Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Digital Borders and Human Rights: A Legal-Critical Analysis of Surveillance, Asylum, and Discrimination through Jurisprudence

Mishtha Sharma[a]

[a]National Law University, Odisha, India

Received 06 June 2025; *Accepted* 07 July 2025; *Published* 11 July 2025

This paper critically examines the convergence of digital technologies, including AI, biometric information, and surveillance networks, with fundamental human rights safeguards in the contexts of asylum and migration. It argues that algorithmic profiling, large-scale biometric records, and computerised risk assessments are increasingly eroding the rights to privacy, non-refoulement, liberty, and non-discrimination, thereby violating obligations under treaties such as the ECHR, ICCPR, and Refugee Convention. By examination of seminal jurisprudence such as Soering v United Kingdom, Roman Zakharov v Russia, and Biao v Denmark, the paper illustrates how digital practices too often do not meet legal protections in terms of necessity, proportionality, and justice. It highlights how such technologies disproportionately impact marginalised groups, promote opaque decision-making, and erode due process. The report concludes by recommending robust legal systems that provide for transparency, accountability, and human oversight in the application of AI and surveillance for managing migration, to safeguard basic human rights in an increasingly digitised context of border management.

Keywords: *asylum, surveillance, privacy, non-refoulement, discrimination.*

INTRODUCTION

In recent years, states around the world have increasingly integrated artificial intelligence (AI), biometric data collection, and advanced surveillance technologies into their immigration and asylum systems. From facial recognition at borders and algorithmic risk assessments for asylum claims to expansive biometric databases and predictive profiling, the governance of migration is rapidly evolving under the influence of digital tools. These technologies are often justified on the grounds of efficiency, security, and fraud prevention, but their implementation raises concerns about human rights under international law, particularly in the European Union.

This Art. Aims to analyse the intersection between emerging digital technologies and core human rights, specifically focusing on the rights to seek asylum, to privacy, and to be free from discrimination. It enquires into the extent to which these tools comply with the legal safeguards enshrined in international legal instruments, such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and especially the European Convention on Human Rights (ECHR).

Through a doctrinal, issue-led methodology supplemented by jurisprudence from the European Court of Human Rights (ECtHR), the United Nations Human Rights Committee (UNHRC) and selected national courts, this Art critically elucidates how surveillance, biometric collection and AI technologies affect legal thresholds related to asylum, liberty and equality. Case laws, including Soering v United Kingdom[1], Roman Zakharov v Russia[2], and Biao v Denmark[3], display the growing conflict between technology-infused migration policy and the fundamental rights that international law aims to safeguard.

The central argument presented here is that the intersection of digital surveillance with migration control consistently violates international legal commitments.

This becomes especially clear when viewed through the lens of fairness, necessity, and equal treatment. These principles are often used in human rights decisions but are usually overlooked in technology-related policymaking.

[1] *Soering v United Kingdom* (1989) 11 EHRR 439 (ECtHR)
[2] *Roman Zakharov v Russia* [2015] [GC] App No 47143/06 (ECtHR)
[3] *Biao v Denmark* [2016] [GC] App No 38590/10 (ECtHR)

THE RIGHT TO ASYLUM & NON-REFOULEMENT

The right to seek asylum and the principle of non-refoulement lie at the heart of refugee law and human rights. It is codified in various legal instruments and reaffirmed by judicial bodies; these principles serve as vital protections against the forced return of individuals to territories where they risk persecution, torture, or other serious harm. As migration governance becomes more digital, with the use of algorithms and biometric surveillance, the strength and reliability of legal protections are being increasingly challenged. This section outlines the legal basis for non-refoulement, its customary status, and how courts have interpreted the threshold for protection.

Treaty and Customary Law Obligations: The foundational articulation of the right to asylum appears in article 14(1) of the UDHR[4], which states that everyone has the right to seek and to enjoy in other countries asylum from persecution. Although the UDHR is a non-binding instrument, its provisions are widely regarded as customary international law, with significant influence over state practice and interpretation. More concretely, the 1951 Refugee Convention, particularly Art. 33(1)[5], enshrines the non-refoulement obligation by stating that [n]o Contracting State shall expel or return (refouler) a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened. Notably, this protection is not contingent on formal recognition as a refugee; it applies de facto to any person who fits the criteria of a refugee or faces similar risks.

