
ALGORITHMS IN EXILE: ARTIFICIAL INTELLIGENCE, HUMAN RIGHTS, AND THE GOVERNANCE OF TECHNOLOGY IN REFUGEE AND FORCED DISPLACEMENT CONTEXTS

Kumar Gautam, Research Scholar, Department of Laws, Panjab University, Chandigarh

ABSTRACT

The deployment of Artificial Intelligence (AI) technologies in the management of refugee and forced displacement crises marks one of the most consequential intersections of emerging technology and international human rights law in the twenty-first century. With over 110 million forcibly displaced persons worldwide, humanitarian organisations, governments, and technology corporations are increasingly turning to AI systems, including biometric identification, predictive analytics, automated decision-making, and surveillance technologies, to manage, monitor, and assist displaced populations. This paper argues that while AI carries genuine transformative potential for improving humanitarian outcomes, its deployment in refugee contexts is attended by a matrix of legal, ethical, and political risks that the existing international and domestic legal order is inadequately equipped to address. Drawing upon international human rights law, refugee law, data protection frameworks, comparative constitutional jurisprudence, and critical algorithmic studies, this paper undertakes a systematic legal and normative analysis of AI's impact on refugees and displaced persons. It demonstrates that without principled governance frameworks grounded in human dignity, non-discrimination, and accountability, AI risks replicating and amplifying the very marginalisation it purports to remedy. The paper concludes with a normative framework for rights-compliant AI governance in humanitarian settings, structured around the principles of legality, proportionality, dignity, accountability, and meaningful human oversight.

Keywords: Artificial Intelligence; Refugees; Forced Displacement; Biometrics; Automated Decision-Making; Data Privacy; Non-Refoulement; Algorithmic Bias; Humanitarian Technology; Human Rights.

I. INTRODUCTION

The global forced displacement crisis has reached a magnitude without precedent in recorded history. According to the United Nations High Commissioner for Refugees (UNHCR), the number of forcibly displaced persons worldwide exceeded 110 million by the end of 2022, with over 35.3 million recognised refugees and approximately 62 million internally displaced persons.¹ The international legal architecture governing the protection of this population, anchored in the 1951 Convention Relating to the Status of Refugees and its 1967 Protocol,² was designed for a world of analogue bureaucracies, physical camps, and human caseworkers. It is now being stress-tested by a fundamentally transformed technological environment in which decisions of life-altering consequence are increasingly delegated to automated systems.

Artificial Intelligence, broadly understood as the application of computational systems to perform tasks ordinarily requiring human intelligence, including recognition, classification, prediction, and decision-making, is being deployed at virtually every stage of the refugee cycle: at the border through biometric screening and risk profiling; in camps through aid distribution management and health surveillance; in the asylum process through automated eligibility assessment and credibility analysis; and in host societies through language integration and employment matching. Each of these applications carries profound implications for the rights, dignity, and physical safety of some of the world's most vulnerable persons.

This paper advances three central propositions. First, the deployment of AI in refugee contexts is not merely a matter of technical efficiency but a deeply normative exercise involving the allocation of decisions of life-altering consequence, including determinations of who receives food, who is recognised as a refugee, who is detained, and who is deported. Second, the existing legal framework, comprising international refugee law, human rights law, and domestic data protection regimes, contains significant conceptual and institutional gaps rendering it inadequate to govern algorithmic systems affecting refugees.³ Third, a purposive, human rights-centred governance framework for AI in humanitarian contexts is not merely desirable

¹UNHCR, Global Trends: Forced Displacement in 2022, at 2, 8 (2023), <https://www.unhcr.org/global-trends-report-2023> [hereinafter UNHCR Global Trends 2022].

²Convention Relating to the Status of Refugees art. 1(A)(2), July 28, 1951, 189 U.N.T.S. 137 [hereinafter 1951 Refugee Convention]; Protocol Relating to the Status of Refugees art. I(2), Jan. 31, 1967, 606 U.N.T.S. 267 [hereinafter 1967 Protocol].

³See Amnesty International, *Automating Injustice: The Use of Automated Decision-Making Systems in the Criminal Justice System in Europe* (2023); Human Rights Watch, *Automated Hardship: How Technology Drives Benefit Cuts in the US* (2021). The systemic risks identified in these reports are replicated with equal force in humanitarian settings.

but legally mandated by states' existing international obligations.

The paper proceeds as follows. Part II situates AI deployment in refugee contexts within the existing international human rights and refugee law framework. Parts III through VI examine the principal applications of AI in humanitarian settings, analysing their potential and their risks. Part VII addresses the systemic challenges of algorithmic bias, data sovereignty, and automated decision-making. Part VIII articulates a normative framework for rights-compliant AI governance in humanitarian contexts. Part IX concludes.

