10 September 2025 POL 30/0290/2025

Advocacy Briefing for Defending the Rights of Refugees, Asylum Seekers, and Migrants in The Digital Age

Illustration by Eliana Rodgers: "A Dream Deterred".
A migrant is confronted by mass surveillance at a border crossing and is reminded of his uncertain future. Activists work to resist these surveillance systems and walls.

Cover image for Amnesty International's primer 'Defending the rights of refugees and migrants in the digital age', 2024, Index: POL 40/7654/2024.

Contents

Introduction

Amnesty International is a global movement of more than 10 million people who are committed to creating a future where human rights are enjoyed by everyone. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

The #ProtectNotSurveil is a Europe-based coalition of activists, organisations, researchers and more working to ensure that digital and migration policies safeguard people on the move from harms emanating from AI systems. Our mission is to challenge the use of digital technologies at different levels of EU policies and advocate for the ability of people to move and to seek safety and opportunity without risking harm, surveillance or discrimination. Our advocacy aims at holding accountable the EU, Member States and private companies profiting from human rights violations at and within the EU borders. We do so by connecting digital rights, migrant rights organisations and racial justice movements to challenge the techno-solutionist approaches in migration policies.

About this document

This document is intended as an advocacy resource for activists, advocates, civil society actors and refugee and migrant communities impacted by digital technologies and surveillance in asylum and migration contexts. It provides a human rights framework and principles through which to analyse the impact of emerging and existing technologies on refugees, asylum seekers and migrants, including how to consider discriminatory and intersectional impacts. It also provides advocacy recommendations that can be taken from the document and given directly to key stakeholders developing and/or deploying digital technologies and surveillance, namely States, companies, inter-governmental organizations, and service providers.

This document was drafted by Amnesty International with the support of AlgorithmWatch, Border Violence Monitoring Network (BVMN), EuroMed Rights, and Privacy International, building on the legal and policy recommendations developed by the #ProtectNotSurveil coalition regarding migration, asylum, and border surveillance technologies, including the development and use of artificial intelligence in this domain. It is intended as a 'living' document, which will be periodically updated as key issues evolve.[1] Please note that the recommendations included are by no means exhaustive but are intended more as a starting point for national and international advocacy. The 'Resources' section at the end includes a list of publications by Amnesty International and partner organizations, where these recommendations were originally formulated.

[1] The document will be reviewed every 12 months and when we receive ad hoc crucial feedback to update recommendations. Feedback can be sent to charlotte.phillips@amnesty.org.

Glossary A-Z

Artificial Intelligence (AI)	Any technique or system that allows computers to mimic human behaviour. While there are ongoing discussions what constitutes an AI system, it is commonly defined as "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."[2]
Algorithmic decision-making (ADM)	An algorithmic system that is used in (support of) various steps of decision-making processes.
Automated decision-making	An algorithmic decision-making system with no human involvement. The decision is taken solely by the system.
Biometric (surveillance) technologies	(Surveillance) technologies used to identify human body characteristics of individuals using biologically unique markers such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements. These include for example technologies which categorise individuals based on biometric characteristics, facial recognition technologies used to identify individuals, and so-called emotion recognition technologies.
Developers	Predominantly companies and international organizations who are investing resources into building AI tools with the intent of providing these tools to other parties for use or putting the tool into action themselves.
Deployers	Those who lead the implementation of an AI tool for its final intended purposes. These can be private or public actors. A single entity such as a company or a public sector agency can simultaneously be a developer and a deployer if

[2] See OECD AI Principles overview. https://oecd.ai/en/ai-principles

	they have in-house capabilities to build AI tools themselves.
Facial Recognition technology (FRT)	Umbrella term that is used to describe a suite of applications that perform a specific task using a human face to verify or identify an individual. FRT is one of numerous biometric technologies being deployed by states and commercial entities across a wide range of use-cases.
Global Majority	A term to refer to people who are racialized, such as Indigenous Peoples, people of African, Asian, or Latin American descent, who together comprise most of the world's population. It is a term used to challenge terms like "minorities" which are often considered marginalizing language and seek to affirm collective agency and solidarity of people subjected to systemic racism and historical racial injustices.[3]
Human Rights Impact Assessment (HRIA)	A HRIA is a process for assessing human rights impact, including for identifying risks through the AI life cycle. HRIAs should include an assessment of the appropriateness of an AI-based solution in a specific scenario. This should include defining who the impacted groups are, what the foreseen impact is, whether impacted communities have been consulted and demonstrate how harm will be mitigated.
Intersectionality	A way of examining how different forms of discrimination can overlap and interact with each other to create a unique and compounding experience of oppression for an individual. It explains how an individual's experience of discrimination based on their belonging to a particular social identity group that suffers oppression because of gender, sexual orientation, race, class, caste, disability, immigration status, religion, ethnicity, Indigenous identity, age or on any other grounds - can work together to make their experience of oppression different from someone else's. It thereby goes further than

