INTERSOS
HUMANITARIAN AID

AI AND HUMAN RIGHTS AT THE FRONTLINES OF HUMANITARIAN CRISES: TOWARDS A RIGHTS-BASED INTEGRATED BORDER AND DISASTER RISK MANAGEMENT (IBDRM).

Marybelle Cherfan - PhD Candidate in Human Rights, Global Politics and Sustainability - Scuola Superiore Sant'Anna (Pisa, Italy)

Mike Bisi - Expert on Rights-based Migration and Border Management and Lecturer at Scuola Superiore Sant'Anna (Pisa, Italy)

Professor Melvis Ndiloseh - Maître des conferences in International Studies, Research Associate at Scuola Superiore Sant'Anna (Pisa, Italy)

ABSTRACT

Humanitarian crises today are increasingly transnational, transcending borders, and straining traditional response systems. From pandemics to conflict-induced displacement and climate-driven migration, these crises shed light on the urgent need for a *Rights-Based Integrated Border and Disaster Risk Management* (IBDRM) framework (a novel term coined in this article) to address the often-overlooked nexus between Border Management (BM) and Disaster Risk Management (DRM). Whilst conventional structures struggle to keep up with the scale and complexity of these crises, AI should and rightly ought to be a key enabler of the proposed IBDRM framework. When embedded within a *Rights-Based* approach and notwithstanding the ethical challenges that arise with its deployment; AI can foster proactive and responsive BM and DRM strategies, ensuring that human rights remain central even amid rapid decision-making and heightened security considerations. This paper subsequently advocates for AI safeguards rooted in (1) foundational principles, (2) ethical frameworks, (3) operational transparency, and (4) tailored practical applications. It also contributes to ongoing debates on humanitarian response by recommending context-contingent and scalable AI strategies that prioritize human rights within and across borders, high-level international coordination, and cohesive regulatory frameworks for more effective *IBDRM through AI*.

Keywords: Humanitarian Crises, Artificial Intelligence (AI), Border Management (BM), Disaster Risk Management (DRM), Human Rights, Rights-Based Integrated Border and Disaster Risk Management (IBDRM), AI Safeguards, International Coordination.

Marybelle Cherfan - PhD Candidate in Human Rights, Global Politics and Sustainability - Scuola Superiore Sant'Anna (Pisa, Italy) - Marybelle.cherfan@santannapisa.it

Mike Bisi - Expert on Rights-based Migration and Border Management and Lecturer at Scuola Superiore Sant'Anna (Pisa, Italy) - bisimike@gmail.com

Professor Melvis Ndiloseh - Maître des conferences in International Studies, Research Associate at Scuola Superiore Sant'Anna (Pisa, Italy) - ndiloseh.melvis@gmail.com

TABLE OF CONTENTS

1. INTRODUCTION: TOWARDS A RIGHTS-BASED IBDRM FRAMEWORK IN HUMANITARIAN CRISES

"When people are forced to flee from their homes through no fault of their own, they should be able to continue living in dignity and safety […] However, the system is under pressure like never before".[1] Contemporary challenges facing displaced populations are deepening as global displacement reaches alarming heights, driven by conflicts, climate change, pandemics, and natural disasters. The frail balance between security and human rights further complicates this landscape,[2] and underscores the urgent need for a comprehensive framework to provide humanitarian aid and manage displacement within and at borders during humanitarian crises.

While AI deployment in humanitarian crises is not new, its ongoing advancements emphasize its potential to foster much-needed anticipatory approaches in Border Management (BM) and Disaster Risk Management (DRM). Technology has long played a role in BM and DRM, yet its deployment has often lacked comprehensive human rights safeguards, leading to significant abuses. As we navigate the rapid evolution of AI, there is an unprecedented opportunity to align technological advancement with both human rights and security imperatives.

AI has the potential to enhance security measures while ensuring that human rights are respected in humanitarian crises. Yet, scholars have increasingly voiced concerns about the associated risks posed by AI deployment during such crises, including but not limited to algorithmic bias, surveillance overreach, and data privacy infringement.[3] These challenges underscore the need for a balanced approach that prioritizes human rights while leveraging AI's capabilities.

Against this backdrop, this article will assess *AI's role in fostering a rights-based and integrated BDRM (IBDRM) that prioritizes human rights within and at borders*, uniting two interconnected arenas within a previously overlooked nexus. Rather than relying on empirical data collection, it analyzes real-world cases and institutional practices to critically assess the potential of AI in a Rights-based Integrated Border and Disaster Risk Management (IBDRM) framework. The selected examples (such as Frontex's EUROSUR, UNHCR's Jetson, and WFP's SKAI) were chosen for their relevance to core IBDRM functions (such as Early Warning, Coordination, Aid Delivery, and Human Rights Protection) and the said analysis is informed by doctrinal research, comparative practice and critical perspectives reconciling Human Rights, International Law, AI governance and AI ethics.

---

[1] UNHCR, *Global Appeal 2024, Geneva, 2023,* available at: https://reporting.unhcr.org/global-appeal-2024.
[2] United Nations Counter-Terrorism Implementation Task Force, *Handbook on Human Rights and Screening in Border Security and Management,* 2018, available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/englsih-human-rights-booklet_un_13.pdf.
[3] Veron, P., *Digitalization in humanitarian aid: opportunities and challenges in forgotten crises*, European Centre for Development Policy Management (ECDPM), *Briefing Note* No. 143, 2022.

1.1. Increasing Displacement in the Context of Humanitarian Crises

Globally, there are 281 million international migrants,[4] 63.3 million internally displaced people, 43.3 million refugees, 6.9 million asylum seekers, and 4.4 million stateless individuals in search of safety, stability, and opportunity.[5] The past year "has brought devastating new conflict in Sudan, continued misery in Ukraine, a string of coups in the Sahel region, more violence in the Democratic Republic of the Congo, displacement in Myanmar, and a renewed conflict in Gaza [and Lebanon] that has raised risks across the region".[6] These words resonate deeply reflecting the dire situation of global displacement, which has reached unprecedented levels. By the end of 2023, over 117,3 million people were forcibly displaced, equating to more than 1 in every 69 people worldwide. Tireless conflicts, the undeniable impact of climate change, and the devastating effects of pandemics and natural disasters have exacerbated the situation, with the number of displaced people increasing annually for 12 consecutive years.[7]

Bearing in mind these stark numbers and the inherent human tragedies beneath them, there is an urgent need to mitigate the challenges of displacement, and part of this challenge lies in ensuring that responses are rooted in human rights-based approaches.

Displacement refers to the forced movement of people from their homes or places of habitual residence due to conflict, violence, persecution, natural disasters, or other life-threatening situations. It can be internal, within the borders of a country, or cross-border, where individuals flee to another country seeking safety and protection.[8]

As displacement continues to surge, the system is under immense pressure, straining traditional approaches to managing displacement and delivering humanitarian aid. The COVID-19 pandemic similarly demonstrated the vulnerability and volatility of global movement systems, with widespread border closures disrupting traditional migration patterns and complicating humanitarian responses. Future crises may equally necessitate rapid and large-scale adjustments in Border and Disaster Risk Management protocols, especially as both frameworks increasingly converge through population displacement: with BM and DRM frameworks that need to be adaptable, resilient and in cohesion.

Complex modern challenges often demand innovative solutions. AI, with its advanced capabilities, offers a promising avenue to strengthen and adapt aid delivery and manage displacement, potentially reshaping how we respond to humanitarian crises within and at borders. By leveraging

[4] McAuliffe, M. and Oucho, L.A. (eds.), World Migration Report 2024, International Organization for Migration (IOM), Geneva, 2024, available at: https://publications.iom.int/books/world-migration-report-2024.
[5] UNHCR, Global Trends Report 2023, Geneva, 2024, available at: https://www.unhcr.org/global-trends-report-2023.
[6] UNHCR (n 1)
[7] UNHCR (n 4)
[8] Adapted from Guiding Principles on Internal Displacement, annexed to United Nations Commission on Human Rights, Report of the Representative of the Secretary-General, Mr Francis M. Deng, Submitted Pursuant to Commission Resolution 1997/39, Addendum (11 February 1998) UN Doc. E/CN.4/1998/53/Add.2, para. 2 of the introduction.

AI, authorities can make informed decisions that minimize harm and ensure that even amidst restrictive measures, the fundamental rights and dignity of displaced and vulnerable populations are protected.

1.2. AI Deployment in Humanitarian Crises

AI is broadly understood as a collection of technologies that combine computing power, data, and algorithms to perform tasks that typically require human intelligence.[9] Learning, reasoning, and problem-solving are just a few examples of how AI can operate to achieve predetermined goals and improve itself autonomously.[10]

In the context of humanitarian crises, defined as a single event or chain of events that threaten the health, safety, and well-being of a large group of people,[11] AI's potential is increasingly recognized for its ability to enhance humanitarian aid delivery and manage population displacement. These crises require swift, coordinated responses to save lives and protect vulnerable populations, and AI can significantly improve these responses. For instance, AI-driven early warning systems can predict natural disasters or conflict outbreaks, enabling faster mobilization of aid.[12] Moreover, AI can optimize resource allocation by analyzing real-time data to determine where resources are most needed and improve coordination among different actors and entities on the ground.[13]

Nonetheless, the deployment of AI in humanitarian crises is not without significant challenges and ethical concerns. The risk of algorithmic bias, data privacy issues, and cybersecurity threats are particularly abundant in BM and DRM,[14] where the balance between ensuring security and upholding human rights is often precarious.[15] As AI continues to be deployed in these arenas, there is an urgent need to address the associated ethical concerns to ensure that AI serves humanitarian and security objectives without compromising fundamental human rights.

[9] **Valavanidis,** A., "Artificial Intelligence (AI) Applications: The most important technology we ever develop, and we must ensure it is safe and beneficial to human civilization," *ResearchGate*, p. 1, 2023 available at: https://www.researchgate.net/publication/369914014_Artificial_Intelligence_AI_Applications_The_most_important_technology_we_ever_develop_and_we_must_ensure_it_is_safe_and_beneficial_to_human_civilization_I.
[10] **Steunebrink, R., Thórisson, R., and Schmidhuber, J.,** "Growing Recursive Self-Improvers," *AGI Conference*, Vol. 16, 2016, available at: https://www.iiim.is/wp/wp-content/uploads/2014/05/AGI16_growing_recursive_self-improvers.pdf
[11] **European Commission, Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG ECHO),** *Humanitarian Protection: Improving Protection Outcomes to Reduce Risks for People in Humanitarian Crises.* Thematic Policy Document No. 8, 2016.
[12] Dineva, S., "Applying Artificial Intelligence (AI) for Mitigation Climate Change Consequences of the Natural Disasters," *Research Journal of Ecology and Environmental Sciences*, 2023, 3(1), pp. 1–8. Available at: https://www.scipublications.com/journal/index.php/rjees/article/view/343.
[13] Ghaffarian, S., Taghikhah, F., and Maier, H., "Explainable Artificial Intelligence in Disaster Risk Management: Achievements and Prospective Futures," *International Journal of Disaster Risk Reduction*, 2023, p. ff., pp. 1-12. DOI: 10.1016/j.ijdrr.2023.104123.
[14] AVELLO MARTÍNEZ, M., "EU Borders and Potential Conflicts between New Technologies and Human Rights," Peace Security - Paix et Sécurité Internationales, No 11, 2023. DOI: http://dx.doi.org/10.25267/Paix_secur_int.2023.i11.1204.
[15] **Beduschi,** A., "Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks," *International Review of the Red Cross* 104, no. 919: 1149–1169, 2022. DOI:10.1017/S1816383122000261.

1.3. Nexus of BM and DRM in Humanitarian Crises

Border Management (BM) has traditionally focused on regulating the flow of people and goods across borders, ensuring national security, and maintaining state sovereignty.[16] As represented by the blue ellipses in Figure 1, state sovereignty and border security remain central pillars of BM's role in protecting a nation's borders from external threats while regulating cross-border activities.

In contrast, Disaster Risk Management (DRM) aims to mitigate the risks associated with disasters through preparedness, response, and recovery efforts: with the integral aim to reduce risks, prevent new risks, and manage residual risks.[17] According to the Sendai Framework, a widely recognized global framework for disaster risk reduction, a disaster is defined as a "serious disruption of the functioning, and of a community or a society at any scale due to hazardous events interacting with conditions of exposure, vulnerability, and capacity[…]".[18] "Disasters can be caused by natural, man-made and technological hazards, as well as various factors that influence the exposure and vulnerability of a community".[19] Consequently, resilience to disasters and emergency response (represented by the red ellipses in Figure 1), both highlight DRM's distinctive role in anticipating, managing, and recovering from disasters that could have devastating impacts on communities.

Nonetheless, the roles of BM and DRM are no longer confined to their traditional scopes, and they no longer operate in isolation. There is, in fact, an inherent overlap between them in areas such as public safety, risk analysis and prevention, aid delivery and humanitarian assistance, and respect for human rights (represented by the purple ellipses in Figure 1),[20] the latter being the overarching rationale for both BM and DRM.

[16] International Organization for Migration IOM, *"Border Management," Global Compact Thematic Paper,* IOM publication, 2017, pp. 1-8.
[17] See Šakić Trogrlić, R., van den Homberg, M,, Budimir, M., McQuistan, C., Sneddon, A., Golding, B., "Towards the 'Perfect' Weather Warning: Bridging Disciplinary Gaps through Research and Practice," *Towards the 'Perfect' Weather Warning, Chapter 2: Early Warning Systems and Their Role in Disaster Risk Reduction,* 2022, pp. 11-36; Sendai Framework Terminology on Disaster Risk Reduction: https://www.undrr.org/terminology/disaster.
[18] Šakić Trogrlić, R (n 17).
[19] See IFRC website: https://www.ifrc.org/our-work/disasters-climate-and-crises/what-disaster.
[20] United Nations. *Human rights at international borders: A Trainer's Guide*, ISBN 978-92-1-154231-8. 2021.

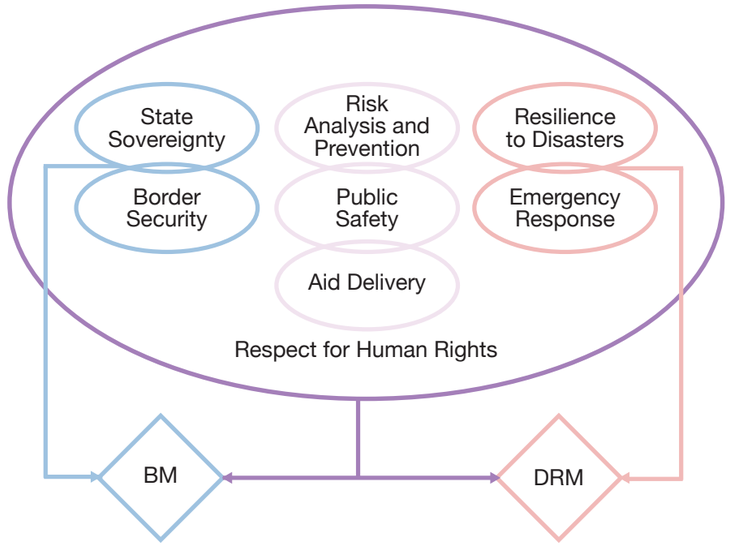

Figure 1: Rationale and Objectives for BM and DRM.

Source: Designed by the Authors of the Article.

The above-mentioned shared objectives are crucial not only for safeguarding national security but also for ensuring the well-being of populations affected by disasters or emergencies.

1.3.1. Integrated BDRM

BM and DRM were initially perceived as two separate frameworks pursuing distinct objectives. However, their roles are increasingly converging, particularly in the context of humanitarian crises with cross-border movement or transboundary impacts.[21] Such crises warrant a dual challenge: (1) managing aid delivery and resource allocation while simultaneously (2) addressing population displacement and protecting vulnerable populations within and at borders. This duality underscores the need for a *holistic framework* and a *comprehensive approach*.[22]

For instance, when a natural disaster strikes a border region, BM and DRM strategies must be harmonized to ensure that both border security and disaster response are effectively managed without compromising either. Similarly, during a pandemic, their objectives converge towards, among others, (1) managing the movement of people and goods, while (2) minimizing the risk of disease spread. Additionally, situations of mass displacement, whether due to conflict, environmental degradation, or large-scale emergencies, often have transnational and cross-border impacts, requiring coordinated efforts to ensure safe passage, provide humanitarian assistance, and maintain regional stability.