Complementary protections are found in Art. 3 of the Convention Against Torture (CAT)[6], which prohibits the expulsion or return of any individual to a state where there are substantial grounds for believing that he would be in danger of being subjected to torture. Similarly, Art. 7 of the ICCPR[7], interpreted by the UN Human Rights Committee, prohibits returning individuals to face inhuman or degrading treatment, regardless of the individual's legal status.

Crucially, the principle of non-refoulement has evolved into a peremptory norm (jus cogens) of international law. This status signifies that the norm is universally binding and cannot be derogated from, even in times of public emergency or conflict. The UNHCR, in its

[4] Universal Declaration of Human Rights 1948, art 14(1)
[5] Convention Relating to the Status of Refugees 1954, art 33(1)
[6] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment 1987, art 3
[7] International Covenant on Civil and Political Rights 1976, art 7

authoritative Note on Non-Refoulement (1977), has emphasised that this principle applies irrespective of whether or not the person concerned has been formally recognised as a refugee, further underscoring its absolute character. State practice and opinio juris affirm the norm's customary law status, as recognised by legal scholars such as James Hathaway, Elihu Lauterpacht, and Guy Goodwin-Gill.[8]

Key Jurisprudence: International and regional courts have played a central role in interpreting and reinforcing non-refoulement protections. A landmark decision in this regard is the ECtHR judgment in Soering v United Kingdom.[9] In 1989. In that case, the applicant, a German national facing extradition to the United States on capital murder charges, argued that the death row phenomenon would amount to inhuman treatment. The ECtHR held that extraditing a person to a country where they faced a real risk of such treatment would violate Art. 3 of the ECHR[10]. Although the Soering case did not involve a refugee, it set an important precedent by extending non-refoulement protections through human rights principles, not just refugee law.

Similarly, in A v Australia[11] in 1997, the UN Human Rights Committee found that Australia's prolonged and indefinite detention of a stateless asylum seeker violated Articles 9 and 7 of the ICCPR[12]. The Committee stressed that detention should not be arbitrary and must be necessary and proportionate to the state's valid objectives. This case reinforced the idea that state responses to perceived immigration risks must conform to international human rights obligations, even when addressing issues of national security or administrative efficiency.

In Zaoui v Attorney-General,[13] the New Zealand Court of Appeal addressed the conflict between national security concerns and non-refoulement obligations. The Court held that even individuals deemed to be a threat to national security could not be deported to countries where they faced a real risk of torture or death, echoing the absolute nature of protections

[8] Elihu Lauterpacht and Daniel Bethlehem, 'The Scope and Content of the Principle of Non-Refoulement: Opinion' in Erika Feller et al. (eds), *Refugee Protection in International Law: UNHCR's Global Consultations on International Protection* (CUP 2003) 87 para 168
[9] *Soering v United Kingdom* [1989] 11 EHRR 439 (ECtHR)
[10] European Convention on Human Rights 1953, art 3
[11] *A v Australia* [1997] Communication No 560/1993 UN Doc CCPR/C/59/D/560/1993
[12] International Covenant on Civil and Political Rights 1976, arts 7 & 9
[13] *Zaoui v Attorney-General* [2005] NZSC 38

under Art. 3 of CAT[14]. The decision underscored that procedural and substantive safeguards under international law override domestic security considerations in such contexts.

Legal Standard for Risk Assessment: Deciding on the point at which non-refoulement protection applies is based on the legal standard of establishing risk. Courts and committees have evolved towards a comparatively generous standard of requiring real and substantial risk, in contrast to a risk of harm that may occur. In the UK case R v Secretary of State for the Home Department[15], the House of Lords made it clear that the test applied was not one of certainty of persecution, but whether there was a real and substantial danger that the applicant would be subjected to serious harm. This is consistent with the approach in the U.S. Supreme Court's logic in INS v Cardoza-Fonseca[16], in which the Court dismissed a stringent burden of proof and reaffirmed that an applicant is not required to demonstrate that persecution is more likely than not, but only that it is a reasonable possibility substantiated by objective evidence.

These standard balances state discretion in immigration issues against the protective intent of refugee law. It recognises that absolute certainty is not possible and not required due to the inherent challenge of establishing future harm. It does, however, place the burden on the applicant to provide credible and verifiable evidence of risk, whether through personal testimony or other reliable sources. Courts have also underscored the fact that generalised violence, economic adversity, or political turmoil does not, per se, constitute persecution. For a claim to prosper, the harm must be linked to one of the five Convention grounds of race, religion, nationality, political opinion, or membership in a specific social group. However, human rights law tends to interpret these grounds broadly, especially in cases where several vulnerabilities intersect, such as those involving women, LGBTQ+ individuals, or ethnic minorities.