[3] See Campbell-Stephens, R.M. (2020). Global Majority: we need to talk about labels such as 'BAME'. https://www.linkedin.com/pulse/global-majority-we-need-talk-labels-bame-campbell-stephens-mbe/; Campbell-Stephens, R.M. (2021). Introduction: Global Majority Decolonising Narratives. In: Educational Leadership and the Global Majority. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88282-2_1

	acknowledging that different forms of oppression exist and examines how together they create a particular pattern of discrimination. For example, if a Black or Muslim asylum seeker is more likely to experience migration related detention, the discrimination and violation of their human rights is due to a combination of their perceived or real race, national origin, immigration, or citizenship status.
Non-refoulement obligation	The legal obligation for states not to return or transfer anyone to a place or jurisdiction where they would be at real risk of persecution or other serious human rights violations or abuses.
Profiling	The automated processing of personal data to evaluate personal aspects of an individual, such as their performance at work, economic situation, health, personal preferences or interests, behaviour, location, or movement.[4]
Racial discrimination	The International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) defines racial discrimination as: "any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life"[5]
Remote Biometric Identification (RBI)	Remote biometric identification (RBI) systems are used to identify people at a distance by comparing their unique biometric attributes with a database. Facial recognition technology is the most common example, as defined above, and can sometimes be used as a term interchangeably with RBI. RBI can be done in real-time, with instantaneous or near-instantaneous processing of

[4] See Article 4.4, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[5] Article 1, United Nations (1965). International Convention on the Elimination of All Forms of Racial Discrimination. [online] OHCHR. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial

	collected information (also called 'live RBI) or retrospectively, where analysis of captured images happens at a later point (also known as 'post RBI').
Risk Assessment tools	The semi- or fully automated processing of data for statistical assessment and/or predictive modelling to identify the risk that an outcome will occur, either at the individual or community level, or specific to an event or scenario.
Social scoring	The use of artificial intelligence and other forms of algorithmic decision-making to evaluate and classify people to make certain assessments or decisions about them. This system of evaluation or classification is usually predictive – for example, it might be programmed to infer the likelihood that a job seeker will find work, or how likely it is that a customer will repay a loan. It relies on information as wide ranging as the person's identity (such as age, gender, race, and ethnicity), past behaviour (such as their employment history or criminal records), or socio-economic situation (such as their income and educational level).[6]
Systemic racism	The United Nations Human Rights Council Advisory Committee has pointed out that racism is a systemic problem that: "operates through an interrelated or closely coordinated network of laws, policies, practices, attitudes, stereotypes, and biases. It is upheld by a wide range of actors, involving State institutions, private sector, and societal structures more broadly. It results not only in express, direct, de jure or intentional discrimination, but also in covert, indirect, de facto, or unintentional discrimination, distinction, exclusion, restriction, or preference based on race, colour, descent or national or ethnic origin. It is frequently rooted in historical legacies of enslavement, the trade in enslaved Africans and colonialism. And it tends to

[6] Adapted from Human Rights Watch, Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. https://www.hrw.org/sites/default/files/media_2021/11/202111hrw_eu_ai_regulation_qa_0.pdf

	govern opportunities and outcomes across generations."[7]

The use of digital technologies in asylum and migration contexts

Digital technologies have become ubiquitous, high-risk, and often experimental tools in shaping and delivering the migration and asylum policies of States and regional organisations, from electronic monitoring, satellites, and drones to facial recognition, "lie detectors" and iris scanning.