[21] Klein, M. I**,** *Cross-Border Collaboration in Disaster Risk Management,* Karlsruhe: Karlsruhe Institute of Technology (KIT), 2022, DOI: 10.5445/KSP/1000146368.
[22] Kanteler, Bakouros. "A Collaborative Framework for Cross-Border Disaster Risk Management in the Balkans." *International Journal of Disaster Risk Reduction,* 2024, p. 104506.

This is where the concept of a “one-stop shop” or “single window” environment becomes indispensable.[23] As illustrated in Figure 2, Integrated Border and Disaster Risk Management (IBDRM) optimally operates through seamless horizontal and vertical coordination and cooperation (represented by the green rectangle in the lower layer of Figure 2) among all stakeholders involved in humanitarian response and aid delivery.[24]

In this integrated approach, BM and DRM converge to pursue shared objectives (represented by purple rectangles in Figure 2). The latter include public safety and human security, as well as displacement management. Key tools (represented by blue rectangles in Figure 2) that aim to secure these objectives encompass: risk analysis and early warning systems, aid delivery and humanitarian assistance, and resource allocation. IBDRM (a novel term coined in this article to reflect this integrated governance approach) is shown to be anchored by overarching principles that must guide all actions within this framework, specifically human rights protection and the protection of vulnerable populations.[25] The former ensures that all actions are grounded in respect of human rights even amid security and disaster response efforts, while the latter reserves particular attention to the most vulnerable groups, ensuring they receive the protection and assistance needed.

[23] World Customs Organization (WCO). *Understanding the Single Window Environment,* Vol. 1, Part I. World Customs Organization, 2011.
[24] Ibid.
[25] United Nations (n 17).

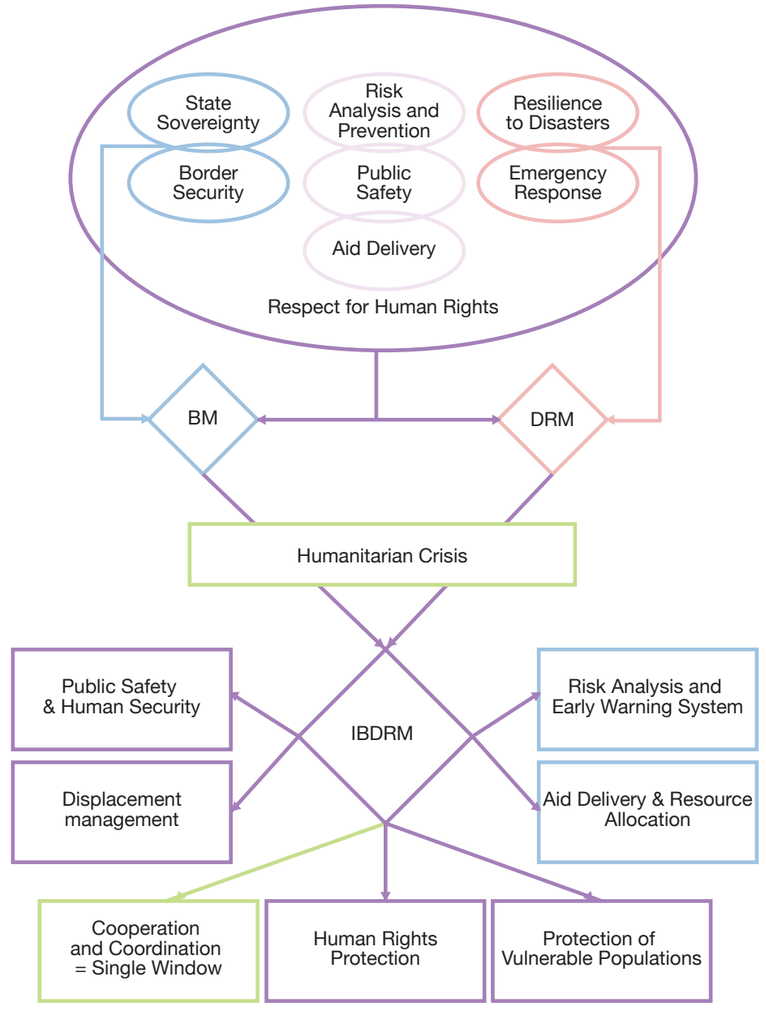

Figure 2: The Nexus of BM and DRM in the Context of Humanitarian Crises.

Source: Designed by the Authors of the Article.

By integrating BM and DRM, IBDRM promotes simplified and harmonized procedures, effective resource use, faster processing of people and goods and enhanced protection of vulnerable populations. DRM efforts might include, for example, establishing humanitarian corridors in coordination with BM to ensure the safe passage of aid and displaced individuals. This integrated response mechanism is crucial for addressing the complex and multifaceted challenges posed by humanitarian crises, particularly those involving mass displacement and cross-border movements.[26]

[26] Kalogiannidis, S. “Analyzing the Challenges of Cross-Border Disaster Response and Management: A European Perspective.” Journal of Risk Analysis and Crisis Response, Vol. 14, No. 2, pp. 178-204, 2024. DOI: 10.54560/jracr.v14i2.470.

However, it is not enough to have a theoretical framework for IBDRM. It must be supported by operational means that translate theory into practice: scalable policies that can be adapted to different contexts, inclusive processes that engage all relevant stakeholders, and rigorous oversight mechanisms to ensure that human rights are consistently upheld.

The success of IBDRM depends on its ability to move beyond theoretical models and provide actionable strategies that can be implemented on the ground, offering practical solutions to the complex challenges faced during humanitarian crises.

1.3.2. Patchwork Agreements in a Leaky Umbrella: Legal and Administrative Gaps in Current BM-DRM Cooperation

While the convergence of BM and DRM is increasingly recognized in practice, particularly in the context of humanitarian crises, the legal mechanisms, whether through soft or hard law, that currently exist to support this cooperation, are often described as frail.[27] The existing instruments offer fragmented solutions to a global problem, much like a *leaky umbrella* that covers certain aspects of the BM-DRM relationship but leaves critical gaps exposed.

Regional agreements like the EU Civil Protection Mechanism (EUCPM) have played a pivotal role in promoting cross-border collaboration for humanitarian assistance by allowing, among others, EU member states to share resources and expertise quickly in response to disasters.[28] Notwithstanding the importance of such a framework, administrative and legal disparities have persisted and have often hindered the mechanisms' overall efficiency. These are even more pronounced in situations of cross-border crises or emergencies with transnational impacts.

Diverse national laws complicate the operational executions of DRM and BM protocols which often result in delays when emergency procedures recognized in one country are not applicable in another, underlining once again an urgent need for a *harmonized legal framework* to ease transnational cooperation.[29] Moreover, administrative hurdles, from varying requirements to inconsistent resource allocation protocols and very often incompatible national systems, can be detrimental to much-needed efficient and rapid responses.[30]

Against that backdrop, bilateral and multilateral agreements frequently form the backbone of current cross-border and international cooperation.[31] These agreements can expedite the flow of resources, personnel, and aid during emergencies.

The U.S.-Mexico Emergency Management Cooperation Agreements, allows, for example, for

[27] T. R. Carter, et al., "A conceptual framework for cross-border impacts of climate change," Vol. 69, No. June, 2021. DOI: 10.1016/j.gloenvcha. 2021.102307.
[28] Fdd C. Berchtold, M. Vollmer, P. Sendrowski, F. Neisser, and L. Mu, "Barriers and Facilitators in Interorganizational Disaster Response : Identifying Examples Across Europe," pp. 46–58, 2020. DOI: 10.1007/s13753-020-00249-y.
[29] Appleby-Arnold, S., Brockdorff N., and Jakovljev, I., "Disaster preparedness and cultural factors : a comparative study in," Vol. 45, No. 3, pp. 664–690, 2021. DOI: 10.1111/disa.12433.
[30] Kanteler, D. and Bakouros, I. "Enhancing cross-border disaster management in the Balkans: a framework for collaboration part I." Journal of Innovation and Entrepreneurship, 13(15), 2024. DOI: 10.1186/s13731-024-00374-8.
[31] Ibid.

the swift cross-border movement of rescue teams and resources, quickly bypassing traditionally lengthy custom procedures.[32] However these agreements, while effective in specific contexts, remain fragmented and often leave critical gaps uncovered.

To illustrate the fragmented yet evolving landscape of legal and operational cooperation across borders, the table below (Table 1) lists selected frameworks that address aspects of Border Management (BM), Disaster Risk Management (DRM), and Humanitarian Coordination (including examples from Europe, Africa, Southeast Asia, and North America). While each initiative indisputably offers valuable mechanisms, ranging from disaster response to refugee reintegration; none provide a fully integrated or enforceable model that bridges BM and DRM through a rights-based lens.

Their diversity in scope, legal force, and implementation capacity underscores the pressing need for a cohesive IBDRM framework that is both context-sensitive and grounded in human rights.

Table 1: Illustrative Examples of Legal and Operational Frameworks in BM and DRM.

Source: Designed by the authors of the article.

FRAMEWORK/ AGREEMENT	SCOPE	STRENGTHS	LEGAL/OPERATIONAL GAPS
EU Civil Protection Mechanism (EUCPM)[33]	Regional (EU)	Quick Resource Sharing and Response Coordination	Uneven Implementation and Lacks Global or BM Reach
U.S.–Mexico Emergency Management Cooperation[34]	Bilateral	Rapid Deployment and Customs Bypass	Limited Applicability; Non-Binding[35]
Sendai Framework for Disaster Risk Reduction[36]	Global	Widely Adopted Risk Reduction Principles	No Binding Enforcement; Not Integrated with BM Mandates
Tripartite AU-HoA-UNHCR Framework (2020)[37]	Regional (Africa)	Coordinated Return and Reintegration of Refugees in the Horn of Africa	Fragile Political Buy-in; Weak enforcement

[32] Kayyem, J., Emergency Management in North America. Working Paper, North America 2.0: Forging a Continental Future, 2022.
[33] European Commission, "EU Civil Protection Mechanism," Directorate-General for European Civil Protection and Humanitarian Aid Operations, 2023. Available at: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en
[34] U.S. Department of State, "U.S.–Mexico Joint Declaration," Bureau of Western Hemisphere Affairs, June 7, 2019. Available: https://2017-2021.state.gov/u-s-mexico-joint-declaration/
[35] Based on MOUs and informal protocols.
[36] United Nations Office for Disaster Risk Reduction (UNDRR), "Sendai Framework for Disaster Risk Reduction 2015–2030," United Nations, 2015. Available: https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030.
[37] See UNHCR, African Union Commission, and IGAD. "Final Communiqué of the Ministerial Stocktaking Meeting on the Nairobi Declaration and Action Plan." 2020. Available at: https://www.refworld.org/docid/5fc125574.html; UNHCR. "Regional Update – East and Horn of Africa and the Great Lakes." 2022. Available at: https://www.unhcr.org/sites/default/files/legacy-pdf/63315ac04.pdfUNHCR+1UNHCR+1.

ASEAN Agreement on Disaster Management and Emergency Response (AADMER)[38]	Regional (Southeast Asia)	Legally Binding Disaster Response Cooperation	Limited Interaction with Border Security Protocols

Further complicating the picture are sovereignty concerns and political considerations, which create additional obstacles to timely intervention. The sovereignty-related hesitation not only delays the provision of crucial aid but also intersects with broader questions about security and human rights considerations within and at borders.

1.3.3. Security vs. Human Rights within and at Borders

While the IBDRM framework offers numerous benefits, it also brings to the forefront a critical tension that has always been simmering under the surface: the balance between ensuring security and upholding human rights within and at borders. This clash is not a new one and can be traced back to the post-9/11 era when the dichotomy between human rights and security was heavily marked.[39] Yet humanitarian crises often act as a catalyst where this tension becomes most pronounced.

State sovereignty and border security have traditionally aligned more closely with security imperatives. For BM, these security imperatives might involve enforcing stricter border controls, prioritizing national resources, or managing the flow of displaced populations.[40] For instance, during a sudden influx of refugees due to a nearby conflict, BM authorities may implement emergency measures to regulate entry, focusing on maintaining national security and public order. These actions, while necessary, can lead to the curtailment of certain human rights, such as freedom of movement or the right to seek asylum.[41]

Conversely, the security objectives within DRM traditionally focused on immediate response and recovery in the face of disasters. This includes deploying emergency response teams, safeguarding critical infrastructure, and ensuring that public safety is maintained even in the face of significant disruption.[42] For example, during a natural disaster with cross-border implications, DRM authorities might coordinate evacuations, manage emergency shelters, and prioritize the distribution of essential resources.[43] These actions are vital for protecting lives but might

[38] ASEAN. "ASEAN Agreement on Disaster Management and Emergency Response (AADMER)." Jakarta: ASEAN Secretariat, 2005. Available at: https://agreement.asean.org/media/download/20220330063139.pdf
[39] Goold, B., and Lazarus, L**.** *Security and Human Rights: The Search for a Language of Reconciliation*. Hart Publishing, 2007, pp. 1-24.
[40] SALGADO, L., FRATZKE, S., HUANG, L., and DORST, E., *Managing International Protection Needs at Borders*, Migration Policy Institute, 2024.
[41] Ibid.
[42] German Federal Ministry for Economic Cooperation and Development (BMZ), *Disaster Risk Management – Understanding Risks, Preventing Disasters, Strengthening Resilience*, BMZ, 2022, pp. 1-32.
[43] Ibid.

sometimes clash with human rights considerations, especially when decisions need to be made rapidly to save as many lives as possible.[44]

While some of the above-mentioned objectives serve security imperatives exclusively, others also serve human rights imperatives. Public safety, for instance, is a common goal that seeks to protect the population from harm, whether from external threats or natural disasters and requires measures that respect individuals' rights. Similarly, aid delivery must be conducted efficiently and equitably, ensuring that all individuals, regardless of their status, receive the necessary support.[45] The overarching principle of respect for human rights, as illustrated in Figures 1 and 2, serves as a reminder that the primacy of human rights must not come into question, and security objectives should not override the fundamental rights and dignity of individuals affected by humanitarian crises.

Conventional perspectives often dictate that security must be ensured before human rights can be addressed, leading to policies where humanitarian assistance is delayed or diminished until perceived threats are neutralized. However, this approach overlooks the fundamental truth that lasting security is inherently linked to the protection and promotion of human rights. The OHCHR's Human Rights at International Borders principle of *immediate assistance* effectively illustrates that prioritizing human rights is not at odds with, but rather integral to, effective border management and crisis response.[46] Thus, by embedding human rights at the core of security strategies, we create a comprehensive approach that strengthens both individual rights and overall security.

The prevailing perception has always been that security should take precedence over human rights, but true security is unattainable without the protection of human rights. Neglecting human rights can only lead to more vulnerability and instability; whereas integrating human rights considerations at the heart of all policies even security policies is essential for developing effective and sustainable IBDRM strategies that truly safeguard individuals and nations.

1.3.4. Towards a Rights-Based IBDRM

"Human rights should be at the heart of all their actions".[47] This guiding principle underlines the importance of human rights in both border governance and Disaster Risk Management. While security measures are paramount in both BM and DRM, they must not come at the expense of human rights. This aligns with the Recommended Principles on Human Rights at International Borders, which emphasize that states shall implement their international legal obligations in good

[44] United Nations Office for Disaster Risk Reduction (UNDRR), Human Rights and Disaster Risk Reduction: Strengthening the Implementation of the Sendai Framework for Disaster Risk Reduction 2015-2030. Considerations from the Asia-Pacific Region, New York, and Geneva: United Nations, 2023. Available at: https://creativecommons.org/licenses/by-nc-nd/3.0/igo/.
[45] Ibid.
[46] Office of the United Nations High Commissioner for Human Rights (OHCHR), *Recommended Principles and Guidelines on Human Rights at International Borders*, Geneva, 2014.
[47] United Nations, *Human Rights and Screening in Border Security and Management: Pocketbook for Field Screening*, Counter-Terrorism Implementation Task Force (CTITF) Working Group on Protecting Human Rights while Countering Terrorism, New York, 2018.

faith and respect, protect, and fulfill human rights in the governance of their borders.[48]

In the context of IBDRM, the said principle implies that whether states are attempting to secure their borders, respond to disasters, or do both, they must do so in a manner that upholds the dignity, safety, and rights of all individuals, particularly those who are most vulnerable.[49] The primacy of Human Rights serves as a foundational element within the IBDRM framework, guiding all actions and decisions.