PRIVACY AND SURVEILLANCE: DIGITAL INTERFERENCE WITH LIBERTY

The sudden exponential expansion of surveillance technology and biometric data collection across migration and border control scenarios has presented international human rights law with unparalleled threats to the right to privacy. Originally premised on physical invasions,

[14] Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment 1987, art 3
[15] *R v Secretary of State for the Home Department, ex p Daly* [2001] 2 AC 532
[16] *Immigration and Naturalization Service v Cardoza-Fonseca* [1987] 480 US 421

the right now covers the sophisticated reality of digital surveillance, algorithmic profiling, and data storage. The introduction of AI and facial recognition in immigration systems presents critical issues regarding legality, accountability and discrimination. This part discusses the law of the land that regulates the right to privacy, the ways courts have understood its limits, and the new threats presented by surveillance-based migration strategies.

Legal Test: Legality, Legitimate Aim, Necessity & Proportional: Right to privacy is incorporated in Art. 12 of the UDHR[17] and Art. 17 of the ICCPR[18], both of which preclude arbitrary or unlawful interference with privacy, family, home, or correspondence. The UNHRC, in General Comment No. 16[19], sets out the circumstances under which interference with privacy can be regarded as lawful. Any such interference that is unreasonable or an illegal disruption of a person's privacy, family life, home, or personal communications should:

1. Be prescribed by law (legality),
2. Pursue a legitimate aim (e.g., national security, public order),
3. It is necessary in a democratic society, and
4. Be proportionate to the aim pursued.

The ECtHR also replicates this test under Art. 8 of the ECHR.[20] Holding that even interference with a legitimate aim must be the least intrusive means necessary. The necessity test, in specific terms, mandates that governments show not only a general interest, but a pressing social need compelling the intrusion.

Judicial rulings on digital monitoring have more and more acknowledged the broad menace presented by such devices to individual autonomy and freedom. In Roman Zakharov v Russia[21], the ECtHR invalidated Russia's legislation on the grounds of permitting mass interception of correspondence without proper protection. The Court highlighted that such extensive surveillance powers, wielded in the absence of serious judicial oversight,

[17] Universal Declaration of Human Rights 1948, art 12
[18] International Covenant on Civil and Political Rights 1976, art 17
[19] 'CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (*UNHCR*, 08 April 1988) <https://www.refworld.org/legal/general/hrc/1988/en/27539> accessed 30 May 2025
[20] European Convention on Human Rights 1953, art 8
[21] *Roman Zakharov v Russia* [2016] App no 47143/06 (ECtHR)

contravened Art. 8 of the ECHR, even if the individual applicant was unable to demonstrate personal targeting. The ruling underscored that regimes of surveillance must integrate sufficient and effective safeguards against abuse, particularly in national security.

In S. and Marper v United Kingdom[22], the ECtHR determined that indefinite retention of DNA profiles and fingerprints of persons who had not been convicted of any offence constituted a disproportionate interference in their right to private life. The Court dismissed the UK's argument based on administrative convenience and public safety, determining that policies of bulk data retention don't pass the proportionality test and must be carefully limited to particular, ascertainable risks.

A further recent case, Glukhin v Russia[23], reaffirmed that the legitimate purpose and the strict necessity test need to apply to surveillance technologies. The ECtHR made it clear that necessity in a democratic society does not mean utility or convenience, but that the interference must be the least intrusive to achieve the objective, with proper respect for individuals' rights.

Biometric Data, AI, & Border Control: As migration control systems continue to be more automated, the collection of biometric information, including fingerprinting, iris scanning, and facial identification, is increasingly raising serious privacy issues. Border and detention camp surveillance systems habitually capture and store individuals' personal information without their knowledge, transparency, or express legal protection. These activities frequently contravene the requirements of lawfulness, fairness, and transparency as set out in Articles 5 and 6 of the GDPR.[24]

A primary concern is that these systems disproportionately impact marginalised groups, such as refugees and asylum seekers, who might not have the legal knowledge or procedural means to contest misuse of data. Report[25] on how facial recognition technologies have high racial and gender bias, especially against Black, Indigenous, and other minority populations. These tools tend to produce false positives or misidentifications, resulting in increased

[22] *S and Marper v United Kingdom* [2008] App nos 30562/04 and 30566/04 (ECtHR)
[23] *Glukhin v Russia* [2021] App No 30671/16 (ECtHR)
[24] General Data Protection Regulation 2016, arts 5–6
[25] 'Xenophobic Machines: Discrimination through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal' (*Amnesty International*, 29 October 2021) <https://www.amnesty.org/en/documents/eur35/4686/2021/en/> accessed 26 May 2025

surveillance, arbitrary detention, or refusal of entry for people solely based on algorithmic outputs.