Both directly and indirectly, digital technologies have the potential to cause and exponentially increase a range of serious human rights violations. Where states are actively pushing an agenda which is at odds with their human rights obligations towards refugees and migrants, these technologies risk exacerbating human rights violations and suffering. The technologies used in delivering asylum and migration policies may also be problematic in their own right, as their systems are vulnerable to bias and errors and often rely on excessive collection, storage and use of information that threaten the right to privacy, non-discrimination, and other human rights. Digital technologies are reinforcing border regimes that discriminate based on race, ethnicity, national origin, and citizenship status. Inherent racism and discrimination are deeply ingrained within migration management and asylum systems. These technologies risk perpetuating and concealing racial bias and discrimination rooted in historical and colonial practices of racialized exclusion under the guise of neutrality and objectivity, including on religious grounds. Their use can result in disproportionate impacts against racialized groups and create different forms of discrimination, perpetuating systemic racism, discrimination, oppression, and violence.

In more recent years there has been the trend towards exempting technologies used for migration and border management purposes, including exemptions from privacy and data protection, public accountability and transparency requirements, and other regulatory obligations[8], within a broader shift towards punitive measures in migration and border management[9] and the conflation of migration, policing and national security policies.[10]

There is an ever growing and urgent need to call on States, companies, and other stakeholders to ensure that any development and use of technology respects and protects the human rights of all, including of refugees, asylum seekers and migrants without discrimination. Transparency is a form of safeguard and can be an important first step towards the realisation of rights, justice, and

[7] Human Rights Council Advisory Committee (8 August 2023). Advancing racial justice and equality by uprooting systemic racism, UN Doc. A/HRC/54/70, para. 7. https://documents.un.org/doc/undoc/gen/g23/140/55/pdf/g2314055.pdf?OpenElement

[8] See for example, #ProtectNotSurveil (2024). Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move. https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/

[9] Equinox Initiative for Racial Justice and #ProtectNotSurveil Coalition (2025): EU: Stop criminalising migration in the Facilitator's Package law. https://www.equinox-eu.com/eu-stop-criminalising-migration-in-the-facilitators-package-law/

[10] See for example, The New York Times (2025). Trump Calls for 20,000 Extra Officers to Help with Deportation Efforts. https://www.nytimes.com/2025/05/10/us/politics/dhs-deportation-extra-officers.html

accountability, but it cannot protect rights in isolation and must be accompanied by other safeguards. Where harm cannot be prevented or mitigated and where technologies are incompatible with international human rights law by design, these technologies must be banned.

Guiding principles and framing

States have binding obligations and duties under international human rights law meaning that they must respect, protect and fulfil human rights for all. International organizations, corporate actors, and other non-state actors must also respect human rights.

To have a human rights-based approach to this thematic area, it can be helpful to keep in mind some overarching principles and framings that should be applied to any potential technology in the field of asylum and migration (and more generally). These include:

Technology is not neutral. Financial and other incentives, structural systems of power and oppression, systemic racism, discrimination, systemic inequality, and policy environments all get baked into technology and reproduced by its use. In many instances, technology is a tool used to operationalize underlying policies which may be xenophobic or discriminatory in purpose or in practice.

Take a cautious/ critical approach to 'techno-solutionism'- the idea that complex social, economic, and political problems can be overcome by technology. Rather than assuming that the development and deployment of technologies are necessary or inevitable, whose risks can be managed through procedural fixes, it is important to fundamentally question early in the process, and on an ongoing basis, whether particular technologies are indeed necessary or useful at all or likely to meaningfully address systemic issues, without exacerbating or inadvertently creating other issues.

Ensure that all technologies respect, protect and promote human rights (both directly and indirectly), including but not limited to non-discrimination, privacy, right to life, right to seek asylum, the right to liberty and the principle of non-refoulement. This also includes when technologies are exported to other jurisdictions.

Intersectionality is key. States and companies should assess both direct and indirect risks and impacts of the technology design and its use. This must be done early, during pre-deployment and on an ongoing basis, and should be done with an intersectional lens. This means that states, companies, and other actors need to examine how different forms of discrimination can overlap and interact with each other at any time to create a unique and compounding experience of oppression for an individual or groups interfacing with technologies.

Measures put in place to regulate technologies should be **binding and enforceable.** This is especially important as there are already many soft, non-binding ethical codes, code of conducts, and guidelines out there that often do not ensure adequate protection.

Freedom of information is a crucial component of the right to freedom of expression.[11] States, companies and other actors must ensure **transparency, accountability, and accessibility** of information, including to enable public scrutiny and participation in policymaking for a range of stakeholders including impacted rights holders. This includes transparency on the roles and responsibilities of those involved in development, procurement, and implementation. While transparency is important, it is only a first step and not sufficient on its own.