II. THE INTERNATIONAL LEGAL FRAMEWORK: REFUGEES, HUMAN RIGHTS, AND THE EMERGING AI GOVERNANCE REGIME

The international protection of refugees rests upon a normative architecture that is simultaneously foundational and fragile. The 1951 Refugee Convention establishes the principle of non-refoulement and a battery of civil, social, and economic rights for recognised refugees. However, the Convention's drafters could not have envisaged a world in which a refugee's fate might be determined not by a human official exercising judgment, but by an algorithmic system processing biometric data at the speed of microseconds.

The Universal Declaration of Human Rights proclaims the right to privacy, freedom from arbitrary interference, and the right to seek and enjoy asylum from persecution.⁴ The International Covenant on Civil and Political Rights (ICCPR) enshrines the right to privacy in Article 17 and the right to equality before the law and equal protection in Article 26, rights that must be enjoyed by all persons within a state's jurisdiction without distinction as to nationality or immigration status.⁵ The Convention on the Rights of the Child equally protects children's privacy and dignity without discrimination.⁶

UNHCR has developed a Data Protection Framework for persons of concern, including a comprehensive Data Protection Policy⁷ and technical guidance on biometric systems deployed

⁴Universal Declaration of Human Rights, G.A. Res. 217(III), arts. 3, 12, 14, U.N. Doc. A/RES/3/217A (Dec. 10, 1948) [hereinafter UDHR].

⁵International Covenant on Civil and Political Rights arts. 17, 26, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]. Both provisions apply to all persons within a state party's territory and subject to its jurisdiction, irrespective of nationality or migration status.

⁶Convention on the Rights of the Child art. 16, Nov. 20, 1989, 1577 U.N.T.S. 3 [hereinafter CRC] (guaranteeing the right of every child to privacy without arbitrary interference, regardless of nationality or immigration status of child or parent).

⁷UNHCR, Policy on the Protection of Personal Data of Persons of Concern to UNHCR (2015) [hereinafter UNHCR Data Protection Policy]; UNHCR, Guidance on Personal Data Protection in the Humanitarian Action

through its PRIMES architecture.⁸ These instruments, while normatively valuable, lack legally binding force and do not establish independent oversight mechanisms capable of holding technology vendors or states accountable for algorithmic harms. The absence of a binding global treaty on AI and human rights, notwithstanding the important regional initiative represented by the European Union AI Act,⁹ constitutes the most significant structural lacuna in the governance architecture.

The interaction between AI and non-refoulement, the peremptory norm prohibiting return to a territory of persecution,¹⁰ is particularly acute. AI-assisted risk profiling at borders, predictive analytics used to assess asylum credibility, and automated border surveillance systems all have the potential to trigger refoulement by generating flawed outputs that form the factual basis for deportation decisions. If an algorithm erroneously classifies a person as a security risk or low-credibility claimant and that classification leads to expulsion to a territory of persecution, the legal responsibility of the deploying state for the resulting human rights violation is undiminished by the interposition of a technological intermediary.¹¹

Scholars have begun to articulate a framework of algorithmic accountability grounded in existing human rights law.¹² Under this framework, states' obligations to respect and ensure human rights extend to AI systems they deploy or authorise, requiring legality, a sufficiently precise legal basis for algorithmic decision-making; necessity and proportionality, the least rights-restrictive means to achieve a legitimate aim; non-discrimination, freedom from arbitrary differential treatment; and accountability, mechanisms for remedy when rights are violated. UNHCR's own AI Principles seek to operationalise these requirements within the

(2016).

⁸UNHCR, PRIMES: Population Registration and Identity Management EcoSystem, <https://www.unhcr.org/primes> (last visited May 10, 2026) [hereinafter PRIMES]; UNHCR, Biometric Identity Management System (BIMS) Technical Guidance Note (2019).

⁹Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689) 1 [hereinafter EU AI Act]; see also European Commission, A European Approach to Artificial Intelligence, COM(2021) 206 final, at 8-10 (Apr. 21, 2021).

¹⁰1951 Refugee Convention, *supra* note 2, art. 33(1). On the peremptory character of non-refoulement, see Elihu Lauterpacht & Daniel Bethlehem, The Scope and Content of the Principle of Non-Refoulement, in *Refugee Protection in International Law* 87, 149 (Erika Feller et al. eds., 2003).

¹¹Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment art. 3, Dec. 10, 1984, 1465 U.N.T.S. 85 [hereinafter CAT]; Petra Molnar, Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective, 8 *Cambridge Int'l L.J.* 305, 318 (2019) (demonstrating that AI-assisted border risk profiling generates a material risk of refoulement by producing flawed outputs that form the factual basis for expulsion decisions).