In addition, most of these systems are implemented with little or no human intervention, violating the right to an effective remedy and due process. Migrants who are targeted by AI risk assessment systems could face enhanced scrutiny, delay, or denial of protection without being aware of the reasons for the decision, a clear contravention of article 17 of the ICCPR[26] and GDPR Recital 60[27], which requires the right to know how one's data is being processed.

ARBITRARY DETENTION IN MIGRATION: LEGAL BOUNDARIES

One of the most controversial topics in modern migration law is the detention of asylum seekers and migrants. While states have the sovereign right to control the entry and stay of foreigners, this power is limited by international human rights laws that require a presumption in favour of personal liberty and forbid arbitrary detention. Practically speaking, most regimes function in violation of both the letter and the spirit of international law. This section explores the central legal framework governing detention in the migration context and discusses how courts have interpreted its boundaries.

Presumption of Liberty in International Law: The freedom from detention is a basic assurance under international human rights law. Art. 9 of the ICCPR[28] and Art. 9 of the UDHR[29] both ban arbitrary detention or arrest and state that no person shall be arbitrarily deprived of liberty except by a procedure provided by law. Notably, the concept of arbitrariness goes beyond legality in the light of domestic law. As has been explained by the UN Human Rights Committee, detention can be legal in a procedural sense yet remain arbitrary if it is not fit for purpose, unjust, or excessive in the context.

In the leading case of A v Australia,[30] the Human Rights Committee established that the indefinite detention of a stateless asylum seeker contravened Articles 9(1) and 9(4) of the ICCPR.[31] The Committee concluded that where there was no effective judicial review and no individualised consideration, the detention was arbitrary. This case confirmed that

[26] International Covenant on Civil and Political Rights 1976, art 17
[27] General Data Protection Regulation 2016, r 60
[28] International Covenant on Civil and Political Rights 1976, art 9
[29] Universal Declaration of Human Rights 1948, art 9
[30] *A v Australia* [1997] Communication No 560/1993 UN Doc CCPR/C/59/D/560/1993
[31] International Covenant on Civil and Political Rights 1976, arts 9(1) and 9(4)

immigration detention always has to be tested for necessity and proportionality, and also that alternatives to detention have to be taken very seriously.

In Amuur v France,[32] the appeal of four Somali asylum seekers detained for 20 days in Paris-Orly Airport's transit zone without judicial review. The Court held that the applicants had been deprived of their liberty in contravention of article 5(1) of the ECHR[33], which guarantees protection against arbitrary detention. The ruling underscored that sending people into a transit zone does not avoid the state's responsibility to ensure legal protection, such as access to courts and humanitarian aid.

Further affirming this principle, the ECtHR in Z.A. and Ors v Russia[34] held that the long-term detention of asylum seekers in an airport transit zone amounted to de facto detention in the absence of a legal basis. The Court emphasised that immigration detention should be regulated by clear rules of law, and the absence of a statutory maximum duration of detention or effective review made the applicants' detention unlawful under the same.

A fundamental case is Winterwerp v Netherlands[35], where the European Court of Human Rights clarified that any deprivation of liberty must comply with the purpose of Article 5, which is to protect individuals from arbitrary detention. The decision explained that the lawfulness of detention does not merely point to conformity with domestic law, but with the general principles of the Convention as well. The Court emphasised that legal protections have to be both procedural and substantive, and that people should not be detained without good reason.

These decisions uphold a fundamental principle of international human rights law: the presumption of freedom should always be the norm, and any departure from it should be supported by cogent, legal, necessary, and proportionate grounds. Detention should not be applied as a mass policy or in the interests of administrative convenience. With border technologies and automatic systems increasingly deciding the fate of migrants, strict compliance with these legal parameters becomes increasingly crucial. The absence of personalised examinations, legal review, or maximum detention times threatens to render protective legal structures formalities alone, eroding the very basis of the right to liberty.

