018 [Interoperability] (11 April 2018) (referring to the Common Identity Repository specifically).

[106] Chris Jones (n104); *See also*, Niovi Vavoula, 'Interoperability of European Centralised Databases: Another Nail in the Coffin of Third-Country Nationals' Privacy?' *EU Migration Law Blog* (8 July 2019).

[107] Article 7(2) (providing that '[a]ny Member State which decides, if provided for under and in accordance with national law, to use ECRIS-TCN for purposes other than those set out in paragraph 1 in order to obtain information on previous convictions through ECRIS, shall,… notify the Commission of such other purposes and any changes to such purposes'.) *See also*, Statewatch, 'EU: Tracking the Pact: Access to criminal records for "screening" of migrants' (26 July 2022).

[108] Human Rights Watch, 'UN Shared Rohingya Data Without Informed Consent,' (15 June 2021),

[109] Ken Klippenstein and Sara Sirota, 'The Taliban have Seized U.S. Military Biometrics Devices' *The Intercept* (17 August 2021) Eileen Guo and Hikmat Noori, 'This is the real story of the Afghan biometric databases abandoned to the Taliban' *MIT Technology Review* (30 August 2021).

[110] Petra Molnar (n44) at 53; Mizue Aizeki and Paromita Shah (n99); Privacy International, 'What Now After Two Decades of Building Data-Intensive Systems?'; Mark Latonero and Paula Kift (n96); Dragana Kaurin, 'Space and imagination: rethinking refugees' digital access' *UNHCR Innovation Service* (April 2020).

[111] Chris Jones (n104) (quoting the European Commission as stating that ' "[p]rovided that the necessity will be demonstrated, decentralised systems such as those operated under the Prüm framework, the Passenger Name Record (PNR) Directive and the Advance Passenger Information Directive may at a later stage be linked up to one or more of the [interoperability] components"') and Dimitri Van Den Meerssche (n52) (noting that, 'iBorderCtrl and Tresspass also promise an architecture of interoperability: both systems are tied to an array of public databases (SIS II, VIS and EURODAC) and aspire to connect with data from social media platforms such as Twitter, Facebook, Instagram and Google+ as well as private credit card providers'). See also Niovi Vavoula (n106); Statewatch, 'Future Group on Travel Intelligence and Border Management' (7 September 2021).

[112] OHCHR (n1), Guideline 10, §11.

[113] Privacy International, 'The EU, the Externalisation of Migration Control, and ID Systems: Here's What's Happening and What Needs to Change' (15 October 2021); *See also*, Statewatch, Building the Biometric State: Police powers and discrimination (28 February 2022).

[114] ODIHR (n90), at 18.

[115] Refugee Law Lab and EDRi (n69) at 21.

4. Recommendations on how to close protection gaps at digital borders

This study analyses some of the far-reaching human rights implications of digital border technologies. While few dedicated laws currently exist at the national, regional or international level regulating the design, development, or deployment of digital technologies used at borders specifically, or AI more generally, the use of digital border technologies does not arise in a regulatory void. States remain obligated to comply with international human rights law and both States and companies should comply with the UN Guiding Principles on Business and Human Rights. However, lack of adherence to these obligations and responsibilities is creating protection gaps in the use of digital border technologies.

Rather than attempting to offer a comprehensive set of recommendations, this study reaches four overarching sets of conclusions and makes recommendations for each aimed at resetting the conversation about digital border technologies, while recognizing that comprehensive guidance on this complex topic requires multi-layered strategies.

First, the deployment of digital border technologies is more likely to result in human rights harm to people on the move where they are introduced as part of securitised border governance policies aimed at preventing migration and with inadequate and ineffective human rights protections in place. The study therefore recommends that States and businesses comply with their respective and existing human rights obligations and responsibilities in constructing and pursuing border governance policies. Second, where a robust human rights protection framework is in place, the study makes recommendations on how proposals to introduce digital border technologies should be assessed and where approved, highlights the necessary processes for their monitoring and oversight, and access to a remedy and accountability where human rights harm occurs. Third, some digital border technologies inherently conflict with human rights standards and norms or present such a serious risk that cannot be adequately protected against and should therefore not be used, but rather subject to a ban. While not providing a comprehensive list of technologies that meet this threshold, we provide examples of technologies currently in use that should be reconsidered and, where applicable, prohibited. Fourth, the study recommends stock-taking by States of all digital border technologies currently in use within their jurisdiction or under their control; publication of a list of those digital technologies now in use as part of a commitment to ongoing public transparency; and subjecting such technologies to human rights impact assessments that are publicly accessible and open to scrutiny. Where existing technologies are found to present potential or actual adverse human rights impacts, we recommend that they are discontinued unless and until such harm can be meaningfully mitigated, and compliance with international human rights standards and norms ensured. Where this is not possible, we recommend that these technologies are withdrawn from use. Finally, the study echoes the request from the UN Secretary-General for OHCHR to provide practical recommendations and guidance to States and other stakeholders regarding the use of digital technologies in border governance.