¹²Lorna McGregor, Daragh Murray & Vivian Ng, International Human Rights Law as a Framework for Algorithmic Accountability, 68 *Int'l & Comp. L.Q.* 309, 315-17 (2019). The authors identify four indispensable requirements: legality, necessity and proportionality, non-discrimination, and accountability with access to remedy.

humanitarian system,¹³ though they are, as yet, aspirational rather than binding.

III. AI IN IDENTITY MANAGEMENT AND BIOMETRIC SYSTEMS

Identity documentation is the gateway to rights. For millions of refugees who have fled persecution without documents, or whose documents have been confiscated, destroyed, or rendered inaccessible, the inability to establish legal identity is the proximate cause of exclusion from food, healthcare, education, and legal protection. UNHCR's deployment of biometric systems, encompassing iris recognition, fingerprint scanning, facial recognition, and voice identification through platforms such as PRIMES, represents the most extensive use of AI in humanitarian settings globally.

The case for biometric identity systems rests upon four pillars: accuracy superior to manual verification; fraud reduction; linkage of entitlements to verified identity; and scalability in large-scale displacement scenarios. The World Food Programme's Building Blocks initiative in Jordan, which used blockchain technology anchored to biometric identifiers to deliver food assistance to Syrian refugees, demonstrated the potential of integrated biometric-digital payment systems to reduce transaction costs and increase financial inclusion.¹⁴

However, the legal and ethical risks of biometric systems in refugee contexts are severe and structurally underappreciated. Three risks merit sustained analytical attention. First, accuracy disparities: research by Buolamwini and Gebru has demonstrated that commercially deployed facial recognition systems exhibit significantly higher error rates for darker-skinned and female subjects.¹⁵ In a refugee context, a misidentification can deny a person food or trigger a security alert leading to detention. Second, function creep: data collected for humanitarian purposes has, in documented cases, been accessed by state security agencies, creating what scholars have termed the humanitarian surveillance complex.¹⁶ Third, the absence of meaningful consent:

¹³UNHCR, AI Principles for UNHCR (2021) [hereinafter UNHCR AI Principles]; see also UN Secretary-General's Roadmap for Digital Cooperation, Follow-up Report, U.N. Doc. A/75/261 (2020). The UNHCR AI Principles affirm transparency, accountability, safety, and privacy as the four pillars of rights-compliant AI deployment in humanitarian settings.

¹⁴World Food Programme, Building Blocks: Blockchain for Zero Hunger (2019), <https://innovation.wfp.org/project/building-blocks>; see also Evan Grund & Mimi Nguyen, Blockchain-Enabled Digital Identity for Refugees: Promise, Perils and Policy Pathways, 14 J. of Int'l Humanitarian Action 1, 5 (2022).

¹⁵Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proc. of Machine Learning Research 1, 7-12 (2018). The study found error rates of up to 34.7 percent for darker-skinned female subjects, compared to 0.8 percent for lighter-skinned males.

¹⁶Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power 176-81 (2019); Vincent Mosco, The Digital Sublime: Myth, Power, and Cyberspace 43-47 (2004). Zuboff's concept of 'behavioral modification' is apposite to humanitarian biometric systems that shape refugee conduct

refugees' structural dependency on humanitarian organisations fundamentally compromises the voluntariness of consent to biometric data collection. Where enrolment in a biometric system is a precondition for receiving food, the notion of free and informed consent is juridically hollow.¹⁷

The applicable legal framework requires that biometric data processing in refugee contexts satisfy the requirements of legality, proportionality, and necessity under the ICCPR¹⁸ and be subject to robust data protection safeguards equivalent to those applicable under the GDPR. The right to privacy, recognised as a fundamental right applicable to all persons by the Indian Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,¹⁹ demands no less. The operationalisation of these requirements in humanitarian settings requires independent data protection oversight, accessible complaint mechanisms, purpose limitation provisions, and time-bound data retention schedules. Facial recognition technology, in particular, presents acute risks that warrant heightened scrutiny, as documented by the European Union Agency for Fundamental Rights.²⁰

IV. AI IN HUMANITARIAN LOGISTICS, AID DISTRIBUTION, AND HEALTHCARE

4.1 Logistics and Aid Distribution

The efficient delivery of humanitarian assistance, including food, shelter, non-food items, and cash transfers, is the operational core of the refugee response. AI's potential to optimise supply chains, predict need, and reduce fraud in aid disbursement has attracted significant investment

through the architecture of digital registration.

¹⁷Regulation (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, 2016 O.J. (L 119) 1 [hereinafter GDPR], arts. 9 (special categories of personal data), 22 (automated individual decision-making).