[32] *Amuur v France* [1996] App No 19776/92 (ECtHR)
[33] European Convention on Human Rights 1953, art 5(1)
[34] *Z.A. and Ors v Russia* [2013] App No 61411/10 (ECtHR)
[35] *Winterwerp v Netherlands* [1979] 2 EHRR 387 (ECtHR)

Discrimination in Digital Migration Systems: Discrimination in the control of migration has been a subject of international concern for some time, but the growing deployment of digital technologies like AI, biometric monitoring, and algorithmic profiling introduced new vectors and mechanisms of discriminatory treatment. These technologies, even when presented as neutral and unbiased, can create and reinforce existing social inequalities, especially based on race, ethnicity, and nationality. International human rights law, both in treaty provisions and in judicial interpretation, affords solid protection against direct as well as indirect discrimination. The following section examines how such principles are applicable in the context of digital border control systems.

Indirect Discrimination and AI: International law not only forbids direct/intentional discrimination but also indirect discrimination, where ostensibly neutral policies disproportionately and negatively affect specific groups. This principle is enshrined in Art. 26 of the ICCPR[36], articles 2 and 7 of the UDHR[37], and Art. 3 of the 1951 Refugee Convention, ensuring non-discrimination in applying rights to refugees.[38]

General Comment No. 18 of the Human Rights Committee recognizes that the word discrimination refers to any distinction, exclusion, restriction, or preference on grounds including but not limited to race, color, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status, and which results in the unequal treatment in law or practice.

Digital migration platforms typically draw on past data, pattern analysis, and forward-looking analysis that perpetuate and reproduce existing social biases. For example, face recognition algorithms learning on predominantly white datasets perform considerably less well at recognising individuals with darker skin. As per research,[39] these technologies have increased error rates for Black, Indigenous, and people of colour, resulting in disproportionate surveillance, misidentification, and even wrongful detention or deportation. Likewise, risk assessment computer programs applied to border control and asylum proceedings can incidentally mark particular nationalities or ethnic groups as high-

[36] International Covenant on Civil and Political Rights 1976, art 26
[37] Universal Declaration of Human Rights 1948, arts 2 and 7
[38] Convention Relating to the Status of Refugees 1954, art 3
[39] Xenophobic Machines: Discrimination through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal (n 25)

risk due to associations established in discriminatory datasets. Even if the people creating or using these systems do not mean to discriminate, international human rights law focuses more on the impact of their actions than on their intentions.

Key Jurisprudence: The ECtHR has been key in defining the legal boundaries of indirect discrimination. In Biao v Denmark,[40] the Court held that Denmark's family reunification policy indirectly discriminated against individuals of non-Danish ethnic background. The Court held that the differential treatment, although not race-based, had a disproportionate impact on persons from immigrant communities, and breached Art. 14 and 8 of the ECHR.[41] The Court underlined the need for statistical and contextual evidence in proving discriminatory impact.

A seminal case on educational discrimination, D.H. and Others v Czech Republic[42], was about systemic segregation of Roma children into special schools for the mentally disabled. The Court found that although the policy was neutral on its face, it had a disproportionate and unjustified effect on a marginalised group of people. The ECtHR held that the absence of discriminatory intent does not exclude the finding of a violation, thus solidifying the doctrine of indirect discrimination in European law.

Likewise, in Hugh Jordan v United Kingdom[43], dealing with an inquiry into a state homicide in Northern Ireland, the Court reaffirmed that a breach of Art. 14[44] need not be evidenced by discriminatory intent. It will suffice if a policy or practice has discriminatory consequences, and the state does not present objective and legitimate reasons for them.

Taken together, these cases show that under international and regional human rights law, neutral systems that result in unequal outcomes, especially based on race or ethnicity, can be considered discriminatory unless properly explained and corrected. When it comes to migration and online governance, the implication is that states have to critically examine the data inputs, the algorithms used, and the outputs of the technologies they use and ensure they do not deepen existing disparities.

