Human Rights and Digital Border Governance

Opportunities and Challenges for the New OHCHR Guidance

Ben Hayes

09.12.2025 doi: 10.59704/247b42409c5abc2e

OHCHR's forthcoming guidance on human rights-based digital border governance consolidates legal standards for data-intensive migration and border control. This contribution identifies where such guidance can help, and where a significant shift in current State practice is needed: clear legal basis and safeguards for intrusive practices, data sharing and interoperability, oversight of algorithmic systems, human rights impact assessment, and the use of security and emergency regimes that dilute rights protections. Each area is framed by the need to ensure legality, necessity and proportionality, non-discrimination, and effective remedy.

Why the new guidance?

Under instruction from the UN Secretary-General, OHCHR was requested to draft Principles and Guidelines on Human Rights-Based Digital Border Governance (hereafter: "guidance"). The initiative builds on a report on the same topic produced by OHCHR and Essex University in 2023. Key issues addressed by the guidance include: (i) biometrics and large databases, (ii) risk screening and profiling, (iii) automated and AI-assisted decision-making, (iv) intra- and inter-state data sharing, and (v) private-sector participation. While the guidance will not be binding on States, it draws on best practice including developments in data protection law and AI regulation. OHCHR also benefited from the mapping conducted by the AFAR project and consultation on the draft with the AFAR team.

Legal basis and safeguards

IHRL requires a clear, accessible, and foreseeable legal basis for interferences with rights, together with appropriate safeguards. Some human rights are absolute, and their violation can never be justified. In the migration context, such rights include *non-refoulement* and the prohibition on torture and inhuman and degrading treatment, and the prohibition of collective expulsion. There is no possible justificatory legal basis for the use of technology that enables such violations. Qualified rights may be subject to justifiable limitations, provided they are necessary, proportionate and based in law.

The deployment of digital border governance technologies often limits the rights of people on the move but the lawful basis is not always clearly established. Border and migration authorities often rely on broad enabling statutes or controller authority for data processing, which is insufficient where intrusive measures are used. Mobile phone extraction is a paradigmatic example: blanket seizure and compelled disclosure of credentials are highly intrusive and demand strict necessity, targeted authorisation, and independent oversight. Courts have begun to restrict indiscriminate practices.[1]

[1] ARJ17 v Minister for Immigration and Border Protection [2018] FCA 909 (Federal Court of Australia); *R v Canfield* 2020 ABCA 383 (Alberta Court of Appeal); Office of the Privacy Commissioner of Canada, "CBSA searches of travellers' digital devices" (2020); District Court of The Hague (Rechtbank Den Haag), various asylum judgments 2020–2022 (unreported, see Lina Alajäk, Zeynep Özkul, Koen Leurs, Karin de Dekker, Ali Salah, *Digital disruption and data-driven migration management: perspectives from Europe* in *Forced Migration Review* 73 (June 2023); Civil Court of Milan, Judgment of 2021 (unreported, asylum detention case, see Civil Court of Milan, Judgment (2021), see Petra Molnar, *Technological Testing Grounds* (Statewatch/EDRi, 2022, 16); High Court of Justice (Administrative Court), Judgment of 25 March 2022 – *HM v Secretary of State for the Home Department* [2022] EWHC 695 (Admin); Federal Administrative Court (Bundesverwaltungsgericht), Judgment of 16 February 2023 – 1 C 19.21; Nabrdalik & Moskwa v. Poland, concerning the detention of two photojournalists and the extraction of data from their mobile devices during a declared state of emergency at the Polish-Belarussian border, will shed further light on the legitimacy of MPE at international borders.

Data sharing and interoperability

The systematic sharing of migration-related data within and between states, and with private actors, is another area of concern. Such practices raise serious risks that key privacy safeguards will be eroded, in particular purpose limitation and proportionality. Interoperability demands greater attention to these safeguards. Opening disparate systems to cross-searches or automated matching enhances surveillance capability and facilitates repurposing. Human rights safeguards must travel with the data, including transfer controls, audit trails, and effective access, rectification, and redress. However, binding agreements regulating transfers appear the exception rather than the rule.

Automated systems and meaningful review

The draft guidance also addresses the growing use of automated decision-making (ADM) and AI in digital border governance (see other articles in this collection). While data protection law and emerging AI regulations contain important safeguards, including the right of individuals not to be subject to ADM producing significant legal effect on an individual, this leaves a significant lacuna – insofar as AI may be used in multiple processes that support decision-making and impact human rights (for example through documentary or behavioural analysis which produces recommendations but does not constitute ADM in law). This exacerbates concerns about the implementation of the 'human in the loop' principle, the veracity of human review of ADM, and the extent to which these requirements will provide meaningful oversight (rather than a "rubber stamp"). (See EDPS–FRA Joint Opinion (2021); UNGA Special Rapporteur (A/75/590, 2020); UNHCR, Discussion Paper (2021); CoE CAHAI(2020)23, 2020; EU FRA Getting the Future Right)

OHCHR has called for moratoria on the deployment of AI use cases that present unacceptable human rights risks, and the EU AI Act introduces some prohibitions. Nevertheless, the private sector continues to devise high-risk uses cases and AI regulation remains uneven or absent in much of the world. The guidelines affirm that AI systems that cannot demonstrably mitigate risks and ensure compliance with IHRL should not be deployed.

Risk assessments matter

To address this challenge, the guidance urges States to undertake comprehensive risk assessments to identify and mitigate human rights risks arising from the deployment of digital border governance technologies. This reflects the growing use of risk assessments across of a range of complex policy domains, from environmental impact to AI. Specifically, the guidance recommends the systematic use of human rights impact assessments (HRIAs), supplemented where necessary by privacy/data protection impact assessments (PIAs/DPIAs, which are legal requirement for high-risk processing operations in many jurisdictions), and algorithmic impact assessments (AIAs), which are required or recommended where AI is developed by public authorities.