¹⁸Human Rights Committee, General Comment No. 16 on the Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art. 17), paras. 3-4, U.N. Doc. HRI/GEN/1/Rev.1 (1988) (affirming that the right to privacy under the ICCPR extends to all individuals within a state's jurisdiction, including non-citizens and persons in irregular status).

¹⁹*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India) (holding that the right to privacy is a fundamental right under Article 21 of the Indian Constitution, applicable to all persons on Indian soil regardless of nationality); Digital Personal Data Protection Act, No. 22 of 2023 (India). Notably, the 2023 Act exempts processing for national security and law enforcement purposes, creating a significant gap for non-citizen data subjects.

²⁰European Union Agency for Fundamental Rights, Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, FRA Report 44-52 (2019). The Report identifies particular risks arising from false matches in populations underrepresented in training datasets, a risk that is structurally elevated for refugee populations.

from humanitarian organisations. The WFP's SCOPE platform leverages biometric authentication and machine learning to manage beneficiary data and automate transfer processes across multiple assistance modalities.²¹

However, algorithmic aid allocation also embeds risks of exclusion and discrimination. AI systems trained on historical distribution data may perpetuate patterns of inequitable access, systematically under-serving communities that were already marginalised in previous response cycles.²² The normative requirement of non-discrimination under Article 26 of the ICCPR and analogous provisions demands that aid allocation algorithms be subject to regular equity audits, disaggregated by gender, ethnicity, disability, and age.²³

4.2 AI in Healthcare for Displaced Populations

Refugees disproportionately suffer from communicable diseases, mental health conditions, and trauma-related disorders, while simultaneously facing barriers of language, documentation, and geographic isolation that impede access to health services. AI-powered diagnostic tools, including machine learning models for tuberculosis detection, malaria diagnosis from blood smear images, and triage algorithms for emergency medicine, offer the prospect of dramatically extending specialist medical expertise to resource-constrained humanitarian settings.²⁴

AI-driven disease surveillance systems can detect early signals of outbreak risk within camps by analysing patterns in health facility visit data, community health worker reports, and environmental indicators, compressing the response time between outbreak detection and public health intervention.²⁵

The ethical and legal dimensions of healthcare AI in refugee contexts are, however, sharply

²¹World Food Programme, SCOPE: A Beneficiary and Transfer Management Platform, Technical Overview (2021); see also UNHCR & WFP, Joint Data Sharing Memorandum of Understanding Guidance Note (2018).

²²Jeff Larson et al., How We Analyzed the COMPAS Recidivism Algorithm, ProPublica (May 23, 2016), <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>; Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor 11-13 (2018).

²³Committee on the Elimination of Discrimination Against Women, General Recommendation No. 32 on the Gender-Related Dimensions of Refugee Status, Asylum, Nationality and Statelessness of Women, U.N. Doc. CEDAW/C/GC/32, paras. 9-11 (2014). The Recommendation affirms that gender-based risk assessment tools must be sensitive to the specific forms of persecution experienced by women.

²⁴International Committee of the Red Cross, Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach 7-12 (2019); Javier Ruiz Calderón, AI for Humanitarian Action: Global Innovation Fund Report 14-19 (2022).

²⁵Patrick Meier, Digital Humanitarians: How Big Data Is Changing the Face of Humanitarian Response 77-82 (2015); Nathaniel Raymond et al., Applying Humanitarian Principles to Current Uses of Information Communication Technologies 12-16 (Harvard Humanitarian Initiative, 2012).

contested. Medical AI systems trained predominantly on data from high-income, majority-population datasets may exhibit systematic performance degradation when applied to refugee populations with different epidemiological profiles, genetic backgrounds, and disease presentations. The right to the highest attainable standard of health under Article 12 of the ICESCR,²⁶ applicable to all persons without discrimination, requires that AI-assisted healthcare systems deployed for refugee populations be validated on representative datasets and subject to ongoing performance monitoring.

V. AI IN EDUCATION, LANGUAGE INTEGRATION, AND ECONOMIC INCLUSION

Education is both a fundamental human right and the most powerful instrument of long-term durable solution for displaced populations. The Convention on the Rights of the Child mandates the right to education for all children without discrimination,²⁷ and Article 13 of the ICESCR recognises it as an inalienable right of every person. Yet for the estimated 3.7 million refugee children currently out of school globally, access to quality education remains a profound and persistent unmet need.