Against this backdrop, a rights-based approach, whether aimed at securing borders or managing disasters, is evaluated through the lens of their potential impact on human rights. For instance, while stringent border controls may be necessary to maintain security, they should not result in the indiscriminate detention of individuals or the denial of their right to seek asylum.[50] Similarly, in DRM, the allocation of resources and prioritization of responses must ensure that all affected populations receive the assistance they need without discrimination.[51] This approach requires states to actively engage in protecting and fulfilling human rights, not merely avoiding corresponding violations. This could involve measures such as ensuring access to legal assistance for those affected by border controls and guaranteeing that emergency responses are inclusive and equitable.

Ultimately, the integration of human rights into the IBDRM framework represents a commitment to safeguarding the inherent dignity of all individuals, even in the most challenging circumstances.[52] It reinforces the notion that security and human rights are not mutually exclusive but can and must be pursued in tandem to ensure a just and humane response to humanitarian crises.

1.4. AI as a Promising Avenue for Rights-Based IBDRM

In the multifaceted landscape of IBDRM, the deployment of AI represents a promising avenue that can enhance operational efficiency and uphold human rights. AI can, among other things, improve risk analysis and early warning systems, enabling predictive capabilities that allow for preemptive actions in crisis-prone areas.[53] It optimizes humanitarian assistance and aid delivery by ensuring that resources are distributed equitably and efficiently and ensures public safety by monitoring real-time data to detect threats and track displacement.[54] AI accordingly offers the potential to help actualize a cohesive IBDRM framework by facilitating the seamless coordination of operations across borders, enhancing decision-making, and addressing the often overlooked

[48] Office of the United Nations High Commissioner for Human Rights (n 32).
[49] Office of the United Nations High Commissioner for Human Rights OHCHR and Global Migration Group, *Principles, and Guidelines on the human rights protection of migrants in vulnerable situations,* 2017.
[50] The European Network of National Human Rights Institutions ENNHRI, *Protecting Human Rights of Migrants at the Borders: Evidence and Work of European National Human Rights Institutions*, December 2019.
[51] Sommario, E., and Venier, S., *Human Rights Law and Disaster Risk Reduction*, QIL, Zoom-in 49, 2018, pp. 29-47.
[52] United Nations, *Transforming Our World: The 2030 Agenda for Sustainable Development*, General Assembly resolution 70/1, Annex, para. 4.
[53] Božić, V., The Role of Artificial Intelligence in Risk Management, Preprint, 2023. DOI: 10.13140/RG.2.2.29886.77126.
[54] Morocco Solidarity Hackathon, "Leveraging AI for Natural Disaster Risk Management: Takeaways from the Moroccan Earthquake," Preprint, 2023. Available at: https://arxiv.org/abs/2311.08999v2.

dynamics between DRM and BM. Nevertheless, the deployment of AI in IBDRM is not without undesirable challenges, such as the risk of algorithmic bias, data privacy concerns, and the potential misuse of AI, which can undermine human rights.[55]AI safeguards thus play a crucial role in mitigating these risks, ensuring that AI systems are designed and deployed in ways that protect human rights.

Given the outlined challenges, the central query of this article is: How can AI be leveraged for a rights-based IBDRM framework that enhances operational efficiency while protecting vulnerable populations during humanitarian crises? The problem statement encapsulates the need for a framework that not only incorporates AI to improve disaster and border management but also ensures that such advancements are not achieved at the expense of human right. The analysis is thus set to identify AI strategies for a Rights-Based IBDRM, and the purpose of the paper is thus twofold. First, it advocates for the implementation of a rights-based IBDRM framework to improve disaster and border management in humanitarian crises. Second, it explores how AI can be leveraged to support this framework, ensuring that human rights protections are at the core of operational advancements.

[55] Velev, D., Zlateva, P. "Challenges of Artificial Intelligence Application for Disaster Risk Management." *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences,* Vol. XLVIII-M-1-2023, 39th International Symposium on Remote Sensing of Environment (ISRSE-39), Antalya, Türkiye, 2023. DOI: https://doi.org/10.5194/isprs-archives-XLVIII-M-1-2023-387-2023.

2. ASSESSING AI'S IMPACT ON RIGHTS-BASED IBDRM

The COVID-19 pandemic has been a stark reminder that everyone's global village needs robust, adaptable responses to humanitarian crises. "Today, artificial intelligence is ubiquitous in its applications […]",[56] and as the world grapples with intensifying humanitarian crises, "it is witnessing first-hand how digital technologies help confront the threat […]".[57] From predictive models that track the virus' spread to AI-driven medical research, these technologies have proven indispensable in mitigating the impact of the pandemic, advancing urgent medical research, and keeping populations informed and connected.[58]

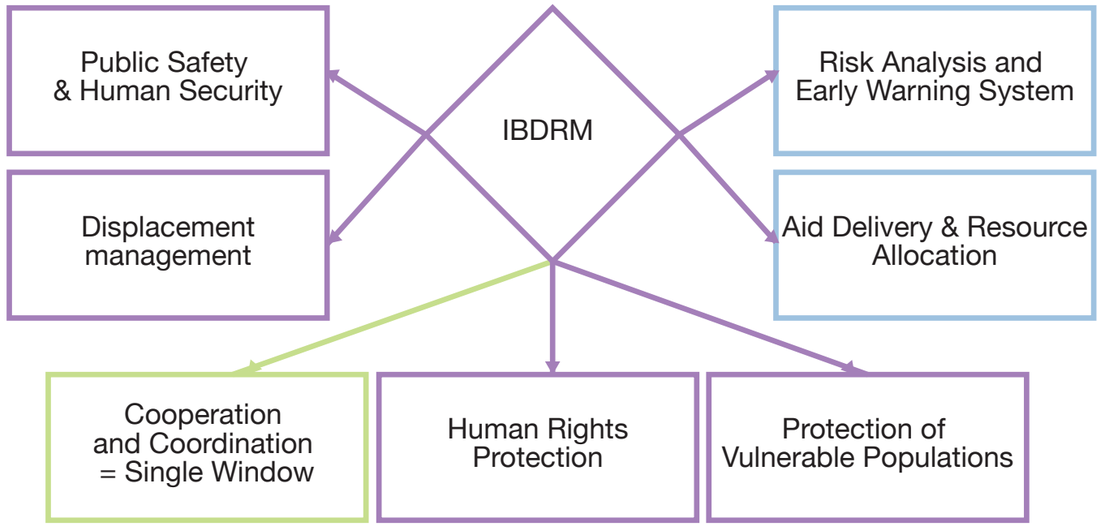

Figure 3: Rights-Based IBDRM Framework in the Context of Humanitarian Crises.

Source: Designed by the Authors of the Article.

[56] UN General Assembly, RoaDRMap for Digital Cooperation: Implementation of the Recommendations of the High-Level Panel on Digital Cooperation. Report of the Secretary-General, UN Doc. A/74/821, 29 May 2020 (Secretary-General's RoaDRMap), para. 6, available at: https://undocs.org/A/74/821 (all internet references were accessed in December 2020).
[57] Ibid.
[58] Pizzi, M., Romanoff, M., & Engelhardt, T., "AI for Humanitarian Action: Human Rights and Ethics", *International Review of the Red Cross*, 2021, 102(913), 145–180. Available at: https://doi.org/10.1017/S1816383121000011.

However, as AI is deployed everywhere, including within BM and DRM frameworks, the need for a structure that embeds human rights at IBDRM's core has never been more urgent. AI's predictive power, adaptability, and scope offer immense opportunities to improve humanitarian response, yet these benefits must be carefully balanced against complex multi-faceted risks that AI deployment might pose; whether the latter are unavoidable consequences of legitimate uses or harmful consequences of malicious uses.[59]

Figure 3 reiterates the theoretical framework for rights-based Integrated Border and Disaster Risk Management (IBDRM) that was portrayed in the introduction. In this integrated framework, BM and DRM converge on shared objectives under a single-window approach: (1) public safety and human security as well as (2) displacement management. These objectives are achieved through the key tools of (A) risk analysis and early warning systems, (B) aid delivery and resource allocation, and finally (C) cooperation and coordination. IBDRM is guided by the overarching principle of human rights protection and hence the equally important principle of protection of vulnerable populations.

With this framework in mind, this article will first (1) assess AI's impact on identified IBDRM objectives, tools, and core principles, by acknowledging that AI is a double-edged sword, before (2) advocating for safeguards and best practices to ensure AI is leveraged for an improved IBDRM with human rights principles embedded at its core.

2.1. AI and Rights-Based IBDRM in Humanitarian Crises

Growing concern over AI deployment in humanitarian action hasn't deterred several organizations from exploring its many advantages. Cutting costs and response time, subtracting human biases, automation at scale, and safeguarding the agency of affected people over their private data, are just a fraction of AI's uncharted potential in humanitarian crises.[60] To fully harness this potential, AI must be thoughtfully integrated into various critical functions of Border Management (BM) and Disaster Risk Management (DRM) through a rights-based approach.

2.1.1. Risk Analysis and Early Warning Systems

In the context of rights-based IBDRM, AI-driven risk analysis and early warning systems are not only pivotal for enhancing border security and disaster response but also for upholding human rights by ensuring that proactive measures are in place to mitigate threats and crises, manage displacement, and protect vulnerable populations.

[59] Ibid.
[60] Coppi, G., Jimenez, R. M., & Kyriazi, S. "Explicability of Humanitarian AI: A Matter of Principles." Journal of International Humanitarian Action, 2021, 6(19). Available at: https://doi.org/10.1186/s41018-021-00096-6.

In DRM, AI-supported disaster mapping has proven to be a turning point. For instance, during Cyclone Idai in 2019, the said tool was a game-changer for enabling swift emergency response in Mozambique.[61] The latter utilized satellite imagery and machine learning algorithms to rapidly assess the extent of flooding and infrastructure damage. The resulting *disaster map* and *real-time updates* were critical for coordinating relief efforts, prioritizing aid delivery, and estimating the number of displaced people.[62] The AI-driven shift from reactive to anticipatory humanitarian action allowed for a more efficient and targeted response. Another significant example within DRM is UNHCR's Jetson project: an initiative that was launched in 2017 by the Office of the United Nations High Commissioner for Refugees (UNHCR).[63] It leverages predictive analytics to forecast forced displacement in Somalia.[64] Machine learning is used to analyze data including but not limited to rainfall patterns, conflict data, market prices, and satellite imagery. It is said that this system can predict events up to three months in advance.[65] This AI-driven initiative helps organizations plan interventions more effectively to ensure that aid reaches those who need it the most.

Similarly in the context of BM, AI-driven risk analysis and early warning systems are crucial for enhancing border security by, for instance, predicting and mitigating potential threats and managing migration flows. One example of AI use at borders is Frontex's European Border Surveillance System (EUROSUR), which integrates various forms of data, such as satellite imagery from the Copernicus program, drone surveillance, and intelligence from member states to provide situational awareness and predictive analytics to detect irregular migration patterns and cross-border crimes.[66] EUROSUR leverages information from large-scale systems to identify changing routes and methods used for illegal immigration and cross-border crime, ensuring a proactive approach to border security and migration management. In addition to its role in border security, EUROSUR is a critical tool in search and rescue operations (though its humanitarian intent has often been contested)[67]: enabling, for example, rapid detection of vessels in distress.[68]

The above-mentioned examples demonstrate how leveraging AI in BM and DRM can enhance humanitarian response efforts within and at the borders through risk analysis and early warning systems in compliance with the principles of a rights-based IBDRM.

[61] United Nations Office for the Coordination of Humanitarian Affairs (OCHA), From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action, New York, 2021.
[62] Ibid.
[63] See the Project Jetson website, available at: https://jetson.unhcr.org.
[64] Ibid.
[65] Morente González, D., & Blasi Casagran, C., "Final EMT Analysis Report." Deliverable 7.5, Horizon 2020 Research and Innovation Programme, Universidad Autónoma de Barcelona, Munster Technological University, and Centre for Research and Technology, August 2023.
[66] Copernicus Support Office (n 62).
[67] While EUROSUR has been described as enhancing situational awareness and supporting search and rescue operations, its effectiveness and intentions have been contested by scholars and human rights organizations, who argue it often serves enforcement rather than humanitarian aims. See Tazzioli, M. 'The Making of Migration: The Biopolitics of Mobility at Europe's Borders', SAGE Publications, 2020; Human Rights Watch 'No Escape from Hell: EU Policies Contribute to Abuse of Migrants in Libya', Available at: https://www.hrw.org/report/2019/01/21/no-escape-hell/eu-policies-contribute-abuse-migrants-libya; Border Forensics, 'Remote Control: EU Surveillance and the Externalization of Borders', 2022 Available at: https://www.borderforensics.org .
[68] Copernicus Support Office, Copernicus Security Services Strategic Research Agenda: Issue 2023 Version 1.0a, 2023, Available at: https://www.copernicus.eu/sites/default/files/2023-09/CSS-SRA%20Guidelines%20for%20call%20HORIZON-CL4-2024-SPACE-01-36.pdf

2.1.2. Aid Delivery and Resource Allocation

AI-driven resource allocation is essential for ensuring that resources reach those in need, swiftly, efficiently, and equitably, within and at borders. This is not only crucial in disaster response but also in addressing humanitarian assistance needs that arise in border regions.

One notable example is the World Food Program's (WFP) partnership with Google to establish SKAI, a mapping project powered by AI. By comparing satellite imagery of buildings before and after a disaster, SKAI can quickly detect damaged structures, directing aid to the most affected areas and ensuring a more targeted and equitable distribution of resources.[69]

Likewise, WFP's HungerMapLIVE, a global food security monitoring tool, identifies food shortages and regions that are sliding towards food insecurity, enabling a preemptive resource allocation and timely responses to emerging food crises.[70] Such tools enhance the operational effectiveness of aid delivery: resources are also allocated more efficiently and equitably to reach the most vulnerable, including those in border areas where populations are often at risk of neglect. Another initiative, the Forecast-based Financing program deployed by the International Federation of Red Cross and Red Crescent Societies (IFRC) uses AI to preemptively allocate resources ensuring timely aid delivery.[71]

Additionally, the UNHCR's Biometric Identity Management System (BIMS) aids in the allocation of resources by verifying identities and managing the flow of displaced persons, particularly in border regions, thus ensuring that aid reaches the right individuals.[72]

These AI-driven approaches not only optimize resource allocation but also highlight the need for integrated and coordinated efforts among humanitarian actors working both within and at borders, setting the stage for a more unified response through a *Single Window* structure.

2.1.3. Single Window: Cooperation and Coordination

Integrated Border Management (IBM) is not a new concept per se; it has long been established as a cornerstone of border control, ensuring the seamless coordination of various agencies, from customs to immigration to law enforcement.[73] Nevertheless, in the context of today's complex humanitarian crises, marked by increased displacement, IBM must evolve into a more comprehensive rights-based Integrated Border and Disaster Risk Management framework. AI-

[69] See the World Food Program's AI for Good page for more details on SKAI and HungerMapLIVE: WFP AI for Good.
[70] Ibid.
[71] IFRC, "Forecast-based Financing: A New Era for the Humanitarian System", 2021.
[72] Su, Y., Cowper-Smith, Y., and Thayaalan, S., "The Double-Edge Sword of Humanitarian Technologies: A Case Study of UNHCR's Use of Biometrics Technologies", Working Paper, Defence and Security Foresight Group, York University, 2023.
[73] European Commission, "Guidelines for Integrated Border Management in European Commission External Cooperation," EuropeAid Cooperation Office, November 2010.

driven tools can be essential allies in this endeavor by facilitating coordination through a single-window approach at multiple layers, including intra-agency, inter-agency, and international levels.

The Smart Borders Framework in the EU exemplifies an advanced model of IBM through AI. The framework, built on four key pillars utilizes AI to streamline operations. (1) The Entry/Exit System (EES) automates the registration of travelers, (2) the European Travel Information and Authorization System (ETIAS) conducts pre-travel checks to verify eligibility, (3) the European Criminal Records Information System - Third Country Nationals ECRIS-TCN enhances cross-border cooperation by sharing criminal records of third-country nationals and (4) interoperability at the core of this structure leverages AI and biometric technologies to enable seamless data exchange, faster identification, harmonized process and enhanced coordination.[74]

AI-powered tools are also enhancing coordination in DRM. In Uganda, AI-powered chatbots were used to enable real-time disaster alerts and damage reporting and ensure a smooth flow of information between affected populations and responders.[75] Crucial access to information and emergency services was at the core of this pilot project to enhance coordination efforts on the ground.