[40] *Biao v Denmark* [2016] App No 38590/10 (ECtHR)
[41] European Convention on Human Rights 1953, arts 8 and 14
[42] *D.H. and Ors v Czech Republic* [2007] App No 57325/00 (ECtHR)
[43] *Hugh Jordan v United Kingdom* [2003] App No 24746/94 (ECtHR)
[44] International Covenant on Civil and Political Rights (1976, art 14

DATA PROTECTION AND DUE PROCESS IN AI DECISION-MAKING

The integration of AI and algorithmic decision-making into immigration systems has raised profound concerns regarding data protection, transparency, and the right to due process. In the context of migration, where decisions can profoundly affect an individual's liberty, safety, and legal status, the opacity and complexity of AI-driven tools pose unique threats to fundamental rights protected under European and international legal frameworks. This section examines key principles under the GDPR, the EU Charter of Fundamental Rights, and the emerging AI Act, focusing on how automated systems challenge lawful, transparent, and accountable governance in immigration contexts.

High-Risk AI in Immigration: AI tools applied in border management, visa application, and asylum screening are usually labelled as high-risk because of their far-reaching effects on individual rights. Algorithms for risk-scoring, biometric matching, and computerised credibility analysis increasingly control admission to lawful protection and freedom of movement. However, these technologies are all too often opaque, with those affected unaware of how or why judgments are taken or on what information they depend. This lack of transparency directly undermines the right to an effective remedy and the ability to challenge adverse decisions.

The GDPR establishes core principles for data protection, including lawfulness, fairness, and transparency (Art 5(1)(a))[45], purpose limitation, and data minimisation. Under Article 6,[46] personal data must be processed only on a legitimate legal basis, such as the individual's informed consent.[47] Nonetheless, consent in the context of migration is not usually freely given or informed, especially if a refusal would risk admission or claims of asylum. By Recital 42 of the GDPR[48], consent needs to be voluntary, precise, and informed by a clear awareness of what its implications will be.

Current enforcement action reveals these shortcomings. In Greece[49], the data protection agency discovered that the national migration system captured biometric information

[45] General Data Protection Regulation 2016, art 5(1)(a)
[46] General Data Protection Regulation 2016, art 6
[47] General Data Protection Regulation 2016, arts 5(1)(a) and 6
[48] General Data Protection Regulation 2016, recital 42
[49] 'HDPA (Greece) - 24/2023' (*GDPR Hub*, 30 October 2023) <https://gdprhub.eu/index.php?title=HDPA_(Greece)_-_24/2023> accessed 30 May 2025

without legal consent or adequate transparency. The same was noted in Lithuania and Spain, where asylum seekers were under surveillance and automated processing without meaningful information or the choice to opt out.

Case Law & Regulatory Frameworks: Recital 39 of the GDPR[50] emphasises that persons should be informed about how their data is processed and used, and also have access to correction and challenge mechanisms. Data controllers should also put in place measures guaranteeing accountability and human intervention, particularly where automated decision-making has a substantial impact on legal rights.

The EU AI Act,[51] introduced for proposal, amplifies these commitments further by categorising AI systems employed in migration and asylum as high-risk in Annexure III. Recitals 33, 60, and 73[52] also emphasise transparency, documentation, and impact assessments to avoid violations of fundamental rights. Nonetheless, until binding technical and legal protections are enacted in their entirety, AI systems will continue to significantly threaten procedural fairness in immigration proceedings.

CONCLUSION AND RECOMMENDATIONS

While states are integrating more AI and surveillance technologies into their migration and asylum frameworks, core human rights are coming under a lot of pressure. This paper has shown that digital technologies such as facial recognition, biometric databases, and risk-scoring algorithms often fail to follow international legal standards on asylum, privacy, freedom, and equality.

By an examination of ECtHR jurisprudence, UN Human Rights Committee jurisprudence, and domestic courts, it is clear that most digital practices in the management of migration contravene the framework of non-refoulement, the right to privacy, and the presumption of freedom. In addition, algorithmic systems have been demonstrated to yield indirect discrimination, disproportionately impacting racial and ethnic minorities, and eroding due process by way of the insecure, impenetrable decisions.

[50] General Data Protection Regulation 2016, recital 39
[51] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final
[52] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final, recital 33, 60, 73

To align technological practices with global human rights obligations, states must establish strong laws and effective oversight systems. This involves guaranteeing transparency in AI decisions, carrying out regular impact assessments, restricting data collection to what is required and legal, and guaranteeing meaningful opportunities for persons to comprehend and contest automated decisions. High-risk systems should not be applied in asylum procedures without human control and strong protection mechanisms.

Finally, technology use in migration must not compromise dignity, fairness, and justice. As digital borders expand, so must the commitment to preserve the rights that define a just and humane international legal order.