In constructing, developing and operationalising a human rights-based approach to migration and the governance of digital border technologies, the voices and experiences of people most affected by such technologies must be foregrounded. This requires the fostering of conversations and the establishment of meaningful knowledge-exchange and participatory mechanisms between affected communities and policymakers, academics, technologists, and civil society on the risks and promises of using new technologies that that ensure the protection of human rights, regardless of the case made for the deployment of digital border technologies. It also requires the ongoing involvement of mobile communities in discussions around the development and deployment of digital border technologies before their deployment of border technologies and not after the fact.

A. Starting Point: a Human Rights-Based Approach to Border Governance

When digital border technologies are embedded as part of wider securitisation strategies, or when private actors operate new and emerging digital technologies without adequate and effective human rights safeguards in place, the deployment of digital border technologies is more likely to result in human rights harm to people on the move. The use of digital border technologies aimed at detecting people on the move at and near physical borders, predicting migration movements, identifying people with alleged irregular status within a State's territory, making risk assessments of migrants and refugees, or providing so-called 'alternatives' to detention, all involve substantial human rights risks.

It is critical that the design, development and deployment of all digital border technologies are subject to robust human rights protections. However, such an approach will be insufficient without also addressing the reasons for their proliferation. A policy shift that commits to a human rights-based approach to border governance rather than an approach based on securitisation and exclusion coupled with a lack of safe and regular migration pathways is essential.

A human rights-based approach embodies international human rights law, standards and norms. Central to this approach are the principles and values underpinning the international human rights framework such as human dignity, inclusion, participation, empowerment, transparency as well as accountability, remedy, equality, and non-discrimination. In the context of migration, a human rights-based approach therefore constitutes a critical counter to racism, discrimination, stereotyping, exclusion, and othering by underscoring the inherent and inalienable human rights of all people on the move, regardless of their nationality or migration status, and promotes the rights, participation and empowerment of people on the move as central to all aspects of migration governance.[116]

A human rights-based approach to migration requires States to meet both their human rights obligations in law, policy and practice and for businesses to adhere to their human rights responsibilities under the UN Guiding Principles on Business and Human Rights through formal policies and operational practice. In addition to compliance with substantive human rights standards and norms, a human rights based approach to migration necessitates the establishment of independent, impartial and effective monitoring, oversight, accountability, and remedial frameworks. It similarly requires that people affected are adequately consulted and are able to effectively access information and justice, including access legal counsel.

B. Ensuring Minimum Human Rights Safeguards for the Introduction, Monitoring and Oversight of Digital Border Technologies

Even where a human rights-based approach to migration is in place, human rights harm emanating from specific technologies is still possible. Dedicated and ongoing processes are thus necessary to assess any proposals to introduce digital border technologies prior to deployment, and to oversee and monitor them, where approved and in use. We therefore recommend:

(1) *Meaningful and Transparent Processes to Assess Digital Border Technologies Prior to Deployment*

This study and wider research document the lack of transparency in States' decisions to deploy digital border technologies whether directly or by private actors they contract to carry out the State function of border governance. As a baseline in the protection of human rights at borders, the burden lies with States and businesses to show that they will not cause human rights harm in their use of digital border technologies. States should develop clear and transparent processes to ensure that no digital border technologies are accepted (for example, through donations or funding by technology companies, other States or international organisations), procured or deployed without public disclosure and scrutiny of the plans to deploy them ahead of time. Public scrutiny of proposals must not be facilitated as a 'tick-box' exercise but should allow for the possibility that the proposed technology will not be procured or used when it presents too high a risk to human rights or safeguards are inadequate or ineffective.

Scrutiny of proposed digital technologies will require a staged approach. First, prior to assessing specific technological models and products within the procurement process, States should be transparent and specific on why they propose to adopt a digital border technology to address a particular issue or realise a policy goal. They should publish an initial human rights impact assessment demonstrating how the proposed digital border technology meets human rights requirements. This includes compliance with the tests of legality, necessity and proportionality, where applicable.

In proposing the introduction of a digital border technology which could interfere with human rights, States must be able to point to a legal basis for the use of the technology. This may require the enactment of a dedicated law or demonstration that the use of the technology is clear and foreseeable under an existing law. As many digital technologies involve the collection, processing, storage and sharing of personal data, where States do not have any data protection legislation or existing legislation contains exemptions for border governance, they must also address those legal deficits in order to establish a legal basis for the use of the technology.