Although these initiatives show significant progress in both IBM and DRM, they have not yet achieved true integration. The ideal IBDRM structure would bring together border control, humanitarian response, and human rights protection within a centralized, interoperable system encompassing diverse operational layers: a structure that involves both horizontal coordination (across agencies such as immigration, health and emergency response) and vertical coordination (local, national and international actors). One example of how this could work in practice would be an integrated digital platform connecting DRM early warning systems with customs and immigration databases, border crossing points, and humanitarian logistics networks. Such an interface would require shared data standards, interoperability protocols, clear accountability structures, and an overarching rights-based governance framework to ensure that operational efficiency does not come at the expense of individual rights and protections.

AI, therefore, emerges as a promising avenue for achieving seamless coordination through a single-window approach at the heart of IBDRM; to better address today's complex humanitarian challenges.

2.1.4. Public Safety and Human Security

Building on AI-driven risk analysis, early warning systems, aid delivery, and resource allocation within and at borders; ensuring public safety and human security is a fundamental objective of a rights-based IBDRM. AI tools like Facebook's safety check facilitate real-time communication

[74] Babel Street, "Border Management Today: Issue 11," International Border Management and Technologies Association Ltd., May 2024.
[75] UNESCO. "Report on Training Workshops on Artificial Intelligence for Disaster Risk Reduction in Uganda", Strengthening Disaster Prevention Approaches in East Africa (STEDPEA), Kampala: Uganda National Commission for UNESCO, 2022.

during disasters, allowing individuals to report their status and alert authorities and loved ones. Other tools such as the Emergency Situation Awareness platform in Australia and New Zealand,[76] or the Artificial Intelligence for Disaster Response build on social media posts and classify content to inform humanitarian actors and improve situational awareness.[77]

Moreover, AI is increasingly being deployed to enhance Search and Rescue (SAR) operations. The International Maritime Rescue Federation (IMRF) has explored the use of remotely operated and autonomous crafts to improve SAR efficiency.[78] Additionally, during public health crises such as pandemics, AI plays a critical role in monitoring cross-border health risks, facilitating contact tracing, and managing quarantine protocols. For example, the European Travel Information and Authorization System (ETIAS) advocated for AI use to pre-screen travelers, by cross-referencing traveler data against health databases, thereby aiding in the containment of pandemics while maintaining smooth and secure travel.[79] Similarly, in 2021, Travizory Border Security implemented an AI-powered biometric corridor for travel screening in the Republic of Seychelles, capable of screening 30 travelers per minute for potential health risks.[80] Such AI-advanced screening systems ensure both public health protection and efficient border management.

2.1.5. Displacement Management

Effective displacement management, another core objective of rights-based IBDRM: relies heavily on AI, as well, to streamline the identification and reunification of displaced individuals. The Trace the Face tool, used by the International Committee of the Red Cross (ICRC), deploys AI-powered facial recognition to automate searches for missing people, expediting the process of reuniting families separated by crises.[81] Mitigating the psychological impact of crises and improving relief efforts are not the only purposes here; managing crossings, and ensuring that displaced individuals receive the protection, care, and assistance they need promptly are also a priority.

Another example is the Primes system - Population Registration and Identity Management Ecosystem, developed by UNHCR. This tool is crucial for border and displacement management as it streamlines the registration and management of refugees and asylum seekers at borders.[82] It also provides vulnerable populations with basic assistance and protection. Early identification

[76] Emergency Situation Awareness website, available at: https://esa.csiro.au/aus/about-public.html.
[77] Artificial Intelligence for Disaster Response website, available at: http://aidr.qcri.org/.
[78] International Maritime Rescue Federation (IMRF), Report of the GMSF Web Meeting on the Subject of Remotely Operated and Autonomous Vessel and SAR Impacts, Global Maritime SAR Forum (GMSF), May 2024, available at: https://www.international-maritime-rescue.org/assurance-of-autonomy.
[79] McGregor, L., & Molnar, P., *Digital Border Governance: A Human Rights Based Approach*, University of Essex and the Office of the United Nations High Commissioner for Human Rights (OHCHR), Funded by the Federal Department of Foreign Affairs of Switzerland, 2023.
[80] Kingham, T., Travizory installed the world's first health biometric corridor in Seychelles, Border Security Report, 2022. Available at: https://www.border-security-report.com/travizory-installed-the-worlds-first-health-biometric-corridor-in-seychelles/
[81] ICRC, "Rewards and Risks in Humanitarian AI: An Example", Inspired: Innovation to Save Lives and Defend Dignity, 2019, available at: https://blogs.icrc.org/inspired/2019/09/06/humanitarian-artificialintelligence/.
[82] United Nations High Commissioner for Refugees (UNHCR), *Registration and Identity Management*. Retrieved from https://www.unhcr.org/what-we-do/protect-human-rights/protection/registration-and-identity-management.

allows for the recognition of individuals with specific needs and their referral to appropriate protection services.[83] Being registered can, for instance, offer protection against *refoulement* (forced return), arbitrary arrest, and detention, while also assisting in keeping families together and reuniting separated children with their families.[84]

2.1.6. Human Rights and Protection of Vulnerable Populations

Upholding human rights is the overarching principle guiding a rights-based IBDRM framework. In light of this canon, AI-driven initiatives like the Humanitarian OpenStreetMap, piloted by HOT exemplify how AI can be harnessed not only to support humanitarian actors but also to empower affected communities.[85] By providing access to vital information through an open-access map and using crowdsourced data, it identifies zones in critical need of aid and gives a voice to affected communities.[86] Additionally, AI tools for biometric data encryption ensure the privacy and security of personal information;[87] giving affected individuals and vulnerable populations agency over their data and protection from potential misuse. Furthermore, GeoMatch, an AI-powered tool designed to connect vulnerable populations with communities where they are most likely to thrive, could be an essential tool in both BM and DRM settings.[88] In the former, GeoMatch might enhance fair and effective resettlement by considering individual needs, skills, and community capacities, thus reducing discrimination and maximizing successful integration. In the latter, it could facilitate the relocation of displaced persons to safer areas with better access to services and support, ensuring that the most vulnerable are placed in environments that promote their safety, dignity, and well-being.

2.2. Challenges in AI deployment for Rights-Based IBDRM

"Everything depends on our manipulating technology in the proper manner as a means […] The will to mastery becomes all the more urgent the more technology threatens to slip from human control. But suppose now that technology were no mere means, how would it stand with the will to master it?"[89] AI's double-edged nature in the context of right-based IBDRM makes it a powerful tool that if not carefully managed could magnify existing inequalities and biases.

[83] Ibid.
[84] Ibid.
[85] Humanitarian OpenStreetMap website, available at: www.hotosm.org.
[86] Madianou, M., Longboan, L., and Corpus Ong J., "Finding a Voice through Humanitarian Technologies? Communication Technologies and Participation in Disaster Recovery", *International Journal of Communication*, Vol. 9, 2015.
[87] Zahoor, M. S., Fawad, A., Jayasundar, J., Nair, R., et al, "Biometric Encryption: Integrating Artificial Intelligence for Robust Authentication," *Journal of Digital Security*, 35(3): 25-33, 2023, DOI: 10.52783/dxjb.v35.121.
[88] Global Compact on Refugees, "GeoMatch: Connecting People to Places Using Artificial Intelligence", Available at: https://globalcompactrefugees.org/good-practices/geomatch-connecting-people-places-using-artificial-int.
[89] Heidegger, M. "The Question Concerning Technology." In The Question Concerning Technology: And Other Essays (W. Lovitt, Trans.), pp. 3–35, 1977.

To mitigate the risks of AI deployment, there is first a need to understand them.

An extensive body of critical literature has already endeavored to examine the human rights risks posed by AI technologies notably in border management and concluded that deeper systemic issues often prevail within the said usage. Listed issues ranged from automation to opacity to data-driven profiling.[90] This raises important questions about power asymmetries and accountability, and whether the latter is even possible.[91]

While this article focuses on a rights-based framework for practical deployment of AI in IBDRM settings, future academic expansions ought to more fully engage with these critical perspectives to ensure that proposed safeguards do not overlook deeper systemic issues.

2.2.1. Trustworthy Data, Algorithm Bias, and Arbitrary/Biased Profiling

Trustworthy data is central for AI systems in rights-based IBDRM. The quality of data used to train AI algorithms directly influences the accuracy and fairness of their outcomes.[92] When data is incomplete, outdated, or biased, it can lead to significant errors: whether in decision-making or predictive analysis. In IBDRM, the stakes are even higher, as vulnerable populations are at the center of concerns.

Even with the misguided assumption that data is always trustworthy; It is essential to remember that in conflict zones, remote or low-connectivity zones where internet access might be limited, obtaining accurate and real-time data is often difficult if not impossible. The shortage of reliable data could entail outdated or incomplete information resulting in erroneous outcomes. AI models used for decision-making during COVID-19, were often derailed by the scarcity of high-quality, timely data, since most historical data was not on Covid specifically, and were often influenced by the overwhelming flood of disinformation.[93]

Another example of a hazardous AI-driven tool is predictive policing algorithms at borders which often rely on historical cross-border crime data, to forecast or identify future threats and crimes and assess recidivism risks.[94] Now supposing the data used to train AI algorithms contained

[90] See Leese, M., 'The new profiling: Algorithms, black boxes, and the failure of anti-discrimination safeguards in the European Union', Security Dialogue, 47(5), pp. 368–382, 2016; Molnar, P. and Gill, L., Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System, Toronto: Citizen Lab and International Human Rights Program, University of Toronto, 2018. Available at: https://citizenlab.ca/2018/09/bots-at-the-gate.
[91] Aliferis, C. and Simon, G, 'Overfitting, Underfitting and General Model Overconfidence and Under-Performance: Pitfalls and Best Practices in Machine Learning and AI', ResearchGate, 2024, Available at: https://www.researchgate.net/publication/378731621_Overfitting_Underfitting_and_General_Model_Overconfidence_and_Under-Performance_Pitfalls_and_Best_Practices_in_Machine_Learning_and_AI and Guild, E., Brouwer, E., Groenendijk, K. and Carrera, S. The Use of Artificial Intelligence in Migration Management and the Impact on the Right to Privacy and Data Protection. Brussels: European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs. 2021. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2021)696968.
[92] Redman, T., "If Your Data Is Bad, Your Machine Learning Tools Are Useless", Harvard Business Review, 2 April 2018, available at: https://hbr.org/2018/04/if-your-data-is-bad-your-machine-learningtools-are-useless.
[93] Wynants L., et al., "Prediction Models for Diagnosis and Prognosis of Covid-19: Systematic Review and Critical Appraisal", BMJ, Vol. 369, 2020.
[94] European Union Agency for Fundamental Rights (FRA). "Artificial Intelligence Supporting Cross-border Cooperation in Criminal Justice." 2023.

prejudice, including for instance police records that could have racial bias,[95] the outcome may then perpetuate existing inequalities and lead to disproportionate surveillance going forward to even exacerbate the arbitrary profiling of certain communities.

"The scale and the power generated by AI technology accentuates the asymmetry between individuals, groups, and nations, including the so-called digital divide within and between nations".[96]

Bias in AI systems goes beyond technical errors. AI systems often mirror societal prejudices and stereotypes embedded in their design and development. When unaddressed, these biases can reinforce discrimination and exacerbate inequalities, violating human rights principles.[97]

In DRM settings, AI-driven facial recognition might frequently misidentify individuals with darker skin tones due to non-diverse training datasets.[98] This could lead to potentially denying them access to critical humanitarian aid. Other scenarios include disproportionately depicting children of color as child soldiers based on the unfair number of online pictures that tend to show children of color with weapons:[99] This kind of biased or arbitrary profiling can perpetuate erroneous or prejudiced narratives and influence humanitarian response in a way that marginalizes vulnerable groups even further. These harmful sequences, if unchecked, can turn into an unrelenting reaction loop due to AI automation.

2.2.2. Data Privacy, Cybersecurity and Surveillance Humanitarianism

Intended for the Greek islands of Lesvos, Samos, Leros, and Kos, the Centaur system was initially aimed at enhancing security within revamped refugee camps labeled closed controlled centers.[100] This AI-driven automated surveillance system includes the use of drones, alarms, cameras along camp perimeters, control gates equipped with metal detectors, and x-ray machines; all relying on motion analysis and AI behavioral analytics to detect incidents.

Emblematic of a broader trend in the use of AI in BM, Centaur is seen as mirroring EUROSUR's trajectory;[101] originally warranted as a tool to save lives at sea, EUROSUR has since evolved into a system primarily focused on combatting illegal migration and cross-border crime, echoing the

[95] Dominik Güss, C., Tuason T., and Devine A., "Problems with Police Reports as Data Sources: A Researchers' Perspective", Frontiers in Psychology, Vol. 11, 2020.
[96] UNESCO, Preliminary Study on the Ethics of Artificial Intelligence, 26 February 2019, para. 22.
[97] Universal Declaration of Human Rights (UDHR), 10 December 1948, Arts 2, 7; International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, Art. 26; European Convention on Human Rights (ECHR), 4 November 1950, Art. 14; American Convention on Human Rights (ACHR), 22 November 1969, Art. 1; African Charter on Human and Peoples' Rights, 27 June 1981, Art. 2.
[98] Joy Buolamwini and Timmit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Proceedings of Machine Learning Research: Conference on Fairness, Accountabilityand Transparency, Vol. 81, 2018.
[99] **Beduschi (n 15).**
[100] Kilpatrick, J., and Jones, C. "A Clear and Present Danger: Missing Safeguards on Migration and Asylum in the EU's AI Act." Statewatch, May 2022. Available at: https://www.statewatch.org/publications/
[101] Ibid.

growing prevalence of security over rights in BM.[102] Comparably, the Centaur project underscores the risk of creating an environment where individuals are continuously observed, their behavior analyzed, and their data collected without their explicit consent. These settings often prioritize security objectives over fundamental human rights and lead to an over-reliance on AI for monitoring. This can erode privacy rights and normalize constant surveillance, dubbed *surveillance humanitarianism*, especially in vulnerable communities.[103] Furthermore, AI-driven surveillance tools collect vast amounts of data, like biometric information for example, or behavioral patterns, locations, or political affiliations, that, if mishandled could expose individuals to significant risks. Even basic information, such as names and addresses could sometimes jeopardize the safety and dignity of vulnerable individuals, and lead to the de-anonymization of cases.[104]

Moreover, the power imbalance between aid providers and recipients heightens concerns around data privacy and informed consent. In such asymmetrical contexts, withholding consent may effectively mean forfeiting access to essential services.[105] And even if the consent is given without overt coercion, the question remains: is it even real? Is it truly informed and voluntary? Vulnerable individuals may lack the support to fully understand what they're consenting to, let alone exercise genuine choice. This challenge is often compounded by linguistic barriers, tedious bureaucratic procedures and inherent power asymmetries.

In both BM and DRM contexts, the over-collection and storage of sensitive data heighten cybersecurity risks, including data breaches or misuse by state and non-state actors. Furthermore, the over-reliance on these systems often increases the vulnerability of those in need of assistance.

2.2.3. Lack of Transparency, Accountability, and Oversight: The Black Box Problem

The biggest challenge for transparency and accountability in AI deployment is the fact that designers, deployers, and users are often operating in different silos within the same ecosystem: each having distinct objectives, priorities, and sway across different stages of the AI lifecycle.

Codes of ethics are often drafted from an end-user perspective or by third-party organizations, while the actual design and control of AI-powered systems remains in the hands of tech companies.[106] Even if efforts to create ethical frameworks for systems design and development are underway: there is no universally agreed-upon framework. And if such a consensus exists, it is not binding which makes it hard to ensure compliance and oversight.

[102] Ibid.
[103] Pierrick Devidal, "Cashless Cash: Financial Inclusion or Surveillance Humanitarianism?", Humanitarian Law and Policy Blog, 2 March 2021.
[104] Latonero, M., "Stop Surveillance Humanitarianism", New York Times, 11 July 2019

[The] Engine Room and Oxfam, Biometrics in the Humanitarian Sector, March 2018.
[105] Madianou M., "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises", Social Media & Society, Vol. 5, No. 3, 2019.
[106] Pizzi (N 45).

Furthermore, these guidelines often mirror the values of those who draft them without necessarily reflecting the viewpoints of those impacted by AI use or those who create AI systems.

Compounding on this issue is the alleged opacity of AI-systems. Unlike traditional algorithms, many AI-systems are often too complex to trace or audit, making it difficult to explain these decisions to the public or to entities responsible for oversight and monitoring.[107] It is not possible to dissect AI systems and understand how decisions are made: as exemplified by the so-called *Black Box* problem. AI systems are said to be obscure for those impacted by their use and for decision-makers.[108] One can recognize the input; and grasp the output but not the causal link nor the process that led to that.[109] Is it then possible to have effective transparency and accountability when the process and its stages are precluded from the assessment?