States, companies, and other actors must ensure **meaningful participation of impacted communities** and the centring of policy discussions around needs and priorities of those communities, enabling equal participation of representative advocates and organizations through resource-allocation, creating a level-field between all stakeholders and rightsholders, and valuing experiential expertise. This includes, crucially, elevating the voices and priorities of impacted communities and civil society actors from the Global Majority.

Recommendations

Recommendations to states

Total bans

Under no circumstances should States allow the development, production, sale, use, export and import of technologies which by their very nature violate human rights, cause irreparable, irreversible harms, and/or pose unacceptable risks. In these cases, States should enact total bans. Technologies that States should prohibit include:

- Automated risk assessment, scoring and profiling systems in the context of migration management, asylum, and border control (including fraud detection systems). Used to determine whether people on the move present a 'risk' of unlawful activity or security threats, these systems are inherently discriminatory, pre-judging people based on factors outside of their control, or on discriminatory inferences based on their personal characteristics. They violate the rights to equality and non-discrimination, privacy, and data protection, as well as the presumption of innocence. They can also lead to unfair infringements on the rights to work, liberty (through unlawful detention), a fair trial, social

[11] United Nations Human Rights Committee (12 September 2011). General Comment 34, International Covenant on Civil and Political Rights. CCPR/C/GC/34, at paras. 18-19. https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

protection, or health. Automated profiling of individuals should be prohibited given the particularly high risk of discrimination in this context.

- Technologies to process or infer sensitive personal characteristics or proxies of characteristics, such as race, political affiliation, beliefs, genetic, health, and biometric data, for the purposes of individual risk-scoring.[12] This includes the use of data regarding citizenship, "foreign affiliation" and nationality. Other examples of this include using data about someone's postcode to infer socio-economic status or using data on dietary requirements as a proxy for religious belief or health status.

- Predictive technologies that generate predictions as to where there is a risk of "irregular migration." These systems can be used to facilitate preventative responses to forbid or halt movement, often conducted by third countries enlisted as gatekeepers. They risk resulting in punitive and abusive border control policies that use racial biases and stereotypes, prevent people from seeking asylum, expose them to a risk of refoulement, and threaten the right to life, liberty, and security of the person.

- AI-based emotion recognition tools, such as AI 'lie-detectors' and behavioural analytics. Systems such as AI 'lie-detectors' are pseudo-scientific technologies claiming to infer emotions based on biometric data, while behavioural analytics are used to detect 'suspicious' individuals based on the way they look, or other unrelated personal characteristics. Their use reinforces a process of racialised suspicion towards people migrating and seeking asylum and can automate discriminatory assumptions based on racial and religious biases and stereotypes, threatening the rights to non-discrimination, privacy, liberty, and fair trial. [13] The purported utility of these technologies is also underpinned by ableist notions of physical, cognitive and behavioural "normalcy" with the aim of "fixing," "curing" and essentially eradicating disability and neurodiversity.

- Retrospective (post) Remote Biometric Identification (RBI), in addition to live (real-time) RBI, such as the use of facial recognition. These technologies facilitate mass and discriminatory surveillance in all contexts, including migration and border management. They can be used to scan border areas as deterrence and part of a wider interdiction regime, preventing people from seeking asylum and undermining States' obligations under international law, particularly the obligation of non-refoulement.

- The practice of mass extraction, processing, merging and exploitation of individuals' data, including sharing of collected data between migration, welfare, policing, and national security authorities. This practice undermines established data protection principles and the right to privacy. The sharing of individual data with third countries via supranational law enforcement agencies under the guise of national security, if they are neither necessary nor proportionate or if there is a risk of human rights violations, should also be prohibited.