AI-powered adaptive learning platforms, which personalise educational content to individual learners' pace, comprehension level, and linguistic background, offer a potentially transformative tool for bridging the educational gap faced by refugee children. Natural language processing systems can accelerate language acquisition in the language of the host country, facilitating integration into national school systems. AI-driven translation tools can make educational content available in minority and rare languages spoken by displaced populations, addressing one of the most persistent barriers to educational access.²⁸

Notwithstanding these potential benefits, the deployment of AI in refugee education raises important equity concerns. AI-driven educational tools require digital infrastructure, including electricity, connectivity, and compatible devices, that is systematically lacking in camp settings

²⁶International Covenant on Economic, Social and Cultural Rights art. 12, Dec. 16, 1966, 993 U.N.T.S. 3 [hereinafter ICESCR]; Committee on Economic, Social and Cultural Rights, General Comment No. 14 on the Right to the Highest Attainable Standard of Health, para. 12(b), U.N. Doc. E/C.12/2000/4 (2000).

²⁷CRC, *supra* note 6, art. 28; Committee on the Rights of the Child, General Comment No. 6, para. 41, U.N. Doc. CRC/GC/2005/6 (2005) (confirming that the right to education extends to all children within a state's jurisdiction, including children with undocumented or irregular migration status).

²⁸UNHCR, *Connected Education: What Works for Refugee Learners?* (2020); UNESCO, *Global Education Monitoring Report 2019: Migration, Displacement and Education* 89-95 (2019) (documenting that only 63 percent of refugee children of primary school age are enrolled in school, compared to a global average of 91 percent).

in low-income host countries. The risk is that AI-enabled education deepens rather than bridges the digital divide, with better-resourced urban refugees gaining access to sophisticated adaptive learning while those in remote camps are left further behind. The UNHCR's digital education strategy and the New York Declaration's commitments on durable solutions²⁹ must grapple directly with this structural inequality.

Designing AI educational solutions that are genuinely inclusive requires hardware-light architectures, offline functionality, and deliberate co-design with refugee communities themselves, in line with the UNESCO AI Recommendation's emphasis on inclusive design.³⁰

In the domain of economic integration, the normative aspiration embedded in the Global Compact on Refugees, that refugees should achieve economic self-reliance and contribute to host economies,³¹ is technologically supportable through AI-driven employment matching platforms. However, if AI employment algorithms are trained on host-country labour market data that systematically discounts refugee credentials or exhibits occupational stereotyping, they risk automating discrimination rather than remedying it.³²

VI. AI IN BORDER SURVEILLANCE, SECURITY, AND THE CRIMINALISATION OF MOVEMENT

The deployment of AI in border management represents the most legally fraught and politically contested dimension of algorithmic humanitarianism. Governments across the globe are investing heavily in AI-powered border surveillance systems: thermal cameras linked to movement detection algorithms, social media monitoring and automated sentiment analysis, predictive risk profiling of travellers and asylum applicants, and drones equipped with facial recognition technology capable of identifying individuals in remote border zones. The European Union's border agency Frontex has invested substantially in AI-enhanced

²⁹UNHCR, COMPASS: Common Pipeline for Durable Solutions 2023 Annual Report (2023); Global Compact on Refugees, G.A. Res. 73/151, Annex, U.N. Doc. A/RES/73/151 (Dec. 17, 2018), paras. 47, 66-68 [hereinafter Global Compact on Refugees]; Declaration and Plan of Action, G.A. Res. 71/1, Annex I, U.N. Doc. A/RES/71/1 (Oct. 3, 2016) [hereinafter New York Declaration].

³⁰UNESCO, Recommendation on the Ethics of Artificial Intelligence, UNESCO Doc. SHS/BIO/REC/2021/1, paras. 44-47 (Nov. 23, 2021) [hereinafter UNESCO AI Recommendation] (calling on states to develop 'AI readiness' programs with particular attention to marginalized and displaced populations).

³¹Global Compact on Refugees, *supra* note 29, para. 47 (calling for 'digital and technological innovations' to improve access to services for refugees 'while respecting the rights and dignity of all concerned').

³²Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* 13-18 (2016); Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* 97-103 (2021).

surveillance technologies, integrating autonomous drones into Mediterranean border monitoring operations.³³

Human rights organisations have extensively documented the ways in which AI-enhanced border systems have facilitated the systematic pushback of asylum seekers in the Aegean and on the Western Balkan route, constituting potential violations of the principle of non-refoulement.³⁴ A state that deploys an AI system which generates risk assessments directing border officials to turn back persons who, unbeknown to the algorithm, are at risk of persecution in their country of origin, bears full legal responsibility for the resulting violation.³⁵ The interposition of an algorithm between the decision-maker and the consequences of the decision does not attenuate state responsibility; it merely introduces a new vector of opacity and impunity.