Even if the assumption, *that the system is understandable without any technical knowledge*, stands, there is a doubt as to whether people would manage to recognize if and why their rights are violated and how they could accordingly seek redress.[110]

This opacity is even stronger in BM and DRM frameworks where individuals are often unaware of where and when AI systems are used for decision-making and how these can affect the enjoyment of their rights. There is often a lack of awareness regarding the "scope, extent, or even existence" of algorithmic processes influencing human rights as explained by David Kaye, former UN special rapporteur on the promotion and protection of freedom of opinion and expression.[111]

Many AI systems suffer from issues like data noise, overfitting (models are excessively tailored to training data and fail to generalize to new contexts) or underfitting (models are too simplistic to capture the complexity of new dynamics): which further complicates explainability and increases the risk of skewed feedback loops in decision-making systems.[112]

Additionally, the structural complexity of AI deployment in humanitarian crises often involves a long sequence of actors which creates challenges in determining who is responsible when an erroneous or discriminatory decision is made.[113] Questions of which party is accountable and how, often remain unresolved, which makes oversight a daunting task.

[107] Buiten, M., "Towards Intelligent Regulation of Artificial Intelligence", European Journal of Risk Regulation, Vol. 10, No. 1, 2019.
[108] Rudin, C. and Radin, J., "Why Are We Using Black Box Models in AI When We Don't Need To?", Harvard Data Science Review, Vol. 1, No. 2, 2019, available at: https://doi.org/10.1162/99608f92. 5a8a3a3d.
[109] Bathaee, Y., "The Artificial Intelligence Black Box and the Failure of Intent and Causation", Harvard Journal of Law and Technology, Vol. 31, No. 2, 2018.
[110] McGregor, L., Murray, D., and Ng, V., "International Human Rights Law as a Framework for Algorithmic Accountability", International and Comparative Law Quarterly, Vol. 68, No. 2, 2019, available at: https://tinyurl.com/yaflu6ku.
[111] David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/73/348, 29 August 2018, para. 40.
[112] Aliferis, C. and Simon, G., 'Overfitting, Underfitting and General Model Overconfidence and Under-Performance: Pitfalls and Best Practices in Machine Learning and AI', ResearchGate, 2024 Available at: https://www.researchgate.net/publication/378731621_Overfitting_Underfitting_and_General_Model_Overconfidence_and_Under-Performance_Pitfalls_and_Best_Practices_in_Machine_Learning_and_AI
[113] Andersen, L., "Artificial Intelligence in International Development: Avoiding Ethical Pitfalls", Journal of Public and International Affairs, 2019, available at: https://jpia.princeton.edu/news/artificialintelligence-international-development-avoiding-ethical-pitfalls.

2.2.4. Justiciability and the Limits of Redress

"The development and use of AI-driven migration technologies cannot operate in the shadows away from public scrutiny but must be fully integrated into a system of accountability."[114] The right and practical ability to appeal or reverse decisions made by opaque data-driven systems, referred to as justiciability, is an omnipresent challenge that arises even among AI systems which are designed considering operational transparency and ethical safeguards.[115] This issue becomes especially critical when decisions affect access to aid or cross-border movement, which must remain subject to legal review. Yet the inherent opacity of machine learning, often exacerbated by proprietary systems or non-intuitive reasoning processes, severely undermines justiciability. Some data engineers question whether AI decisions can, in fact, be meaningfully traced or justified, particularly in systems governed by complex neural networks where decision logic is neither transparent nor intuitive.[116] This problem is compounded when systems are developed by private actors invoking trade secrecy or intellectual property protections, making access to datasets legally inaccessible.[117] As a result, individuals subjected to such systems are often left without a clear pathway to challenge decisions or seek redress. Against this backdrop, justiciability must be addressed as a structural concern, not a technical afterthought: a foundational legal requirement embedded at every stage, from system design to deployment and oversight. Failure to do so risks institutionalizing a form of digital opacity that places automated decisions beyond the reach of legal scrutiny.[118]

2.2.5. Resistance to AI Technologies

"Life and death decisions should not be delegated to machines".[119] The previous statement mirrors the core of resistance to AI technologies in humanitarian settings and more so in BM and DRM.

Techno-solutionism has often been met with serious criticism and doubt and the idea that technology can solve every problem hasn't always been seen in the best of light. In fact, some see the reliance on AI as a diversion from more fundamental needs, such as investing in robust public health infrastructure. This was a critical takeaway from the Ebola outbreaks in West Africa, where stakeholders believed better public health systems would be more effective than relying on AI-driven early warning systems.[120]

Additionally, stakeholders may often resist adopting AI due to ethical concerns and mistrust of

[114] Stewart, L.S., *The regulation of AI-based migration technologies under the EU AI Act: (Still) operating in the shadows? European Law Journal*, 30(1–2), pp.122–135, 2024. https://doi.org/10.1111/eulj.12516.
[115] Ibid.
[116] Chesterman, S., *Through a Glass, Darkly: Artificial Intelligence and the Problem of Opacity*, NUS Law Working Paper No. 2020/011, Forthcoming in *American Journal of Comparative Law*, 2020, Available at: https://ssrn.com/abstract=3572588.
[117] Ibid.
[118] Wang, Y. 'Data Privacy, Human Rights, and Algorithmic Opacity', *California Law Review*, 112(3), pp. 887-934, 2024. Available at: https://www.californialawreview.org/print/data-privacy-human-rights-and-algorithmic-opacity.
[119] United Nations General Assembly (n 43)
[120] Wamsley, D., and Chin-Yee, B., "COVID-19, Digital Health Technology and the Politics of the Unprecedented", Big Data & Society, Vol. 8, No. 1, 2021, p. 3.

automated systems.[121] Fears about data privacy, algorithmic bias, and the lack of transparency, as cited in the segments above, exacerbate this resistance. Even if the motive for resistance is eliminated, the lack of training and capacity building is frequently a significant barrier to AI adoption. Many may not have the technical expertise required to deploy, manage, and justify AI usage in humanitarian crises. This knowledge gap may lead to a lack of confidence in AI systems and a preference for more traditional methods.[122] Without adequate support, training, and capacity building, resistance to AI will likely persist. Ultimately, cultural and contextual factors can also play a role in deciding whether AI usage is seen as favorable or not by affected local communities and aid deliverers.

2.2.6. Context-Blind AI Systems

The disconnect between the design and application stages of AI projects is often disregarded. Yet, this failure to acknowledge and adapt to the particular environments where AI is deployed is often detrimental in humanitarian settings. Given that most AI tools are business-oriented or designed with developed-world contexts in mind, the latter might not convert effectively to the delicate and complex reality of humanitarian aid.[123] An AI system conceived in a European research hub might not consider the unique socio-political dynamics of a conflict zone in the Middle East. Developers may not realize that certain marginalized groups might for instance be underrepresented or even invisible in typical data sets: leading to biased and erroneous outcomes. Internally displaced persons are often excluded from official datasets, reinforcing existing biases and harming stigmatized groups even further.[124]

Furthermore, inadequate expertise and training among those deploying AI tools in humanitarian settings can exacerbate their mishandling. Whether a lack of understanding of AI outcomes or an over-reliance on automated decisions: it's crucial to understand that limited technical capacity can have harmful consequences.[125]

An AI-driven tool that uses crowdsourced data for disaster mapping might not produce the expected results in situations of armed conflict and vice versa. When AI systems are not adapted to local realities, they risk failing and spreading more harm than good. AI is often portrayed as a universal solution. But in reality, AI systems are highly specialized (datasets, goals) and context-dependent.

[121] Yang, Y., Ngai, E. W. T., and Wang, L. "Resistance to Artificial Intelligence in Health Care: Literature Review, Conceptual Framework, and Research Agenda." *Information & Management*, 61(4), 103961, 2024.
[122] Ibid.
[123] Chui M., et al., Notes from the AI Frontier: Modeling the Impact of AI on the World Economy, McKinsey Global Institute, September 2018.
[124] Baal, N., and Ronkainen, L., Obtaining Representative Data on IDPs: Challenges and Recommendations, UNHCR Statistics Technical Series No. 2017/1, 2017.
[125] Ibid.

3. AI SAFEGUARDS FOR RIGHTS-BASED IBDRM

Without proper safeguards, AI deployment may lead to decisions that have the power to affect the enjoyment of human rights,[126], particularly for vulnerable populations in humanitarian crises. As AI-driven tools become an everyday occurrence in IBDRM settings, it is imperative to ensure that design, usage, and oversight principles are aligned with human rights principles.

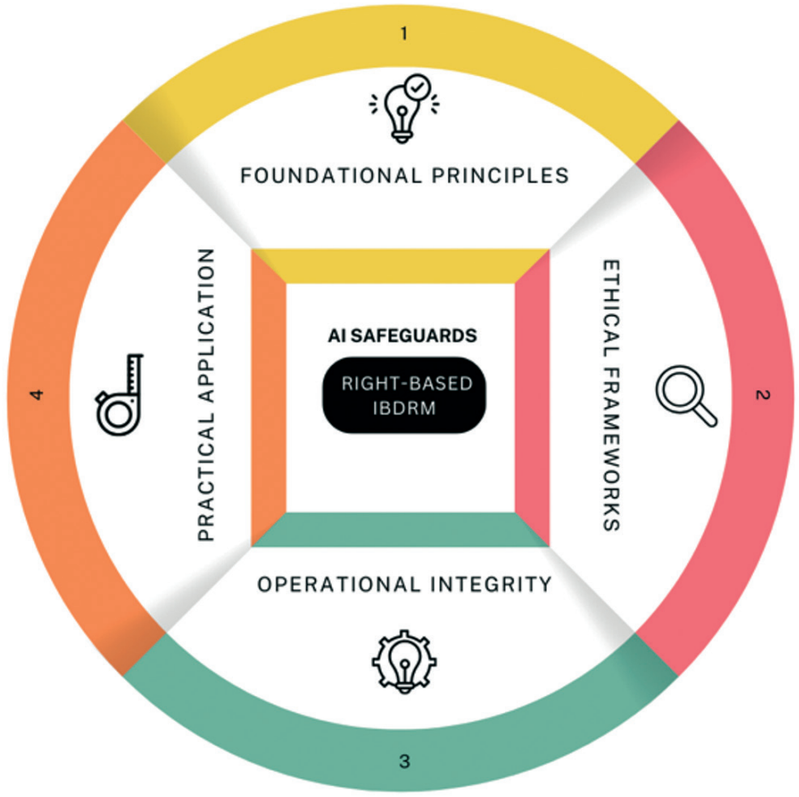

Figure 4: AI Safeguards for Rights-Based IBDRM.

Source: Designed by the Authors.

Figure 4, labeled "AI Safeguards for Rights-Based IBDRM", visually represents a cycle for deploying AI safeguards in line with rights-based principles. At the core lies the *foundational principles*, such as privacy by design which embeds rights-based imperatives at the onset. Moving forward, the *ethical framework*, advocates for the "Do No Harm" approach, and includes codes of conduct for AI deployment within and at borders. The third layer dubbed *Operational integrity*, underscores

[126] UNGA Res. 73/179, 2018.

the importance of transparency, accountability, and redress mechanisms. Finally, *practical application* promotes tailored approaches to AI deployment and underlines that AI should never be a one-size-fits-all solution. This cycle represents an ongoing process that should continuously adapt to ensure a rights-based and responsible use of AI in IBDRM scenarios. Its iterative nature ensures that AI systems are continuously refined and improved, addressing new challenges while reinforcing the safeguarding of human rights. Each stage impacts the next, creating a feedback loop where, for example, improved operational integrity strengthens foundational principles through open reporting, ethical frameworks shape practical applications through codes of ethics, and stakeholders' attitudes evolve to promote a more effective and rights-centered approach over time.

3.1. Foundational Principles

Ethical considerations should not be an afterthought but rather a core component at all stages in the AI life cycle starting from the design to the development, deployment, and oversight. By embedding privacy, inclusivity, and human rights considerations from the outset, AI systems can better align with human rights principles and better protect vulnerable populations.

3.1.1. Privacy and Inclusivity by Design

In humanitarian settings protecting vulnerable individuals and affected communities also entails protecting their personal data, yet privacy is often overlooked by those who design and develop AI systems. Against this backdrop, privacy by design principles could be the bedrock of privacy-conscious AI processes. The idea is to build better data privacy protection through proactive and preventive user-centric principles upon the design and development of AI systems.[127] This could mean, among other practices: minimizing data collection, securing storage, and eventual deletion of data (the right to be forgotten) when no longer required.[128] Humanitarian organizations should ensure that AI systems whether developed in-house or by third parties, embed data protection by design and by default. The system hence should inherently obtain consent for processing personal information or rely on legal obligations to do so. Data collection should be limited to what is strictly necessary and be stored in optimal security.[129] It should be used just for the purpose for which it was originally collected and then securely deleted or anonymized after its intended use.

Inclusivity by design is crucial to ensure that AI systems are equitable and non-discriminatory. AI systems should thus be developed with a diverse range of perspectives and needs in mind,

[127] Resolution on Privacy by Design", 32nd International Conference of Data Protection and Privacy Commissioners, 27–29 October 2010.
[128] Bygrave, L., "Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements", Oslo Law Review, Vol. 4, No. 2, 2017.
[129] Kuner, C., and Marelli, M., Handbook on Data Protection in Humanitarian Action, 2nd ed., ICRC, Geneva, 2020, p. 39; OCHA, above note 15, p. 10; ICRC, The Engine Room and Block Party, above note 52, p. 32

incorporating input from various communities, including those most likely to be affected by the deployment of this tool.[130] This would entail including a broad spectrum of stakeholders throughout the design and development phase and ensuring that datasets used to train AI systems are representative of its target audience. If training data for AI systems don't reflect the diversity of the population, they aim to serve: the risk of reinforcing existing biases or creating new ones is unavoidable.

3.1.2. Human Rights and Data Protection Impact Assessments

Risk analysis and Impact assessments are valuable instruments to mitigate AI risks and protect affected populations from unwanted harm. Not only do they identify potential risks, but they also underscore potential solutions for risk mitigation. As such, if the costs of deployment might include serious breaches of data privacy and/or violations of human rights, the organization might deem that this specific tool should not be deployed in this specific context.[131] A data protection impact assessment (DPIA) can for instance be used to identify situations in which datasets used to train AI systems might be retrieved, thereby exposing sensitive information or leading to the re-identification of anonymized data.[132]

Moreover, human rights impact assessments (HRIAs) help organizations identify potential adverse impacts on human rights that can stem from AI deployment. The objective is to see whether an AI tool aligns with human rights principles and whether it might directly cause or contribute to potential violations of human rights.[133] This helps in deciding whether the tool should be used, how, where, and when to deploy it, and the severity of potential outcomes. Other tools such as Global Pulse's Risks, Harms, and Benefits Assessment combine elements of both DPIAs and HRIAs.[134]

Unlike regulatory frameworks which might be more rigid, these tools: (1) are often in line with technological change,[135] (2) recognize that contextual elements are key when assessing adverse risks to human rights, and (3) can be tailored for case-specific assessments.[136]

[130] Pizzi **(n 45).**
[131] Bedusci (n 15).
[132] Ibis.
[133] Cath, C., Latonero, M., Marda, V., and Pakzad, R., "Leap of FATE: Human Rights as a Complementary Framework for AI Policy and Practice".
[134] UN Global Pulse, "Risks Harms and Benefits Assessment", available at: www.unglobalpulse.org/policy/ risk-assessment/.
[135] Microsoft's human rights impact assessment (HRIA) and Google's Celebrity Recognition HRIA.
[136] Element AI, Supporting Rights-Respecting AI, 2019; Telefonica, "Our Commitments: Human Rights," available at: www.telefonica.com/en/web/responsible-business/ human-rights.

3.2. Ethical Frameworks

The global approach to AI must be in full alignment with human rights.[137] This alignment makes sure that AI tools and technologies do not perpetuate harm or injustice but instead serve as tools for promoting human rights and protecting vulnerable populations.

3.2.1. Do No Harm Principle

As collaborations between tech companies and humanitarian organizations become more common, there is the constant risk that AI systems will reflect the priorities of those who designed them: potentially overlooking the perspective and needs of vulnerable populations. The principle of "Do No Harm" has thus been introduced to emphasize careful consideration of potential impacts when deploying any kind of technology.[138] The aim is to ensure that the said technology, in this case AI, does not inadvertently cause harm and exacerbate existing vulnerabilities or create new ones. Impact Assessments, which were explained in the previous segment, are often one way to make sure the AI system in question won't cause harm to affected populations.