[12] Lighthouse Reports (2023). Whistleblower reveals Netherlands' use of secret and potentially illegal algorithm to score visa applicants. Ethnic Profiling. https://www.lighthousereports.com/investigation/ethnic-profiling/

[13] A civil society statement (2022). AI Act must protect all people, regardless of migration status. https://edri.org/wp-content/uploads/2022/12/Joint-Statement_The-EU-AI-Act-must-protect-people-on-the-move_December-2022.docx.pdf

Before deployment

In addition to clear prohibitions on technologies incompatible with human rights, ***States should, before any technology system is deployed:***

- Assess and demonstrate the legality, necessity, and proportionality of any new digital technology, as well as their value and impact. Any technology adopted must be in line with
    - the international human rights framework and principles, including the prohibition of discrimination.
    - data protection standards, including the principles of lawfulness, fairness, and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality (security), and accountability.[14]
- Refrain from enacting laws that facilitate digital (and non-digital) discrimination, reinforcing and escalating existing systems of oppression and marginalisation.
- Enact binding and enforceable rights-respecting governance frameworks around the development and deployment of digital technologies, that aim to protect and promote the rights of all, including migrants, refugees and asylum seekers. Notably, such legal frameworks must be free from blanket exemptions for national security or similar purposes, as such exemptions are neither necessary nor proportionate and can result in discriminatory impacts.
- Enact or amend established norms, policies, and laws to ensure that the use of automated decision-making systems in asylum, migration and related fields does not perpetuate discrimination based on income, race, ethnicity, religion, migration status, or any other characteristics, and ensures that such deployment complies with relevant international human rights standards.
- Impose strict accountability and public transparency obligations on all public bodies deploying digital technologies, including national security, law enforcement, migration, and border control authorities. These obligations include:
    - Establishing a publicly accessible database where they are required to disclose information regarding their digital technologies and collaboration with private developers of technologies when relevant, on where and how the technology will be/is being used.
    - Based on the obligation to ensure equality and prevent racial discrimination, collecting and disclosing official disaggregated data and information of any discriminatory impacts.
    - Establishing a human rights risk assessment process and systematically conduct human rights impact assessments (HRIAs) and data protection impact assessments

[14] The Data Protection Commission. Principles of Data Protection. https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection

to identify and mitigate the risks to the human rights of those subject to digital border governance technologies and policies, including discriminatory impacts. These assessments should be conducted with sufficient human and financial resourcing and human rights expertise and include disaggregated data on race, ethnicity, gender, and other grounds of discrimination, in consultation with relevant stakeholders, including those impacted by the technologies. The findings and analysis of these assessments should be published and publicly available for transparency. Their results and implementation of recommendations should be overseen by an independent, public body with the mandate to enforce the applicable digital governance framework. These assessments should also be continuously conducted well before implementation and throughout the lifecycle of technologies. Any identified risks to human rights must be mitigated and prevented before deployment of the technology is allowed. Specific attention should be paid to any intersectional harms or discriminatory impacts against refugees and migrants, racialized groups, people living in poverty, older people, people with disabilities and other marginalized populations, as well as children and young people. If it is found that risks to human rights cannot be mitigated, the use of these technologies should be halted.

- Assess and address any environmental impacts of the development and deployment of technologies, considering growing evidence that these technologies rely extensively on fossil fuels, put considerable pressure on natural resources, such as land and water, exacerbating climate change and environmental degradation.[15]

- Adopt mandatory due diligence laws that require businesses involved in developing and providing technologies in the context of asylum, migration and border enforcement, including big data, AI and biometric systems, to undertake human rights due diligence, in line with international standards such as the UN Guiding Principles on Business and Human Rights and the OECD's Guidance on due diligence.

- As far as possible, explore any alternative, non-invasive (or less restrictive of rights) avenues that could meet the needs or tasks identified without unduly compromising the right to privacy, equality and non-discrimination, freedom from surveillance and other human rights abuses.

- Ensure support for impacted communities, civil society organizations and human right experts to meaningfully engage in the development and deployment of AI technologies, as well as in the implementation, monitoring, and evaluation of relevant AI regulation.

- Enact whistle-blower protections to support public accountability by AI developers and deployers of AI technologies.

[15] A civil society statement (2025). Within Bounds: Limiting AI's environmental impact. https://greenscreen.network/en/blog/within-bounds-limiting-ai-environmental-impact/#:~:text=AI%20technologies%20must%20not%20be,to%20power%20new%20data%20centres

During deployment

During the lifecycle of technologies, States should:

- Give individuals the opportunity to know about, freely provide or withdraw consent for, and challenge any measures to collect, aggregate, retain, and use their personal data. This should be done through access to information, in a language that they understand, and clear explanation about who is collecting the data, what data is being collected and how it will be used. Individuals should be given a genuine choice, without any kind of coercion, manipulation, or intimidation. It should be easy to withdraw consent and have data deleted, without fear of reprisals. This also applies where data is collected unintentionally, for example drone footage that unintentionally captures personal data.