The legal analysis must proceed from first principles. Non-refoulement is a peremptory norm of international law admitting of no derogation, not even in the name of border security or counter-terrorism. A refugee who is erroneously classified as a security threat by an opaque automated system and turned back to a territory of persecution is entitled to the same legal protection as one turned back by a deliberately indifferent human official. This principle is affirmed by the doctrinal analysis of Molnar and Gill.

AI-driven surveillance within refugee camps, including closed-circuit television linked to facial recognition, mobile data collection, and social network analysis, raises analogous concerns. The use of such systems to police and monitor already traumatised populations reproduces the power asymmetries of the carceral state within the humanitarian space. Community accountability mechanisms must be built into any camp-level AI surveillance deployment.³⁶ The UN Special Rapporteur on Privacy has affirmed that the right to privacy in

³³Frontex, Risk Analysis for 2022, at 8-14 (2022). Frontex's investment in AI-enhanced surveillance includes drone operations in the Mediterranean and automated vessel detection systems linked to predictive analytics.

³⁴Human Rights Watch, Algorithms of Oppression: Big Data Discrimination Against Refugees at European Borders (2022); Amnesty International, Libya's Dark Web of Collusion: Abuses Against Europe-Bound Refugees and Migrants 43-49 (2017).

³⁵Petra Molnar & Lex Gill, Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System 23-29 (2018). The report documents how the Canadian immigration system's use of predictive scoring tools systematically disadvantaged claimants from low-income countries of origin.

³⁶S. Enria & J. Achtnich, Community Accountability in Humanitarian Settings: Lessons from AI-Assisted Aid Distribution, 45 Disasters: J. of Disaster Stud. & Mgmt. 1, 8 (2021); see also Oxfam, Responsible Program Data Policy 11-14 (2012) (on community feedback mechanisms in humanitarian data governance).

the digital age extends with full force to persons in refugee and displacement situations.³⁷

VII. SYSTEMIC CHALLENGES: ALGORITHMIC BIAS, DATA SOVEREIGNTY, AND AUTOMATED DECISION-MAKING

7.1 Algorithmic Bias and Structural Discrimination

Algorithmic bias, understood as the systematic and unjustified differential treatment of persons by computational systems on the basis of protected characteristics such as race, gender, ethnicity, religion, or national origin, is not a marginal or correctable flaw in AI systems. As scholars including O'Neil, Crawford, and Benjamin have argued, it is a structural feature of systems that learn from data generated by, and optimised for, dominant social orders.³⁸ Training data that reflects historical patterns of racial exclusion will produce algorithms that replicate those patterns; optimisation functions designed to maximise aggregate efficiency will systematically sacrifice the interests of minority groups.

In the refugee context, the risks of algorithmic bias are compounded by the extreme power asymmetry between the deploying organisation and the affected population. A refugee who is misidentified by a facial recognition system, denied food by an erroneous distribution algorithm, or rejected by an automated asylum credibility tool, lacks the social capital, legal status, and institutional access to challenge those decisions effectively. The result is a form of structural disenfranchisement, what Citron and Pasquale have termed the scored society, in which algorithmic outputs are treated as objective facts rather than contested predictions requiring scrutiny and accountability.³⁹

The ICCPR's prohibition on discrimination and the UNESCO Recommendation on the Ethics of Artificial Intelligence⁴⁰ jointly demand that AI systems deployed in refugee contexts be

³⁷Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/51/17, paras. 11-14 (Aug. 4, 2022) [hereinafter OHCHR Privacy Report]; Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Report, U.N. Doc. A/73/348, paras. 16-20 (Aug. 29, 2018).

³⁸Algorithm Watch, *Automating Society: A Report on Automated Decision-Making in Europe* 44-51 (2019); Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* 59-73 (2019). Benjamin's concept of the 'New Jim Code' captures the way in which algorithmic systems can encode racial hierarchy under a veneer of technical neutrality.

³⁹Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 18-23 (2014); Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 59-65 (2015).

⁴⁰UNESCO AI Recommendation, *supra* note 30, paras. 3, 40-42 (affirming the principles of human oversight, transparency, and non-discrimination as foundational to the ethical development and deployment of AI systems).

subject to mandatory pre-deployment algorithmic impact assessments, ongoing bias monitoring, and transparent public reporting on performance disaggregated by protected characteristics. The EU AI Act's classification of AI systems used in migration, asylum, and border control management as high-risk applications subject to enhanced conformity assessment requirements⁴¹ represents an important normative step. The ethical requirement of meaningful human control, developed in the context of autonomous weapons systems,⁴² is equally applicable to AI systems that make determinations about refugee status and entitlements.

7.2 Data Sovereignty and the Rights of Refugee Data Subjects

Refugees occupy a uniquely precarious position with respect to data governance. They are typically subject to data collection by multiple actors, including humanitarian organisations, host state authorities, and technology vendors, without effective capacity to exercise the data subject rights recognised under international and domestic data protection law: the rights of access, rectification, erasure, and objection.