While these assessment tools offer distinct frameworks for identifying and mitigating the risks they address their methodologies overlap,[2] suggesting significant (though largely unexplored) scope for consolidation. This could remove the need for duplication where multiple assessments of the same digital border governance systems are required by law or recommended as best practice.

Currently, HRIAs appear vastly underutilised in respect to digital border governance initiatives. Indeed, beyond the "fundamental rights implications" annexed to a handful of European Commission impact assessments, evidence of HRIAs in this area is vanishingly thin. Concern at such a low bar is exacerbated by the challenges that HRIAs present: they are complex and highly technical, requiring in-depth research and analysis, specialist expertise, extensive stakeholder consultations, and commensurate resourcing. There is

[2] All require: (i) extensive scoping to understand and document system purposes, use cases, stakeholders and context; (ii) the mapping of risks and potential adverse impacts; (iii) risk assessment and consultation of relevant stakeholders, including those affected by the system; (iv) the development of appropriate mitigating measures and safeguards; (v) documentation and transparency of the findings; (vi) review and iteration to take into account of systems changes and evolving risks.

also a surprising lack of authoritative guidance on how to conduct HRIAs beyond the Danish Institute for Human Rights' widely respected toolkit for HRIA of digital activities – which amounts to 261 pages. While States are inevitably keen to simplify assessment processes, shortcuts and checklists risk undermining the value and validity of the exercise, particularly the requisite necessity and proportionality tests.

Given the current lack of transparency in digital border governance and the lack of alternative means to comprehensively address and mitigate the adverse human rights impact of new technologies prior to their deployment, political commitment and considerable resources are needed to ensure that States do conduct HRIAs, that those assessments are rigorous and comprehensive, and that the findings determine not just how the technology is deployed, but if it should be used at all.

Security and emergency regimes

Finally, attempts to institutionalise human rights-based approaches risk frustration by the invocation of regimes that place limits on the application of IHRL. Since the '9/11' terrorist attacks, States have increasingly asserted that migration and border control is a national security issue. This conjunction has had significant effects, framing people on the move as an implicit security threat resulting in the differential and harmful treatment of "suspect communities". After 9/11, States invoked concern with terrorism as a justification for the detention and expulsion of third country (and even dual) nationals. More recently, these practices have been supplanted by the systematic national security screening of asylum-seekers, applicants for visas and residence permits, and international travellers whose entry into many countries now requires pre-authorisation. This is a remarkable shift whose underlying assumption is that "all travellers are put under surveillance and are considered a priori as potential law breakers". The ensuing screening systems, now required under a Chapter VII UN Security Council Resolution 2396, incorporate various methods impacting human rights: the collection and analysis of a wide range of data points, the transnational pooling of national security "watchlists", the inclusion of protected characteristics in risk profiles, and the use of AI and automated decision-making to determine the risk posed by specific individuals. All of this raises important questions about necessity, proportionality, non-discrimination, procedural fairness and access to remedies.

The blurring of the boundaries between administrative immigration procedures and national security has also resulted in broad exemptions to legal frameworks that should protect the rights of people on the move and facilitate public scrutiny of State practices. Most data protection regimes exempt data processed for national security purposes. The EU AI Act fully exempts AI systems used for national security purposes and limits transparency requirements for those systems used for migration and border control. This will likely undermine attempts by civil society and human rights bodies to hold operators and systems to account, and may hamper the work of regulators with a formal oversight mandate.

An increase in the use of emergency powers by States to counter so-called "mass influxes" of migrants may have the same effect. In recent years, at least 11 countries across the Americas, southern and eastern Europe have declared national or localised states of emergency (or similar crisis regimes) for this purpose.[3]

These have seen military forces deployed to support border authorities; restrictions on asylum rights; fast-track detention and expulsion; broader powers to conduct identity checks and search-and-seizure; the expanded use of surveillance drones and biometric systems; and the restriction of public and media access to border areas.

While States assert that the use of emergency powers is strictly required by the exigencies of the situation (and thus in accordance with IHRL) the suspension of constitutional and human rights, due process and oversight is fundamentally at odds with human-rights based approaches. The expansion and repeated renewal of emergency migration decrees by States risks the normalisation of extended contain-

[3] Chile, Costa Rica, Ecuador, Hungary, Italy, Latvia, Lithuania, North Macedonia, Peru, Poland, United States.

ment and the implementation of unaccountable digital border governance regimes, whose deployment may be fast-tracked in the absence of scrutiny or safeguards. The guidance reminds States that national security should not be used as a pretext for vague or arbitrary limitations on human rights.

Where next?

OHCHR's guidance clarifies baseline human rights requirements for the deployment of digital border governance technologies. At a minimum, States should conduct comprehensive, pre-deployment HRIAs, enhance transparency, institute oversight mechanisms capable of addressing the inherent risk of new technologies, and provide meaningful forms of redress. Without this recalibration, enhanced digital border governance continues to represent a huge risk to vulnerable and marginalised communities.

ABOUT THE AUTHOR

Ben Hayes

Ben Hayes is a consultant to the United Nations Office of the High Commissioner for Human Rights (OHCHR) on digital border guidance.Ben Hayes is a consultant to the United Nations Office of the High Commissioner for Human Rights (OHCHR) on digital border guidance.

SUGGESTED CITATION

Hayes, Ben: Human Rights and Digital Border Governance: Opportunities and Challenges for the New OHCHR Guidance, Verfassungsblog, 09.12.2025, doi: 10.59704/247b42409c5abc2e.

Licensed under CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20251209-172150-0.