- Oblige deployers of AI to inform individuals when decisions pertaining to them are supported by AI technologies, including by algorithmic decision-making. This should include at minimum meaningful and accessible information on how an AI assessment was reached, how their data was processed, to what extent has it shaped the final decision by a human decision-maker, as well as information on their right to appeal, redress and remedy, and existing mechanisms to seek those rights.

- Where violations do occur, hold developers and deployers liable for the human rights harms they have caused or contributed to, and for their failure to conduct adequate human rights due diligence and data protection, calling for redress, as needed.

- Ensure that individuals who have suffered human rights violations resulting from the misuse of technologies have access to effective remedies, both judicial and non-judicial, without fear of it jeopardizing ongoing asylum applications or their existing right to stay or enter. Public interest organisations must be enabled to provide support to impacted individuals to bring forward cases, as well as lodge cases on their own initiative, including through access to legal aid.

- Eliminate any discriminatory impacts or effects resulting from the use of digital technologies and take measures to prevent any form of discrimination based on international human rights law.

Recommendations to companies

Companies involved at any point in the lifecycle of technologies, including businesses involved in developing and providing technologies for asylum, migration, and border enforcement, should:

- Respect human rights wherever they operate in the world and throughout their operations – adhering to the globally acknowledged UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct.[16]

[16] UN Office of the High Commissioner for Human Rights (2011). Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, UN Doc. HR/PUB/11/04.

- Undertake human rights due diligence, systematically conducting human rights impact assessments (HRIAs) and data protection impact assessments, in line with international standards such as the UN Guiding Principles on Business and Human Rights and the OECD Due Diligence Guidance For Responsible Business Conduct.[17] These assessments should be conducted early and on an ongoing basis by those deploying the technologies with sufficient human and financial resourcing and human rights expertise and include disaggregated data on race, ethnicity, gender, age, and other grounds of discrimination, in consultation with relevant stakeholders, including those impacted by the technologies. The findings and analysis of these assessments should be published and publicly available for transparency. Their results and implementation of recommendations should be overseen by an independent, public body with the mandate to enforce the applicable digital governance framework. These assessments should also be continuously conducted throughout the lifecycle of technologies. Any identified risks to human rights, including potential discriminatory impacts, must be mitigated or prevented before deployment of the technology is allowed or continues. Specific attention should be paid to any intersectional harms or discriminatory impacts against racialized groups, people living in poverty, older people, people with disabilities and other marginalized populations, as well as children and young people. If it is found that risks to human rights cannot be mitigated, the use of these technologies should be halted.

- Explore and prioritise any alternative non-invasive avenues that could meet the needs identified, without unduly compromising the right to privacy, equality and non-discrimination, freedom from surveillance and other human rights abuses.

- Protect people's data from being used for rights-violating purposes, including ensuring principles of data minimization, security of any personal data collected and of any devices, applications, networks, or services involved in collection, transmission, processing, and storage. Give individuals the opportunity to know about, freely provide or withdraw consent for, and challenge any measures to collect, aggregate, retain, and use their personal data. This should be done through access to information, in a language that they understand, and clear explanation about who is collecting the data, what data is being collected and how it will be used. Individuals should be given a genuine choice, without any kind of coercion, intimidation, or manipulation. It should be easy to withdraw consent and have data deleted, without fear of reprisals. This also applies where data is collected unintentionally, for example drone footage that unintentionally captures personal data.

- Refrain from causing or contributing to human rights abuses through their own business activities, and address impacts in which they are involved, including by remediating any actual abuses. This should take account of the supply chain and lifecycle of the product or

https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf; Organization for Economic Co-Operation and Development (2023). OECD Guidelines for Multinational Enterprises on Responsible Business Conduct. https://doi.org/10.1787/81f92357-en

[17] Organization for Economic Co-Operation and Development (2018). OECD Due Diligence Guidance for Responsible Business Conduct. https://doi.org/10.1787/15f5f4b3-en

activity, including exports. This should also include instances of unintentional discriminatory impacts that result from the use of digital technologies in practice.

- Prevent or mitigate adverse human rights impacts linked to their operations, products, or services by their business relationships, even if they have not contributed to those impacts. Exercise any leverage they may have on these business relationships to mitigate and prevent these risks and impacts.