Before adopting such a system, humanitarian actors should evaluate whether there is a need to deploy it, whether there is an added value, and if they can do so in a manner that protects vulnerable populations from additional harm. This principle is also a guiding compass for codes of conduct, which should ensure that AI deployment doesn't compromise the security and dignity of those they aim to aid.

3.2.2. Code of Conduct for AI Deployment within and at Borders

While there is a consensus that International Human Rights Law (IHRL) should be the basis of any AI governance, providing a universal binding comprehensive framework for mitigating AI risks for both states and businesses;[139] in a world where technology is constantly evolving, ethical guidelines offer a welcomed complementary approach. These guidelines add a layer of adaptability, responsiveness, and flexibility that traditional frameworks may lack. Additionally, ethical principles are often perceived as addressing the broader impacts of AI systems and raising standards beyond mere legal compliance. Whether the chicken comes before the egg or the egg before the chicken is ultimately beside the point; human rights and ethics must thus work in synergy to guide responsible AI conduct.[140]

Codes of conduct should subsequently reinforce the foundational principles set by human rights while providing practical directives to those who should abide by them and promote responsive

[137] United Nations General Assembly (n 43)
[138] ICRC, "ICRC Protection Policy", International Review of the Red Cross, Vol. 90, No. 871, 2008, p. 753.
139 McGregor (n 89).
[140] Business for Social Responsibility (BSR) and World Economic Forum (WEF), Responsible Use of Technology, August 2019, p. 7.

practices that correspond to the evolving needs on the ground. For example, the code of conduct for AI deployment within and at borders in humanitarian settings would specify that AI systems used for border control, such as facial recognition, must adhere to the "Do No Harm" principle, ensuring that they do not perpetuate discrimination or violate privacy rights. The code of conduct would also go further to mandate how this should be done. The idea is to offer concrete and actionable directives to ensure compliance.[141] Such a code would require, among other imperatives, transparency in how AI tools are used and clear procedures to avoid discriminatory outcomes or privacy violations. It could include, for instance, provisions that humanitarian actors must promptly inform affected communities about any data security breaches that may compromise personal information and clearly communicate measures taken to rectify the situation.[142] These codes of conduct not only establish a framework for rights-based AI use but also build trust between humanitarian actors and affected communities through the promotion of human rights and the protection of vulnerable populations.

3.3. Operational Transparency

Clear visibility into how AI systems function, make decisions, and impact individuals and communities in humanitarian settings is critical for rights-based IBDRM. Operational transparency of AI systems should hence encompass the in-house explainability and transparency of the system itself, but also external oversight and accountability processes such as audit and redress mechanisms.

3.3.1. Transparency and Explainability

Adopting a code of ethics is just the starting point; it does not guarantee that IBDRM actors will prioritize human rights in deploying AI tools. To have an impact, these principles need to be operationalized through robust management and oversight structures.[143] Commitments to human rights must translate into concrete tools and procedures at every stage of the AI life cycle, in part through explainability and transparency procedures.

Transparency and explainability are prerequisites for accountability in AI systems, yet achieving full, transparency is often a challenging task. Explainability refers to the ability to describe in understandable terms how AI systems make specific decisions or predictions: in that sense transparency is an even broader concept.[144] Automated AI algorithms can, for example, rank data based on patterns it identifies itself without any way to fully understand how it does what it does. The opacity of these systems makes it harder to ensure transparency: one that includes

[141] European Commission, Ethics Guidelines for Trustworthy AI, 8 April 2019, available at: https://ec.europa.eu/digital-singlemarket/en/news/ethics-guidelines-trustworthy-ai.
[142] ICRC, "Cyber Security Incident: How Could It Affect Me?", 7 February 2022, available at: www.icrc.org/ en/document/cyber-security-how-it-affect-me.
[143] Pizzi **(n 45).**
[144] Larsson, S., and Heintz, F., "Transparency in Artificial Intelligence", Internet Policy Review, Vol. 9, No. 2, 2020.

clarity about the models, algorithms, and data sets, but also precision on the purpose, funding, commissioning, decisions, and applications of AI systems.[145] Both are critical in humanitarian contexts: explainability allows stakeholders to understand and scrutinize the basis for an AI-driven decision, while transparency ensures that all aspects of AI deployment (such as objectives and funding) are communicated and available for external review.

The proprietary nature of AI systems makes the above-mentioned tasks even harder. Technical details are often kept confidential, and organizations are often reluctant to report or share information about potential failures or harms. *Data-sharing agreements* that encourage the documentation and dissemination of AI-related risks and incidents are thus useful to promote transparency.

3.3.2. Standards, Audits, Accountability, and Redress

At its core, accountability entails: (1) an obligation to explain and justify conduct, (2) assessing whether an action or omission was justified, and (3) whether the individual or entity is responsible for any negative consequences.[146] Accountability can take different forms, including but not limited to technical audits to verify an AI system's compliance with human rights standards, social accountability which, entails engaging the public, and legal accountability which, holds parties accountable for negative outcomes.[147]

BM and DRM actors must, for example, always transparently notify beneficiaries of any incidents, explain their actions, and introduce a model for effective accountability and remedy. Additionally, individuals should have the right to challenge any decisions, automated or otherwise, that adversely impact their rights.[148] Robust grievance mechanisms are thus imperative, including judicial and non-judicial mechanisms (administrative complaints, alternative dispute resolution, and internal remedy mechanisms) to provide accessible and effective avenues for remedy.[149] Moreover, whistle-blowing mechanisms are also critical in that aspect to expose abuses.[150]

Finally, oversight mechanisms and independent oversight bodies, whether at national, international, or industry levels, are necessary for monitoring and certifying AI tools. Kitemarks, benchmarks and third-party certifications for AI systems could demonstrate compliance with rights-based principles, while regular audits (internal or external) are also necessary to monitor compliance and adherence to global standards.[151]

International standards are also complementing these mechanisms and playing an increasingly central role in shaping responsible AI deployment. Bodies such as the International Organization

[145] McGregor (n 89).
[146] Bovens, M., "Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism", West European Politics, Vol. 33, No. 5, 2010, p. 951.
[147] UN Human Rights, UN Human Rights Business and Human Rights in Technology Project (B-Tech): Overview and Scope, November 2019.
[148] Rubin, E., "The Myth of Accountability and the Anti-aDRMinistrative Impulse", Michigan Law Review, Vol. 103, No. 8, 2005.
[149] Beduschi (n 15).
[150] Pizzi **(n 45).**
[151] Kirchner, F., Metzinger, T., Ferretti, L., Brauneis, R., Wischmeyer, T., and Paganini, P., *A Catalog of General Ethical Requirements for AI Certification: Normative Foundations and Practical Implementation*, arXiv preprint, Aug. 2024. Available at: https://arxiv.org/abs/2408.12289

for Standardization (ISO) and the European Committees for Standardization and Electrotechnical Standardization (CEN-CENELEC) have, for instance, developed technical frameworks on AI Trustworthiness and Risk Management, which offer a harmonized approach to operationalizing rights-based principles across sectors.[152] For BM and DRM actors in particular, such standards can help close the gap between legal obligations and technical implementation. Whether these standards are integrated into procurement and certification processes or adopted voluntarily: they could serve as powerful accountability tools, notably in jurisdictions that suffer from a lack of binding regulations, or those where the latter is still evolving. Adherence to harmonized standards under the AI Act, for example, confers an automatic presumption of conformity with legal requirements.[153]

3.4. Practical Application

AI systems are not a one-size-fits-all solution, especially when it comes to rights-based IBDRM. Each humanitarian context brings its own legal, logistical, and cultural constraints; requiring a tailored approach that addresses specific needs and is sensitive to local dynamics. Empowering local communities and training IBDRM actors is also necessary for the successful deployment of AI in humanitarian settings.

3.4.1. Tailored Approach and Responsiveness

AI tools deployed in humanitarian settings must be carefully adapted to the unique environments in which they operate. The failure to consider cultural, social and, political realities can lead to biased and misleading outcomes, exacerbating existing inequalities and even creating new ones.[154] This adaptation goes beyond mere geographical considerations; it also involves understanding context-contingent vulnerabilities and safeguarding mechanisms that vary based on specific humanitarian scenarios or types of crises. The plug-and-play approach rarely works in real-world settings. Tools designed for flood response for instance may not be suitable to manage emergencies in conflict zones. AI systems designed for developed countries might fail to function well in developing countries and vice-versa.[155] To ensure effective deployment, humanitarian organizations should leverage regulatory frameworks as well as collaborative consortiums, and partnerships that enhance the understanding of diverse contexts and bolster AI's applicability. A holistic and inclusive approach is also essential, via needs-assessment processes, public consultations, accessible communication channels, and reporting mechanisms.[156]

[152] See ISO, *ISO/IEC TR 24028:2020 – Information technology – Artificial intelligence – Overview of trustworthiness in AI*, International Organization for Standardization, 2020; ISO, *ISO/IEC 23894:2023 – Artificial intelligence – Guidance on risk management*, International Organization for Standardization, 2023.
[153] European Commission, *Harmonized Standards for the European AI Act*, 2024. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC139430
[154] Ibis.
[155] Baal (n 97).
[156] Committee on the Elimination of Racial Discrimination, General Recommendation No. 36 on Preventing and Combating Racial Profiling by Law Enforcement Officials, UN Doc. CERD/C/GC/36, 17 December 2020, para. 66.

3.4.2. Empowerment and Capacity Building

Building capacity and fostering public engagement and knowledge-sharing are crucial steps to ensure that AI deployment is in compliance with human rights principles and AI codes of ethics.[157] Many organizations, especially in the public and NGO sectors, lack the resources and expertise necessary to effectively steer AI systems while adhering to human rights principles. Addressing these typical gaps often requires targeted capacity building for those deploying AI tools, those overseeing their use, human rights organizations, data protection authorities, and so on. By training a broad range of stakeholders from data scientists to policymakers: trust in AI systems is promoted and confidence in those who operate them is successfully fostered.[158] The technical know-how also helps actors understand and adapt AI systems to ensure that their deployment aligns with local needs and protects vulnerable populations. At a broader level, AI governance must be a collaborative effort. Knowledge-sharing platforms, model impact assessment tools, and benchmarking standards could be useful resources. At the national level, having dedicated governance bodies could be a way to ensure more responsible AI usage, as well as empowering local communities to make their voices heard through reporting, whistleblowing, and so forth.[159]

4. CONCLUSION: LEVERAGING AI FOR RIGHTS-BASED IBDRM IN HUMANITARIAN CRISES

Over the last 20 years, humanitarian needs have surged, with crises now lasting an average of over nine years.[160] These sobering realities underline an urgent need for more proactive and adaptive humanitarian strategies, recognizing that disasters are increasingly transnational, transcending borders and requiring coordinated, rights-based AI-driven responses.

4.1. A Holistic Framework: IBDRM for Effective Humanitarian Responses

In humanitarian crises, such as those arising from conflicts, natural disasters, or pandemics; borders and disaster zones often become critical points of an indispensable coordinated response. This paper emphasizes that management in these contexts should not be confined to traditional roles, like maintaining border security or solely responding to disasters. Instead, there should be a comprehensive approach that incorporates both Border Management and Disaster Risk Management strategies to ensure humanitarian support, safe passage, and the protection of human rights for people on the move: one *rights-based framework* through a *single-window* approach. The sponsored framework, labeled IBDRM, emphasizes the need for a coordinated approach across multiple jurisdictions. It advocates for cooperation that often goes beyond a single

[157] UN Data Strategy of 2020 strongly emphasizes the need for capacity-building among civil servants across the UN in the areas of data use and emerging technologies.
[158] Chui (n 96).
[159] Access Now, Human Rights in the Age of Artificial Intelligence, 2018.
[160] McGregor, L., (n. 68).

state, especially in regions where shared borders, regional needs, or the scope of disaster-prone zones, necessitate a collaborative response, synchronized early warning systems, harmonized humanitarian corridors for safe passage, and mutual assistance agreements that integrate both BM and DRM needs. While the idea of an Integrated BDRM framework may seem ambitious, the paper argues that such convergence is already happening in practice, especially in crises involving cross-border movements and regional disasters. The goal is not to merge these fields but rather to foster a sort of alignment and greater cooperation where objectives overlap, such as *in public safety, displacement management, and above all, the protection of human rights and vulnerable populations.*

4.2. The Primacy of Human Rights: Advocating Scalable and Rights-Based Approaches

“Human rights obligations are not optional. Human rights apply to every person”[161], and must be at the core of all actions, even those traditionally centered on security objectives. BM workers have, for instance, often viewed their responsibilities as purely security-driven, yet in practice, especially during humanitarian crises, they frequently are first responders at borders. As lines between security and humanitarian roles blur, human rights must remain a guiding principle at the heart of all IBDRM actions. Moreover, the paper does not see AI as a panacea but emphasizes the need for scalable, rights-based, and context-sensitive AI strategies. The IBDRM framework is inherently flexible and adaptable, recognizing that borders and disaster zones are complex areas shaped by local, national, and regional actors; with even broader concerns and transnational challenges when humanitarian crises involve multiple states. AI-driven technologies cannot, thence, be approached with a *plug-and-play* mentality; their deployment must be deeply informed by the unique challenges, contexts, and communities they are meant to serve:[162] *one size does not and cannot fit all.*

AI deployment must reflect local realities, such as limited technological infrastructure, differing levels of political will, and the presence of protracted humanitarian crises that span multiple borders.

4.3. High-Level International Coordination through Cohesive Regulatory Frameworks

The 2023 High-Level Meeting on Pandemic Preparedness marked a critical step in addressing

[161] United Nations Counter-Terrorism Implementation Task Force (CTITF), “Human Rights and Screening in Border Security and Management: Pocketbook for Field Screening,” 2018.
[162] Qiang, V., Rhim, J. and Moon, A., No such thing as one-size-fits-all in AI ethics frameworks: a comparative case study, AI & Soc 39, 1975–1994, 2024. https://doi.org/10.1007/s00146-023-01653-w.

global coordination gaps that became flagrant during the Covid-19 pandemic.[163] This flagship political declaration was the first of its kind and emphasized the need for robust international frameworks: not only for health emergencies but also and especially for all crises that transcend national boundaries. Among others, it advocated for (1) improved global coordination, (2) equitable access to resources, and more comprehensive mechanisms.

Ongoing efforts to codify a universal treaty further highlight the fragmented nature of the current international legal architecture, and the absence of a globally binding treaty leaves free reign to a patchwork of regional agreements and soft law instruments that lack coherence and fail to provide a unified approach to crisis response within, at and across borders.

This legal fragmentation is equally relevant in AI governance within IBDRM settings. The EU's AI regulatory landscape, for instance, characterized by its AI Act, General Data Protection Regulations (GDPR), and the Law Enforcement Directive (LED), sets stringent standards for rights protection but does not fully address the unique challenges and vulnerabilities of displaced populations. Much like a leaky umbrella, the existing legal framework provides partial coverage but leaves gaps in critical areas, especially for vulnerable populations in IBDRM scenarios.

High-level international coordination, supported by robust legal and operational frameworks for both IBDRM and AI, is critical to ensure that human rights remain central to all disaster and border management actions. In this context, international standards, such as those developed by ISO and CEN-CENELEC, offer a harmonized baseline for operationalizing human rights in AI systems across jurisdictions and help mitigate fragmentation and foster coherence in AI governance.[164]

Ultimately, AI can serve as a powerful tool for IBDRM if embedded within a right-based framework that transcends political and geographic boundaries. A fractured approach to crisis response weakens the collective ability to protect everyone, and above all, the most vulnerable.

[163] United Nations. Adopting Landmark Declaration, General Assembly Calls for Strengthening High-level International Coordination to Improve Pandemic Prevention, Preparedness, Response, 2023, UN Press.

[164] While these international standards focus, for example, on AI trustworthiness and risk management rather than explicit human rights obligations, they incorporate key principles, such as transparency, human oversight, and accountability, that align with rights-based governance. In this sense, they serve as foundational components of a rights-based approach to AI in IBDRM contexts.