A growing number of states are experimenting with AI systems to assist in the assessment of asylum claims, including automated credibility analysis, risk profiling based on country-of-origin data, and algorithmic triage of case complexity.⁴³ These systems raise acute concerns under the right to an effective remedy and the principle of procedural fairness. The opacity of commercially developed AI systems protected by intellectual property claims renders them particularly resistant to adversarial legal challenge. The counterfactual explanation methodology developed by Wachter, Mittelstadt, and Russell⁴⁴ represents a partial, though

⁴¹EU AI Act, *supra* note 9, arts. 6(2), Annex III (classifying AI systems used in biometric identification, migration and asylum management, and border control as 'high-risk' applications subject to mandatory conformity assessment and fundamental rights impact assessment requirements before deployment).

⁴²International Committee of the Red Cross, *Ethics and Autonomous Weapon Systems: An Ethical Basis for Human Control?*, Expert Meeting Report 9-13 (2018); see also UN Group of Governmental Experts on Lethal Autonomous Weapons Systems, Report, U.N. Doc. CCW/GGE.2/2019/3 (2019). The ethical principle of meaningful human control, developed in the context of autonomous weapons, is directly transposable to AI systems that generate life-altering determinations about refugees.

⁴³Natasha Staton, *AI and Refugee Status Determination: Can Machines Decide Who Is a Refugee?*, 34 *Int'l J. Refugee L.* 157, 162-67 (2022). Staton examines deployments in the UK, Australia, and the United States, finding that automated credibility assessment tools systematically discount culturally specific narrative styles that are common among non-Western asylum applicants.

⁴⁴Sandra Wachter, Brent Mittelstadt & Chris Russell, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 31 *Harv. J.L. & Tech.* 841, 855-62 (2018); Ignacio Cofone, *Algorithmic Discrimination Is an Information Problem*, 70 *Hastings L.J.* 1389, 1402-08 (2019).

insufficient, response to this challenge.

Meaningful protection of refugee data sovereignty requires: first, legally binding data sharing agreements between humanitarian organisations and host states with explicit prohibitions on use for migration enforcement, security surveillance, or political profiling; second, independent data protection supervisory authorities with jurisdiction over humanitarian data processing; third, genuine and revocable consent mechanisms for biometric and sensitive data collection; and fourth, technical architectures including differential privacy, federated learning, and cryptographic access controls that structurally limit re-identification and unauthorised access. These requirements are grounded in the foundational principles of AI ethics articulated by Floridi and colleagues.⁴⁵

VIII. TOWARD RIGHTS-COMPLIANT AI GOVERNANCE IN HUMANITARIAN SETTINGS: A NORMATIVE FRAMEWORK

The analysis in preceding sections demonstrates that the deployment of AI in refugee and humanitarian contexts is neither inherently progressive nor inherently harmful; it is a profoundly contingent normative and political choice, the consequences of which depend entirely upon the governance frameworks within which AI systems are designed, deployed, monitored, and held accountable. This Part articulates a normative framework for rights-compliant AI governance in humanitarian settings, organised around five principles.

A. Legality and Transparency

Every AI system deployed in a context affecting refugees' rights must have a sufficiently precise, publicly accessible, and rights-compliant legal basis. The principle of legality, recognised in the ICCPR and affirmed by the UNESCO AI Recommendation, demands that persons whose lives are affected by algorithmic systems be able to know of their existence, understand their purpose, and access information sufficient to enable challenge. Opacity by design, including commercial confidentiality claims over refugee-affecting AI systems, must be unacceptable as a matter of human rights law. The UN AI Advisory Body's 2024 report calls

⁴⁵Luciano Floridi et al., *An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, 28 *Minds & Machines* 689, 699-703 (2018) (articulating the principles of beneficence, non-maleficence, autonomy, justice, and explicability as the ethical foundations of AI governance).

for global AI governance standards with explicit application to vulnerable populations.⁴⁶

B. Non-Discrimination and Algorithmic Impact Assessment

All AI systems deployed in humanitarian settings must be subject to mandatory pre-deployment algorithmic impact assessments, conducted by independent experts, with results publicly available. These assessments must specifically evaluate the risk of discriminatory outcomes for refugees disaggregated by race, gender, ethnicity, disability, and age. UNHCR's Age, Gender and Diversity Policy⁴⁷ provides the analytical categories for such disaggregation. The EU AI Act's fundamental rights impact assessment requirement should be adopted as a minimum global standard for humanitarian AI deployments, independent of the jurisdiction of the deploying entity.