- Adopt transparency and accountability mechanisms, disclosing information regarding their AI technologies, including on where and how the technology will be/is being used.

- Refrain from lobbying governments to obtain concessions or advantages, such as changes in laws or policies which may result in negative impact on the human rights of others.

- Proactively engage with and meaningfully consult community organisations, especially those representing marginalised communities and civil society actors during the development of technologies.

Recommendations to international organisations (including United Nation Agencies)

- Assess and demonstrate the legality, necessity, and proportionality of developing or deploying any new technology. Any technology adopted must be in line with

    - the international human rights framework and principles, including in the prohibition of discrimination,

    - data protection standards, including the principles of lawfulness, fairness, and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality (security), and accountability.[18]

- Address risks that these tools will facilitate discrimination and other human rights abuses against anyone, establishing a human rights risk assessment process and systematically conducting human rights impact assessments (HRIAs) and data protection impact assessments to identify and mitigate the risks to the human rights of those subject to digital border governance technologies and policies, including discriminatory impacts.

    - These assessments should be conducted with sufficient human and financial resourcing and human rights expertise and include disaggregated data on race, ethnicity, gender, and other grounds of discrimination, in consultation with relevant stakeholders, including those impacted by the technologies.

    - The findings and analysis of these assessments should be published and publicly available for transparency.

[18] The Data Protection Commission. Principles of Data Protection. https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection

    - Their results and implementation of recommendations should be overseen by an independent, public body with the mandate to enforce the applicable digital governance framework.

    - These assessments should also be continuously conducted well before implementation and throughout the lifecycle of technologies.

    - Any identified risks to human rights must be mitigated and prevented before deployment of the technology is allowed. If it is found that risks to human rights cannot be mitigated, the use of these technologies should be halted.

    - specific attention should be paid to any intersectional harms or discriminatory impact on racialised people and communities, refugees and migrants, people living in poverty, older people, people with disabilities and other marginalized populations, as well as children and young people.

- Explore and prioritise any alternative non-invasive avenues that could meet the needs identified, without unduly compromising the right to privacy, equality and non-discrimination, freedom from surveillance and other human rights abuses.

- Protect people's data from being used for rights-violating purposes, including ensuring principles of data minimization, security of any personal data collected and of any devices, applications, networks, or services involved in collection, transmission, processing, and storage.

- Give individuals the opportunity to know about, freely give or withdraw consent for and challenge any measures to collect, aggregate, retain, and use their personal data, including biometric data. This should be done through access to information, in a language that they understand, and clear explanation about who is collecting the data, what data is being collected and how it will be used. Individuals should be given a genuine choice, without any kind of coercion, manipulation, or intimidation. It should be easy to withdraw consent and have data deleted, without fear of reprisals including denial of access to rights or services. This also applies when data is collected unintentionally.

- Inform individuals when decisions pertaining to them are supported by AI technologies, including by algorithmic decision-making. This should include at minimum meaningful and accessible information on how an AI assessment was reached, how their data was processed, to what extent has it shaped the final decision by a human decision-maker, as well as information on their right to appeal, redress and remedy, and existing mechanisms to seek those rights.

- Ensure that individuals who have suffered human rights violations resulting from the misuse of technologies have access to effective remedies.

- Incorporate explicit and specific safeguards against abuse of any use of technologies, including data sharing with national security agencies or county of origin States which could lead to violations of human rights.

- Ensure impacted communities can meaningfully engage in the development and deployment of AI technologies, as well as in their implementation, monitoring, and evaluation.

- Act in line with relevant human rights responsibilities and ensure that any support, including funding and technical support programmes do not lead to the proliferation of technologies that lead to the violation of the rights of migrants, refugees, and asylum seekers.

Recommendations to other service providers

To service providers deploying digital technologies in the fields of asylum, migration, border enforcement and humanitarian aid, including non-governmental organisations (NGOs) and humanitarian non-profit service providers:

- Respect human rights wherever they operate in the world and throughout their operations, including adhering to the globally acknowledged UN Guiding Principles on Business and Human Rights, the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct[19] and the Sphere standards.[20]

- Address risks that digital technologies will facilitate discrimination and other human rights abuses against anyone, including through conducting human rights impact assessments (HRIAs) with specific attention to the intersectional impact on racialised people and communities, refugees and migrants, people living in poverty, older people, people with disabilities and other marginalized populations, as well as children and young people.