TABLE OF FIGURES:

TABLE OF TABLES:

INTERSOS HUMANITARIAN AID

INTERSOS HUMANITARIAN CONGRESS - ROME, 11 OCTOBER 2024

Humanitarian Access: Changes and Challenges

Paper Proposal

DIGITAL OTHERING AND MIGRATION – ON THE USE OF BIOMETRICS IN EU POLICY AND MIGRATION

Federico Pierucci (PhD Candidate, Sant'Anna School of Advanced Studies)
Alexander Köhler (PhD Candidate, Sant'Anna School of Advanced Studies)

Paper Proposal

Title:

Digital Othering and Migration – On the use of Biometrics in EU policy and migration

Authors:
Federico Pierucci (PhD Candidate, Sant'Anna School of Advanced Studies)
Alexander Köhler (PhD Candidate, Sant'Anna School of Advanced Studies)

ABSTRACT

This paper explores how technological advancements have reshaped migration governance, focusing on the increasing role of digital and biometric technologies in managing migrants' identities. The process of datafication—where migrants' personal information is captured, stored, and used through digital systems—has led to significant shifts in how borders and migration are controlled. A key focus of the analysis is the divide between the digital rights afforded to EU citizens, who are protected by the privacy frameworks enshrined in the EU regulatory efforts on data protection and digital identity, and the extensive surveillance and data collection imposed on migrants. While EU citizens benefit from privacy protections that offer control over their digital identities, migrants are subject to intensified monitoring through biometric technologies and databases like EURODAC, which are specifically designed to track and manage their movement. This paper introduces the concept of "Digital Othering," highlighting how such technologies can perpetuate exclusion by positioning migrants as subjects of surveillance rather than individuals with rights. The paper concludes with policy recommendations to ensure that technological interventions in migration management respect privacy and human dignity, while also addressing security concerns.

1. INTRODUCTION

In an era where digital technologies increasingly mediate our interactions with the world, the concept of borders has expanded beyond physical frontiers to include complex sociotechnical practices that define and differentiate who belongs within a given space—both geographically and digitally. As the world becomes progressively more permeated by digital technologies, an unparalleled amount of data is generated. Through what is often referred to as the process of "datafication",[1] portions of the everyday life of individuals and communities are transformed into arrays of numerical representations. Transformed into data, those aspects of the physical, political, and social world can be stored in databases and processed through algorithms.

Borders do not represent an exception to this dynamic. Instead, they are one of the paramount examples of datafication in action. Scholars and humanitarian actors have long stressed the complexity of discussing the issue of borders from a multifaceted perspective. Far from being solely geographical boundaries that separate nation-states, borders can be considered discursive, material, and technological practices enacted by states to pursue political goals. Through concepts such as "bordering"[2] and "borderscapes"[3] migration studies have attempted to investigate borders transitioning away from fixed linear entities to show their dynamic and multidimensional nature. This shift challenges the conventional cartographic representation of borders as a geographical or administrative image, offering a more nuanced perspective on borders as a dynamic, multifaceted phenomenon.

Through the lenses of Science and Technology studies, migration studies have been enriched with the investigation of the impact of Information and Communication Technologies (ICT) on practices of state and non-state actors in border and migration management. The increasing integration of digital technologies into border management has fundamentally reshaped the concept of borders, extending them beyond their traditional physical and territorial boundaries into the digital realm. This shift is particularly evident in the European Union's approach to migration control, where digital databases and surveillance systems have become central to identifying, managing, and regulating the movement of migrants. It also has, to a significantly smaller degree, effects on the work of humanitarian organizations.

Scholars have critically examined the EU's development of digital infrastructures, such as the Schengen Information System (II), Eurodac, and the Visa Information System, which collectively function to monitor and control irregular migration within and across EU borders.[4] These digital systems are not merely tools for managing migration; they represent a significant extension of

[1] Ulises A. Mejias e Nick Couldry, «Datafication», *Internet Policy Review* 8, Vol. 4 (29 November 2019), https://doi.org/10.14763/2019.4.1428.
[2] Alexander C. Diener and Joshua Hagen, *Borders: a very short introduction* (New York: Oxford University Press, 2012).
[3] Dina Krichker, «Making Sense of Borderscapes: Space, Imagination and Experience», *Geopolitics* 26, Vol. 4 (5 July 2021): 1224–42, https://doi.org/10.1080/14650045.2019.1683542.
[4] Dennis Broeders, «The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants», *International Sociology* 22, Vol. 1 (January 2007): 71–92, https://doi.org/10.1177/0268580907070126.

the EU's capacity to surveil and regulate migrant populations, often leading to new forms of social and political exclusion.[5] The concept of "digital borders" captures the ways in which digital technologies, including biometric data collection and social media monitoring, are increasingly used to create and enforce boundaries that are both symbolic and territorial. Digital borders operate through an assemblage of technologies that not only track and control the physical movements of migrants but also shape public narratives and perceptions about migration.[6] This dual function of digital borders—both as instruments of control and as tools for narrative construction—raises critical ethical and political questions, particularly regarding the potential for these technologies to perpetuate discrimination and inequality.

The digital infrastructures that enable migrant movement, such as mobile devices and social media, can also be repurposed by states and corporations for surveillance and control, further complicating the relationship between mobility and security in the digital age.[7] The EU's reliance on digital systems for border management reflects broader trends in global governance, where digital sovereignty—defined as the control over digital data, infrastructure, and technologies—has become a central concern for states.[8] As digital borders become more pervasive, they raise important questions about the balance between security and rights, particularly in relation to the treatment of marginalized and vulnerable populations, such as in the case of refugees, asylum seeker and victims of trafficking.[9] This paper will focus on a form of hidden marginalization that affects migrant populations through an analysis of the digital control exercised during their identification process.

The concept of the digital border is characterized by its inherent dynamism, transcending the physical limitations of state sovereignty. Unlike the more overt forms of control and surveillance exercised at a state's geographical borders, digital border control can be subtler and more pervasive. Through the widespread use of digital technologies, harsher forms of control can be enacted, often masked by a techno-solutionist approach that presents technology as neutral and objective. Recent approaches to investigating technologies and the data they produce have moved beyond a positivistic framework. This outlook considers technology and data as mere technical phenomena, overlooking the social and political implications carried by technological change. This paradigm shift has brought the phenomena of migration under the lenses of novel

[5] Philippa Metcalfe and Lina Dencik, 'The Politics of Big Borders: Data (in)Justice and the Governance of Refugees', *First Monday*, 1 April 2019, https://doi.org/10.5210/fm.v24i4.9934.
[6] Lilie Chouliaraki and Myria Georgiou, 'The Digital Border: Mobility beyond Territorial and Symbolic Divides', *European Journal of Communication* 34, no. 6 (December 2019): 594–605, https://doi.org/10.1177/0267323119886147.we develop a definition of the digital border as an assemblage of mediations that articulates digital and other technologies with symbolic resources to draw boundaries of inside/outside both on the ground (territorial border
[7] Mark Latonero and Paula Kift, 'On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control', *Social Media + Society* 4, no. 1 (January 2018): 205630511876443, https://doi.org/10.1177/2056305118764432.
[8] Bruno Oliveira Martins, Kristoffer Lidén, and Maria Gabrielsen Jumbert, 'Border Security and the Digitalisation of Sovereignty: Insights from EU Borderwork', *European Security* 31, no. 3 (3 July 2022): 475–94, https://doi.org/10.1080/09662839.2022.2101884.
[9] E. Tendayi Achiume, 'Digital Racial Borders', *AJIL Unbound* 115 (2021): 333–38, https://doi.org/10.1017/aju.2021.52.{\\i{}AJIL Unbound} 115 (2021

perspectives such as critical data studies,[10] post-colonial data studies,[11] and feminist data studies.[12] These approaches emphasize that technology does not exist in a vacuum; rather, it reflects and potentially amplifies existing power dynamics and imbalances from the physical world, albeit in ways that may be less detectable. Since the digital border is not tied to a specific location, it can manifest anywhere, following migrants throughout their journey to their final destinations. This process, which Broeders and Dijstelbloem[13] describe as the "datafication of mobility and migration management," involves the accumulation of personal and sensitive data—particularly biometric data—creating a digital representation of the migrant, often referred to as a "data double."

This digital identity is shaped within a socio-technical infrastructure that, in Foucauldian terms, exerts knowledge and power over the migrant's existence. The creation of a migrant's digital identity involves practices of subjectivation that establish migrants as digital subjects governed by rules, laws, and both technical and human practices. This process of digital subject formation occurs simultaneously with the creation of European digital subjectivity through EU policies and regulations. However, these two pathways diverge significantly. While the evolution of policies regarding the digital identity of European citizens is geared towards establishing rights over their identities and personal data, the process for migrants is the opposite, marked by a continual increase in the amount of data (biometric, facial, informational) extracted from them upon their arrival. This dynamic creates a clear distinction between migrants and European citizens, reinforcing the status of the former as "others." Just as migrants experience physical exclusion through restrictions on their movement, they are similarly excluded at the digital level. Thus, we argue that a practice of "digital othering" exists, further entrenching the exclusion of migrants from their lives through the loss of their right to control their personal data. While EU citizenship grants various rights from which non-EU citizens are automatically excluded, the evolving securitarian nature of the Eurodac regulation exacerbates these disparities. This evolution exemplifies digital othering: migrants, lacking EU citizenship, increasingly lose control over their personal data and are compelled to share more information without corresponding benefits.

[10] Andrew Iliadis and Federica Russo, 'Critical Data Studies: An Introduction', *Big Data & Society* 3, no. 2 (December 2016): 205395171667423, https://doi.org/10.1177/2053951716674238.
[11] Didier Bigo, Engin F. Isin, e Evelyn Sharon Ruppert, *Data politics: worlds, subjects, rights*, Routledge studies in international political sociology (London ; New York: Routledge, Taylor & Francis Group, 2019).
[12] Catherine D'Ignazio and Lauren F. Klein, *Data Feminism*, First MIT Press paperback edition (Cambridge, Massachusetts: The MIT Press, 2023); Georgiana Turculet, 'Data Feminism and Border Ethics: Power, Invisibility and Indeterminacy', *Journal of Global Ethics* 19, no. 3 (2 September 2023): 323–34, https://doi.org/10.1080/17449626.2023.2278533.
[13] Dennis Broeders and Huug Dijstelbloem, *The Datafication of Mobility and Migration Management*

The Mediating State and Its Consequence, p.242-260 in Ymkje Hilda Ploeg and Jason Pridmore, *Digitizing Identities: Doing Identity in a Networked World*, Routledge Studies in Science, Technology and Society 30 (New York: Routledge, 2016).

2. OTHERING AND IDENTITY

2.1 Tracing the Development of "Othering"

The concept of "othering" has evolved through a complex intellectual lineage rooted in the study of power dynamics and social differentiation in relation to class, as theorized by Hegel in his lord-bondsman dialectic, adapted to culture by Said, and finally culminating in its current ubiquity in the age of identity politics. At its core, othering as it is understood today refers to the processes, systems, or actions that create and reinforce distinctions between groups, typically by a dominant group (the "self" or in-group) against a marginalized group (the "other" or out-group). This process often involves the homogenization of the out-group as inherently inferior, perceived as a monolithic entity, while the in-group is recognized for its individuality.[14,15] The boundaries between self and other are fluid and context-specific, such as rivalries between sports teams (where the "other" is the fan of the opposing team), cultural differences, or geographical boundaries.

Throughout the 20th century, the Hegelian dialectic of the self (lord) consolidating its identity by objectifying and assigning negative attributes to the other (bondsman) expanded beyond class dynamics to become an important tool in sociological and cultural analysis. Simone de Beauvoir applied the Hegelian dialectic to gender relations in her seminal 1949 work, Le Deuxième Sexe (The Second Sex)[16], illustrating how men (the norm) are seen as the active subjects, while women are cast as the deviant other, defined only in opposition to men. The prominent Palestinian-American philosopher Edward Said developed the concept further in 1978 with his seminal concept of 'Orientalism'.[17] Examining othering through the lens of race and culture, particularly in the context of colonialism, he argued that Western colonial powers, particularly the French and British empires, constructed the Orient as an inherently different and inferior Other in order to justify their dominance. The Orient was portrayed as a vague, monolithic entity encompassing diverse regions from North Africa to China, in a way that served to rationalize Western superiority and control. It is this latest development of the concept, as developed by Said and a cornerstone of 21st century postcolonial studies, that serves as the theoretical basis of this paper. His illustration of how the 'West' has historically objectified and marginalized non-Western cultures in order to maintain power provides a theoretical pathway into the detrimental downstream effects on the lived realities of migrants.

As a framework, othering is adaptable to different contexts in which group distinctions and hierarchies are imposed. Beyond its theoretical genesis in the nineteenth century, in its most

[14] Klaus Abbink and Donna Harris, 'In-Group Favouritism and out-Group Discrimination in Naturally Occurring Groups', ed. Pablo Brañas-Garza, *PLOS ONE* 14, no. 9 (4 September 2019): e0221616, https://doi.org/10.1371/journal.pone.0221616.
[15] Hassan Mahamdallie, 'Islamophobia: The Othering of Europe's Muslims', *International Socialism*, no. 146 (2015).
[16] Simone de Beauvoir, *The Second Sex* (Random House, 2009).
[17] Edward W. Said, *Orientalism* (New York: Pantheon Books, 1978).

primordial form it is an evolutionary reflex that originally served survival in pre-modern societies. The rapid categorization of in-group and out-group members was a life-or-death instinct in prehistoric communities.[18] However, the persistence of this instinct in modern times often exacerbates social divisions and oppression. In political arenas, othering remains a powerful tool used to justify action or inaction towards marginalized groups. It is also replicated in bureaucracies, where the other is constantly reminded of its non-belonging. Finally, and this is the subject of this research, it has implications on humanitarianism; the techno-administrative aspect of humanitarian work often reflects these imbalances, where both state bureaucrats and the core administrative staff of humanitarian organizations are citizens and part of the 'in-group' compared to their migrant clientele. Ultimately, all applications of othering are characterized by power imbalances: the self is superior to the other, men to women, citizens to migrants.[19,20] The concept is deeply embedded in the positionality of the agent, making it a crucial lens through which to analyze social and political dynamics.

2.2 Convergence of Marginalization

Most arenas of social and political life in pluralistic countries are characterized by at least rudimentary representation, i.e. the existence of pressure groups, associations or other forms of collective political action. They represent women campaigning for gender equality (e.g. European Women's Lobby), the plight of members of the LGBTQ community (e.g. Inter-LGBT France), family businesses (e.g. Die Familienunternehmer) or ceramic tile manufacturers (European Ceramic Tile Manufacturers Federation). However, the voices, experiences and opinions of asylum seekers, refugees and people on the move in general are largely absent. While there are several international and local organizations that speak on behalf of migrants, they themselves lack direct political agency without mediation in Berlin, Paris, Rome or Brussels, i.e. there is no political party by and for migrants. There are many reasons for this, including lack of clear status and associated political rights, language issues, lack of knowledge of potential avenues for political engagement, lack of access to funding and other resources, and geographical isolation (once in camps or informal settlements).

In addition to a lack of direct representation, migrants are faced with technocratic overreach of governments and unwanted consequences of "Digital Humanitarianism." While digital tools in general carry largely positive potential for the improvement of humanitarian responses, the advent of "Digital Humanitarianism" has been accompanied by several issues, including the over-reliance on digital tools and algorithms at the expense of traditional humanitarian practices or the entrenchment of power imbalances as platforms, tools, and technologies used in humanitarian

[18] Oliver Sng, Keelah E. G. Williams, and Steven L. Neuberg, 'Evolutionary Approaches to Stereotyping and Prejudice', in *The Cambridge Handbook of the Psychology of Prejudice*, ed. Chris G. Sibley and Fiona Kate Barlow, 1st ed. (Cambridge University Press, 2016), 21–46, https://doi.org/10.1017/9781316161579.002.
[19] Gabriele Griffin, *A Dictionary of Gender Studies* (Oxford: Oxford University Press, 2017).
[20] Annalisa Pelizza, 'Processing Alterity, Enacting Europe: Migrant Registration and Identification as Co-Construction of Individuals and Polities', *Science, Technology, & Human Values* 45, no. 2 (March 2020): 262–88, https://doi.org/10.1177/0162243919827927.

work are mainly developed and controlled by organizations in the Global North.[21] This chapter aims to highlight some of the potential risks that could develop at the intersection of digital identity and digital humanitarianism.