In addition to the principle of legality, States need to explain how the technology meets the tests of necessity and proportionality and constitutes the least intrusive measure to the human rights with which its use interferes. In making this assessment, possible non-technological approaches must be considered and compared to the proposed technological solution. Key principles of data protection will also be relevant such as demonstration of strict adherence to the principle of data minimisation and purpose limitation in addition to the clear establishment of firewalls to prevent data sharing with other state agencies or private actors. A person's ability to consent should be analysed contextually, paying particular attention to areas with fraught power differentials which may weaken, if not vitiate, consent.

Second, where the proposal for the introduction of a technology is generally accepted, further impact assessments will be required into specific uses and providers. Where private actors bid for a government contract, they should include a human rights impact assessment with their proposal. However, the State is still under a separate obligation to conduct an ongoing and iterative assessment of potential and real impact of the technology as well as the private actors under consideration. This assessment should be conducted by an independent and impartial entity, in consultation with relevant stakeholders, including migrants and refugees, and should be published in full prior to a decision being taken to allow for transparency and public scrutiny during the procurement process. Each impact assessment should include:

- Details on the specific technological product;
- How the specific technological product and providers/operators have been assessed against other non-technological and technological options and providers/operators;
- Full details of data acquisition and sharing arrangements;
- Full details on the purpose(s) and planned use case(s) of the technology;
- The providers' explanations as to how the technology can meet the State's goals;
- The State's assessment of the legality, necessity and proportionality of the use of the specific technology relative to its stated aim; and
- The safeguards in place to mitigate adverse human rights impacts.

The same process should be adhered to where private actors offer to 'donate' digital border technologies to States or international organizations, or to facilitate a trial of the technology.

Once selected, further transparency and public scrutiny will be required on the technology(ies) and the actors involved in developing and deploying the technology, including State, private, and international entities with specification of their role and relationship to the State, for example, in supporting its operation, accessing and using the data gained from the system, and in making decisions based on the data produced. As above, the original impact assessment should be updated on this basis or a new one produced.

(2) *Regular Review and Ongoing Oversight*

In order to ensure that people on the move can effectively participate in such assessments without fear of repercussions, independent bodies should be fully resourced to collect views in anonymised form. Impact assessments should be made publicly available for other actors to scrutinise and challenge, where necessary. States should also ensure that they have established and fully resourced impartial and independent oversight bodies capable of investigating the use of border digital technologies.[117]

It is critical that such oversight bodies have full capacity to access the information they require to assess the technologies being deployed and their implications for the human rights of migrants and refugees without any barriers such as claims of proprietary interest by the technology providers and that they have the requisite expertise to make such assessments both from a technological and human rights perspective (which should be understood as connected to, but not conflated with, data protection). Where they find that the technologies do not comply with human rights standards and norms, their mandate should allow them to require the suspension or termination of the use of the technology unless and until adequate and effective protections can be put in place.

(3) *Access to Adequate and Effective Remedies*

As set out above, impartial and independent complaints-handling bodies should be put in place with competence to receive and investigate complaints in relation to border governance and to issue binding decisions aimed at holding actors to account for human rights harms and ensuring that migrants and refugees receive adequate and effective remedies and reparation. As with monitoring and oversight bodies, complaints-handling bodies must be well-resourced, able to access the information they require to reach a decision on a complaint, and have relevant expertise in digital border technologies as well as the human rights of people on the move.

In order for people on the move to exercise their right to access to justice and to a remedy and reparation and for complaints-handling bodies to assess their complaints, States and businesses must be fully transparent in their use of digital technologies. This includes the provision of meaningful information such that an individual can understand whether the use of the technology has affected their human rights and if so, how. Furthermore, in situations where additional technical expertise is required to understand the use of a particular technology, the time required to gain access to, and analyse, the technology may result in the person being denied entry or removed before their claim is resolved. To avoid such barriers to access to justice, the burden should be placed on the actors using the technology to make it understandable to those to whom it has been applied.

C. Refraining from the Use and Banning Digital Border Technologies that Present Inherent or Severe Harms to Human Rights

A range of new technologies raise such serious concerns that refraining from their use may be the best way to avoid human rights harms. In 2021, the then UN High Commissioner for Human Rights stated that 'a risk-proportionate approach to legislation and regulation will require the prohibition of certain AI technologies, applications or use cases, where they would create potential or actual impacts that are not justified under international human rights law, including those that fail the necessity and proportionality tests.'[118] Too little is currently known about all of the types of technologies being used or their full human rights impact to offer a full and comprehensive list of technologies that would meet this threshold. Further, technologies are continually being developed and deployed. However, as stated by the former High Commissioner, it is critical to articulate how international human rights standards and norms apply to the use of digital border technologies and to develop a process to identify and establish where technological bans are appropriate, particularly given the positional vulnerability and power differentials entailed in border governance.