- Explore and prioritise any alternative non-invasive avenues that could meet the needs identified-without unduly compromising the right to privacy, equality and non-discrimination, freedom from surveillance and other human rights abuses.

- Protect people's data from being used for rights-violating purposes, including ensuring principles of data minimization, security of any personal data collected and of any devices, applications, networks, or services involved in collection, transmission, processing, and storage. Give individuals the opportunity to know about, freely give or withdraw consent for and challenge any measures to collect, aggregate, retain, and use their personal data, including biometric data. This should be done through access to information, in a language that they understand, and clear explanation about who is collecting the data, what data is being collected and how it will be used. Individuals should be given a genuine choice, without any kind of coercion, manipulation, or intimidation. It should be easy to withdraw

[19] UN Office of the High Commissioner for Human Rights (2011). Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, UN Doc. HR/PUB/11/04. https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf; Organization for Economic Co-Operation and Development (2023). OECD Guidelines for Multinational Enterprises on Responsible Business Conduct. https://doi.org/10.1787/81f92357-en

[20] Sphere. Humanitarian standards. https://www.spherestandards.org/humanitarian-standards/

consent and have data deleted, without fear of reprisals including denial of access to rights or services.

- Incorporate explicit and specific safeguards against abuse of any use of technologies, including data sharing with national security agencies or county of origin States which could lead to violations of human rights.

Contact

Please direct any questions, concerns and feedback, including regarding accessibility of this document and requests for translation to charlotte.phillips@amnesty.org and mher.hakobyan@amnesty.org.

Resources

- Amnesty International, Primer on Defending the Rights of Refugees and Migrants in the Digital Age, February 2024, AI Index: POL 40/7654/2024. https://www.amnesty.org/en/documents/pol40/7654/2024/en/
- Amnesty International, Letter: The EU must respect human rights of migrants in the AI Act, April 2023, The EU must respect human rights of migrants in the AI Act – European Institutions Office. https://www.amnesty.eu/news/the-eu-must-respect-human-rights-of-migrants-in-the-ai-act/
- Amnesty International, Realising the Right to Social Security: Submission to the Office of the United Nations High Commissioner for Human Rights, 2024, AI Index: IOR 40/7558/2024. https://www.amnesty.org/en/documents/ior40/7558/2024/en/
- Amnesty International, Denmark: Coded Injustice: Surveillance and Discrimination in Denmark's automated welfare state, 2004, AI Index: EUR 18/8709/2024. https://www.amnesty.org/en/latest/news/2024/11/denmark-ai-powered-welfare-system-fuels-mass-surveillance-and-risks-discriminating-against-marginalized-groups-report/#:~:text=The%20Danish%20welfare%20authority%2C%20Udbetaling%20Danmark%20%28UDK%29%2C%20risks,Amnesty%20International%20said%20today%20in%20a%20new%20report.
- Denmark: Easy-to-read version: Coded Injustice: Surveillance and Discrimination in Denmark's automated welfare state, 21 May 2025, Index Number: EUR 18/9419/2025. https://www.amnesty.org/en/documents/eur18/9419/2025/en/
- Amnesty International, The Digital Border: Migration, Technology and Inequality, 21 May 2024, Index Number: POL 40/7772/2024. https://www.amnesty.org/en/documents/pol40/7772/2024/en/
- #Protect Not Surveil coalition, which Amnesty is a part of, see website: EU AI | Protect Not Surveil. https://protectnotsurveil.eu/
- #ProtectNotSuveil coalition, Joint Statement, A dangerous precedent: how the EU AI Act fails migrants and people on the move, 13 March 2024. https://www.accessnow.org/press-release/joint-statement-ai-act-fails-migrants-and-people-on-the-move/

- #ProtectNotSuveil, Joint Statement, the EU Migration Pact: a dangerous regime of migrant surveillance, 10 April 2024. https://www.accessnow.org/press-release/joint-statement-eu-migration-pact-a-dangerous-regime-of-migrant-surveillance/
- Amnesty International, USA/Global: Tech made by Palantir and Babel Street pose surveillance threats to pro-Palestine student protestors & migrants, August 2025. https://www.amnesty.org/en/latest/news/2025/08/usa-global-tech-made-by-palantir-and-babel-street-pose-surveillance-threats-to-pro-palestine-student-protestors-migrants/