C. Human Oversight and Meaningful Review

No AI system should have final, unreviewable authority over decisions that significantly affect the rights of refugees, including decisions on registration, aid eligibility, asylum status, detention, and deportation. Human oversight must be genuine rather than nominal: human decision-makers must be provided with sufficient information, time, and institutional authority to meaningfully review, override, and be held responsible for algorithmic recommendations. The right to an effective remedy for adverse algorithmic decisions must be operationalised through accessible, timely, and linguistically appropriate complaint and appeal mechanisms, consistent with the obligations of states under the ICCPR.

D. Data Sovereignty and Purpose Limitation

Data collected from refugees for humanitarian purposes must not be shared with or accessible to state security agencies, immigration enforcement authorities, or commercial entities without explicit, specific, and revocable consent. Purpose limitation provisions in humanitarian data sharing agreements must be legally binding and subject to independent audit. The Special Rapporteur on Migrants has documented with particular clarity the harms arising from data

⁴⁶UN Secretary-General, *Governing AI for Humanity: Final Report of the AI Advisory Body*, at 14-19 (Sept. 2024) [hereinafter UN AI Advisory Body Report]; see also High-level Panel on Digital Cooperation, *The Age of Digital Interdependence* (2019).

⁴⁷UNHCR, *Policy on Age, Gender and Diversity* (2018) [hereinafter UNHCR AGD Policy]. The AGD Policy requires all UNHCR operations to ensure that programming is sensitive to the differentiated needs and protection risks of women, children, older persons, and persons with disabilities.

sharing between humanitarian actors and state immigration enforcement.⁴⁸ Technical architectures should embed privacy-by-design principles that structurally prevent re-identification and mission creep.

E. Inclusive Design and Community Participation

The design, deployment, and governance of AI systems affecting refugees should involve the meaningful participation of refugee communities themselves. As the UNESCO AI Recommendation affirms, AI must be designed and governed in a manner that preserves human agency and respects cultural diversity. Refugees, who are routinely the subjects of AI systems but almost never the designers, funders, or regulators, must have structured and resourced opportunities to shape the technologies that govern their lives. Gender-responsive design, co-creation methodologies, and community feedback loops are requirements of the human rights principle of participation,⁴⁹ implemented through the operational framework of responsible AI as articulated by Dignum.⁵⁰

IX. CONCLUSION

Artificial Intelligence is not a neutral technology. In the context of forced displacement, it is a set of choices, technical, political, financial, and normative, made by powerful actors about how to manage some of the world's most vulnerable persons. Those choices have profound and measurable consequences: for the Rohingya family whose biometric data was shared with the security apparatus of their persecutors; for the asylum seeker whose narrative was assessed as low credibility by an opaque algorithm and whose appeal was denied without explanation; for the refugee child who cannot access an AI-driven learning platform because there is no electricity in her camp.

This paper has argued that the deployment of AI in refugee contexts is governed by, and must

⁴⁸Special Rapporteur on the Human Rights of Migrants, Report on the Human Rights of Migrants at Borders, U.N. Doc. A/HRC/47/30, paras. 27-32 (May 12, 2021) (documenting how AI-enabled border management systems disproportionately harm women, children, and other vulnerable migrants, and calling for binding legal frameworks to govern data sharing between humanitarian actors and immigration enforcement authorities).

⁴⁹Tendai Pasipanodya, A Richer Sense of CEDAW's Transformative Equality: AI and Refugee Women's Dignity, 39 Neth. Q. Hum. Rts. 4, 11 (2021); UNHCR, Safe from the Start: UNHCR's Work on Gender-Based Violence Prevention and Response in Emergencies 18-22 (2020).

⁵⁰Virginia Dignum, Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way 97-102 (2019). Dignum's AETHER framework (Accountability, Explicability, Trustworthiness, Human-centredness, Ethics-based, Reliability) provides a comprehensive operational vocabulary for the governance principles proposed in this paper.

be held accountable to, a robust body of existing international human rights and refugee law. Non-refoulement, the prohibition on discrimination, the right to privacy, the right to an effective remedy, and the rights of the child are not suspended by the algorithmic character of the decision-making process. States and humanitarian organisations that deploy AI systems affecting refugees bear full legal responsibility for the rights violations those systems produce.

The normative framework proposed in this paper, grounded in legality, non-discrimination, human oversight, data sovereignty, and inclusive design, provides a principled basis for AI governance in humanitarian settings. Its realisation requires the concerted action of international organisations, states, technology companies, and, above all, the refugee communities whose dignity, safety, and futures are at stake. The promise of AI in the service of forced displacement response is real; but it will remain unredeemed until the algorithms that govern displaced persons are themselves governed by law.