As a starting point, certain forms of technology will be inherently incompatible with human rights and should therefore not be used. Technologies that are explicitly designed to circumvent human rights standards or cannot be designed without such an effect, even if unintentional,[119] or undermine the essence of the right will reach such a threshold and therefore merit a ban.[120] For example, OHCHR has previously called for the prohibition of 'uses of AI that inherently conflict with the prohibition of discrimination' and international human rights law more generally, pointing to 'social scoring of individuals by Governments or AI systems that categorize individuals into clusters on prohibited discriminatory grounds,'[121] which in the border governance context can result from the use of characteristics such as nationality, ethnicity, race, or religion as part of algorithmic risk assessments. The use of emotion recognition technologies, such as polygraphs, to try to infer how a person feels, what they think, or the veracity of what they are saying, is not only technologically flawed but also highly likely to result in discriminatory, bias, and stereotyped outcomes and interfere with freedom of thought and therefore provides another example of a digital border technology which should be refrained from use and banned.[122] As also discussed in this study, remote biometric technologies raise serious concerns with regard to their proportionality as well as possible discriminatory outcomes from their use. At borders, their use may lead to identification, detention, and removal. Against this background, aligning with the growing number of decisions by various legislative and administrative bodies to ban remote biometric technologies in public spaces,[123] States should refrain from using such technologies at borders.

D. Stock-Take and Impact Assessment of Technology Already Deployed

Finally, as discussed throughout this study, States have deployed digital border technologies often without full transparency or subjecting them to an independent and impartial human rights impact assessment, oversight or monitoring. We recommend that all States conduct a stocktaking of technologies that are already in use and review their human rights compatibility by carrying out human rights impact assessments of these technologies individually and collectively. They should also review whether the legal, policy, institutional, and operational frameworks they have in place offer robust human rights protection for the use of digital border technologies as set out above, including monitoring, oversight, and complaints-handling bodies. In conducting such a review, States should assess the adequacy and effectiveness of overall data protection frameworks, including by ensuring that where personal data is collected, processed, stored and shared, they strictly adhere to the principle of data minimisation and purpose limitation including reviewing any areas of the repurposing of data and the compatibility of any large scale or interoperable databases with such principles. They should also ensure that clear firewalls are in place between border enforcement agencies and other State agencies, particularly those responsible for the delivery of rights and services, and those engaged in criminal justice and national security.

While carrying out such a review, we recommend that States discontinue the use of any technology which is alleged to produce human rights harms, in order to create space to assess whether such harms can be mitigated and compliance with international human rights law ensured. Where they cannot, the technology should be withdrawn. For example, the Working Group on the use of mercenaries has underscored that,

> [w]here the use of certain technologies is found to have contributed to or directly caused human rights violations and abuses, States should discontinue or revise their use to ensure they are used in line with their international law obligations only. They should communicate the findings to companies with requirements regarding modifications of their products and services, or notification of the discontinuation of the use of the technologies.[124]

Similarly, OHCHR has recommended that States 'implement moratoriums on the domestic and transnational sale and use of surveillance systems, such as hacking tools and biometric systems that can be used for the identification or classification of individuals in public places, until adequate safeguards to protect human rights are in place.'[125] Such action prevents further roll-out of digital border technologies without adequate and effective frameworks in place to properly assess and address their potential human rights impact. This approach also creates the space for the reassessment of digital border technologies which may have already been deployed without a human rights impact assessment or public scrutiny of their legality, necessity, and proportionality.

E. Bridging the Gap: Advancing Practical Recommendations and Guidance

In order to improve human rights protection and bridge existing gaps, in addition to the recommendations set forth in this study, we echo the request of the UN Secretary-General for OHCHR to provide practical recommendations and guidance regarding the use of digital technologies in border governance in consultation and collaboration with States and other stakeholders to effectively address human rights risks and challenges in this context.[126]

Endnotes

[116] OHCHR, *Towards a human rights-based approach to migration: training guide* (2023).

[117] OHCHR, 'The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights' A/HRC/39/29 (3 August 2018) at §40 (on oversight frameworks).

[118] OHCHR (n85), at §45.

[119] McGregor et al (n85), at 335.

[120] OHCHR, 'The right to privacy in the digital age' A/HRC/51/17 (4 August 2022) at §19 and 56; OHCHR (n85) at §6;

[121] OHCHR (n85), at §45.

[122] Vidushi Marda (ARTICLE 19) and Ella Jakubowska, 'Emotion (Mis)Recognition: is the EU missing the point?' EDRi, (2 February, 2023).

[123] *See*, for example European Parliament, 'MEPs ready to negotiate first-ever rules for safe and transparent AI,'(14 June 2023).

[124] Report of the Working Group on the use of mercenaries (n8).

[125] OHCHR (n85); at §45. See also, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (n22), at §6 and 62.

[126] Report of the Secretary General on the human rights of migrants, A/HRC/54/81 (2023) at §83.

essex.ac.uk