From a state-centric perspective, the rationale for making migrants digitally transparent is to maximize security. Humanitarian actors, on the other hand, operate under the maxim of efficiency in their aid and relief operations. While their goals may be different, the tools to achieve them can converge. NGOs, while mostly not collecting fingerprints themselves for example, may rely on existing data infrastructures built by governments and IOs (e.g. data bases of the UN and its agencies) which are not uncontroversial regarding data privacy and autonomy.[22] The process of establishing these data bases is not simply one of collecting information about migrants' histories and identities, but one of actively creating them: Through the collection of data points, digital images and fingerprints, the identity of the othered subject (i.e. the migrant) is created and consolidated in a continuous process.[23]

It is this convergence of marginalization(s), the lived realities of migrants, and their lack of ability to effectively voice political grievances that places them in a vulnerable position with regard to technocratic overreach. They are therefore more likely to fall prey to the consequences of techno-solutionism, for example in techno-regulatory 'sandboxes', which often describe nothing more than the absence of civil rights safeguards in limited spheres of application. In several cases, they have become a "laboratory for the implementation of new data practices"[24] (e.g. UNHCR's PRIMES data base, "refugees on the blockchain"[25] in WFP's Building Blocks program[26], ID2020[27] which aims to provide undocumented people, incl. refugees, with a digital identity with unclear privacy safeguards[28]). It is precisely this bifurcation of society–citizens as subjects with digital rights and migrants as objects of digital surveying–that we refer to below as the digital othering of migrants. The digital other, as subjects conceptually removed from that of the enfranchised citizen, becomes a testing ground for what is technologically possible but legally controversial in destination countries. And because they are Others, regulatory oversight of projects is minimal and accountability is largely reduced to reports by humanitarian organizations, rendering the lived realities of the digitally transparent migrant an opaque space of high-risk decision-making.

[21] Patrick Meier, *Digital Humanitarians: How Big Data Is Changing the Face of Humanitarian Response.* (Routledge, 2015).
[22] Katja Franko Aas, '"The Body Does Not Lie": Identity, Risk and Trust in Technoculture', *Crime, Media, Culture: An International Journal* 2, no. 2 (August 2006): 143–58, https://doi.org/10.1177/1741659006065401.
[23] Radha S. Hegde, 'Itinerant Data: Unveiling Gendered Scrutiny at the Border', *Television & New Media* 20, no. 6 (September 2019): 617–33, https://doi.org/10.1177/1527476419857686.
[24] Sandra Ponzanesi, 'Migration and Mobility in a Digital Age: (Re)Mapping Connectivity and Belonging', *Television & New Media* 20, no. 6 (September 2019): 522, https://doi.org/10.1177/1527476419857687.
[25] Jessi Hempel, 'How Refugees Are Helping Create Blockchain's Brand New World', *Wired*, 2018, https://www.wired.com/story/refugees-but-on-the-blockchain/.
[26] Farah Awan and Soheib Nunhuck, 'Governing Blocks: Building Interagency Consensus to Coordinate Humanitarian Aid', *Journal of Science Policy & Governance* 16, no. 02 (27 May 2020), https://doi.org/10.38126/JSPG160201.
[27] Btihaj Ajana, 'Chapter 24 Digital Biopolitics, Humanitarianism and the Datafication of Refugees', in *Refugee Imaginaries*, by Lyndsey Stonebridge et al. (Edinburgh University Press, 2019), 463–79, https://doi.org/10.1515/9781474443210-033.
28https://medium.com/berkman-klein-center/the-dangers-of-blockchain-enabled-immunity-passports-for-covid-19-5ff84cacb290

3. HUMANITARIAN BIOMETRICS – BIOMETRIC HUMANITARIANISM

3.1 Biometrics

Digital othering transcends "regular" othering insofar as it combines both the socio-political imposition of identity, which constructs the out-group with different histories, lifestyles, and abilities compared to the in-group, and a techno-administrative dimension, in which migrants are assigned a digital identity to mark them as part of the out-group. The latter is a process that can be born out of different rationales; humanitarian organizations need to fixate digital identities in order to deliver aid efficiently while ensuring internal and external accountability. States registering refugees at their borders or elsewhere tend to invoke security and surveillance motives for digitally capturing migrants' identities.

While biometrics and other forms of digital identity creation are not the standard in the humanitarian sector, UN agencies increasingly appear to see them as a promising solution in times of demand for greater transparency and traceability of donor money. The World Food Program (WFP), for example, started using the iris scan technology 'Eye Pay' already in 2016 in the Jordanian Za'atari refugee camp to allow migrants to buy food without cards, cash or vouchers.[29] Such biometric technologies are a frequently used way to create digital identities, through "the recognition of people on the basis of intrinsic physical or behavioral characteristics."[30] In Yemen, the WFP is conducting similar biometric datafication of aid recipients through its digital assistance platform SCOPE, with permission by the Houthis–detailed in a contract which is confidential and as such not accessible to those whose data is concerned.[31] Biometrics may include iris scans,[32] facial scans (ICRC's "Trace the Face,"[33] or finger-/handprints). Less common forms of biometry which are currently not used in the humanitarian sector are the recognition of DNA and vascular patterns and behavioral biometrics such as the recognition of voices and of handwriting, and even gait recognition.[34]

[29] Orla Nicole Hadjisophocleous, Tahir Abbas Syed, and Hana Lee, 'Blockchain-Enabled Humanitarian Aid: A Case Study of the World Food Programme', 2021.
[30] Mark Maguire, 'The Birth of Biometric Security', *Anthropology Today* 25, no. 2 (April 2009): 9, https://doi.org/10.1111/j.1467-8322.2009.00654.x.
[31] Marie-Louise Clausen, 'Piloting Humanitarian Biometrics in Yemen', MidEast Policy Brief (Peace Research Institute Oslo, 2021).
[32] Katja Lindskov Jacobsen, 'Experimentation in Humanitarian Locations', *Security Dialogue* 46, no. 2 (2015): 144–64.
[33] Kerrie Holloway, Reem Al Masri, and Afnan Abu Yahia, 'Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises' (Humanitarian Policy Group, 2021).
[34] Mark Maguire, 'The Birth of Biometric Security' (no 42).

3.2 The dual nature of digital technologies

Already in 2013, the United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA) addressed the challenges and potential trajectories of digital technology in its field, and thus the inevitable arrival of "humanitarianism in the network age."[35] In its report, the agency concluded that digitization poses challenges to the approach to humanitarian assistance that governments and NGOs have been accustomed to, as aid recipients become increasingly autonomous, self-confident, and well-connected thanks to emerging digital technologies.

Likewise, some experimental digital pathways into the lives of migrants are made under the premise of increased autonomy. Rather than a threat to organizational control, the use of digital technologies in aid delivery is framed as an empowering development that increases migrants' agency.[36] Tazzioli's case study of Greece, host country of the EU's first Mastercard-supported cash assistance program, illustrates the discrepancies between claims of autonomy and experienced restrictions.[37] In this example, instead of traditional aid delivery, such as rations of rice, migrants are provided with bank cards tied to their digital identities, which they can use to purchase a specific amount and type of goods from designated stores. The gain in autonomy–the recipient can decide when, what, and how much to buy within certain limits–comes with exponentially increased traceability of movements and consumption habits, while the parameters remain entirely in the hands of the donor. In order to receive the ATM- and point-of-sale enabled bank card, migrants had to agree to stay in designated shelters. In contrast to greater autonomy, they remain restricted not only in what and where they can buy, but more importantly, where they can live.

3.3 Forms of Othering

The process of data-enabled othering of migrants can be understood as a consequence of the fact that "making vulnerable populations *knowable* is central to humanitarian governance."[38] In the age of Digital Humanitarianism, humanitarian knowledge is increasingly generated using digitized quantitative data – "a move away from the of local immersion and culturally specific knowledge that had characterized earlier phases of the work of NGOs."[39] Two distinct but cumulative forms of othering occur: Migrants are othered because laws and regulations that protect citizens or "ordinary" migrants do not apply to them. Conceptually, they become part of an extra-legal entity, an out-group that does not enjoy the same digital rights as their in-group counterparts. This form

[35] UNOCHA, 'Humanitarianism in the Network Age. Including World Humanitarian Data and Trends 2012' (New York: United Nations Office for the Coordination of Humanitarian Affairs, 2013), https:// www.unocha.org/sites/unocha/files/HINA_0.pdf.
[36] Martina Tazzioli, 'The Technological Obstructions of Asylum: Asylum Seekers as Forced Techno-Users and Governing through Disorientation', *Security Dialogue* 53, no. 3 (June 2022): 202–19, https://doi.org/10.1177/09670106211026080.
[37] Ibid.
[38] Elisa Pascucci, 'Labor', in *The Routledge International Handbook of Critical Philanthropy and Humanitarianism*, ed. Katharyne Mitchell and Polly Pallister-Wilkins, 1st ed. (London: Routledge, 2023), https://doi.org/10.4324/9781003162711.
[39] Ivi. 55

of othering then predicates different digital articulations that reinforce each other. As a datafied digital other, one's claim to freedom of movement and personal data is invalid. Therefore, one's location can be tracked and fixed through coercion (e.g., withholding aid in case of movement).[40] The possibilities and modalities of opting out are largely unclear. As a recipient of aid, either directly from government agencies or through humanitarian organizations, one's eligibility for such aid must be confirmed, and its reception must be traceable to reassure donors and taxpayers.[41,42,43,44] To facilitate this, privacy and other freedoms must be restricted. The reciprocal and mutually reinforcing nature of this relationship not only leaves migrants in a bureaucratic limbo, but also solidifies their being as the inherent and eternal other, both digitally and physically.

[40] Ivi. 41
[41] Vicki Squire and Modesta Alozie, 'Coloniality and Frictions: Data-Driven Humanitarianism in North-Eastern Nigeria and South Sudan', *Big Data & Society* 10, no. 1 (January 2023): 205395172311631, https://doi.org/10.1177/20539517231163171.
[42] Katja Lindskov Jacobsen and Larissa Fast, 'Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care', *Disasters* 43, no. S2 (April 2019), https://doi.org/10.1111/disa.12333.
[43] Mirca Madianou, 'The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies', *Television & New Media* 20, no. 6 (September 2019): 581–99, https://doi.org/10.1177/1527476419857682.
[44] Sandra Ponzanesi, 'Migration and Mobility in a Digital Age: (Re)Mapping Connectivity and Belonging' (no. 22)

4. THE EUROPEAN DIGITAL IDENTITY AND THE EURODAC DATABASE

4.1 The First Path: A Digital Identity for All Europeans

The EU is keen on creating a new digital identity framework that claims to empower European citizens, offering the ability to control their data.[45] Prominent EU diplomats and representatives have voiced the need to develop a community identity layer to foster the sovereignty and control over data produced by European citizens and within European borders. In her address to the State of the Union in 2020, Ursula von der Leyen pushed the idea of bolstering a European digital identity solution:
"Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data. That is why the Commission will propose a secure European e-identity. One that we trust, and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data is used and how."[46]

In order to follow these objectives, the European Digital Identity Wallet will allow all Europeans to have a secure digital identity that protects personal data and works in all Member States.[47] The technological requirements needed to develop such a solution have overlapped with the needs of agenda setting among the policy options of the EU digital strategy. Weigl[48] convincingly shows how a hastened policy activity at the EU level with respect to digital identity has shifted the legal landscape, starting from the first regulations that aimed to achieve interoperability among EU countries. The EIDAS Regulation (Electronic Identification Authentication and Trust Services) in 2014[49] marked a step forward as it was the first comprehensive legal framework at the European level designed to create consistency and trust in the digital identity landscape

[45] Silvia Lips et al., 'Re-Shaping the EU Digital Identity Framework', in *DG.O 2022: The 23rd Annual International Conference on Digital Government Research* (dg.o 2022: The 23st Annual International Conference on Digital Government Research, Virtual Event Republic of Korea: ACM, 2022), 13–21, https://doi.org/10.1145/3543434.3543652.
[46] Ursula Von Der Leyen*, State of the Union Address by President von der Leyen at the European Parliament Plenary,* 16 September 2020*.*
[47] https://ec.europa.eu/digital-buildingblocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home. *Accessed on the 1/09/2024*
[48] Linda Weigl et al., 'The EU's Digital Identity Policy: Tracing Policy Punctuations', in *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance* (ICEGOV 2022: 15th International Conference on Theory and Practice of Electronic Governance, Guimarães Portugal: ACM, 2022), 74–81, https://doi.org/10.1145/3560107.3560121.
[49] 'Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC', L 257 Official Journal of the European Union § (2014).

across the EU.[50,51,52,53] Its primary objectives were to establish a secure and interoperable system for electronic identification and to facilitate cross-border access to online public services between EU countries. These requirements were originally envisioned within a certification scheme left at the will of the single European countries. As there were no obligations in place for EU countries to adopt a framework for their national identity solution, the regulation has seen a limited uptake, limited to public services, leaving the private sector behind.[54]

The eIDAS Regulation aimed to provide a long-lasting legal basis for a European identity ecosystem by enabling member states to mutually recognize electronic identities. By the late 2010s, the focus shifted away from merely facilitating cross-border access to online public services. The need for a more robust and harmonized digital identity framework became apparent, driven by concerns over digital sovereignty, data control, and the increasing dominance of large online platforms in the digital economy.[55] There is increasing attention at both academic and policy levels on strengthening European digital sovereignty to ensure control over crucial technologies and data. European officials are also concerned about the growing influence of private corporations on the internet, prompting efforts to establish constitutional control and sovereignty over European technologies.[56,57]

Hence, the EU main bodies (with the kickstart of the EU commission) have drafted a plan to further entrench digital identity regulation within key policy priorities that address and further strengthen the role of the EU in the global digital arena (Bradford 2020, 2023a, 2023b). In response to these changing dynamics, the European Commission proposed the European Digital Identity Framework (EDIF) as a new legislative measure. This proposal, introduced in 2021 and entered into force in 2024,[58] represented a substantial shift in ambition compared to the original eIDAS Regulation. It aimed to create a more unified and powerful digital identity system across the EU with a stronger

[50] Stefan Mocanu et al., «Identification and Trust Techniques Compatible with eIDAS Regulation», in *Security and Privacy in New Computing Environments*, a c. di Jin Li, Zheli Liu, and Hao Peng, vol. 284, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (Cham: Springer International Publishing, 2019), 656–65, https://doi.org/10.1007/978-3-030-21373-2_55.

[51] Daniela Gregušová, Zuzana Halásová, and Tomáš Peráček, «eIDAS Regulation and Its Impact on National Legislation: The Case of the Slovak Republic», *Administrative Sciences* 12, Vol. 4 (6 December 2022): 187, https://doi.org/10.3390/admsci12040187.

[52] Amir Sharif et al., «The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes», *Applied Sciences* 12, Vol. 24 (10 December 2022): 12679, https://doi.org/10.3390/app122412679.related to privacy and security

[53] Marko Hölbl, Boštjan Kežmah, and Marko Kompara, «eIDAS Interoperability and Cross-Border Compliance Issues», *Mathematics* 11, Vol. 2 (13 January 2023): 430, https://doi.org/10.3390/math11020430.

[54] European Parliamentary Research Service, 'The EU's Strategic Autonomy: Framework for Discussion and Possible Future Developments' (European Parliament, 2022), https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf.

[55] C. Codagnone et al., 'Europe's Digital Decade and Autonomy', *Publication for the Committee on Industry, Research and Energy, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg*, 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695465/IPOL_STU(2021)695465_EN.pdf.

[56] Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge Studies in European Law and Policy (Cambridge: Cambridge university press, 2022).

[57] Giovanni De Gregorio and Roxana Radu, 'Digital Constitutionalism in the New Era of Internet Governance', *International Journal of Law and Information Technology* 30, no. 1 (15 April 2022): 68–87, https://doi.org/10.1093/ijlit/eaac004.

[58] 'Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework', L 1183 Official Journal of the European Union § (2024).

focus on giving citizens control over their data, creating an EU-made identity solution that ensures privacy and reduces dependence on non-European technologies and platforms through strengthening the EU's digital sovereignty.[59] This regulation introduces the concept of a European Digital Identity Wallet, which would be mandatory for member states to issue under a notified eID scheme and required private companies to accept it for strong authentication.

Zooming in on the issue of data sovereignty, Hummel[60] maintains that at the EU policy level, the main understanding of data sovereignty is a process that increases the degree of control of European citizens over their identity data through an apparatus of technical standards, hard and soft laws (such as the Data Governance Act and the Data Act). In synergy with the provisions on data minimization concerning EU citizens and the technological capabilities of decentralized identity models,[61] the European Digital Identity framework creates at the EU level a set of guarantees for European citizens over any private or public provider that wants to access their identity data. Connected to this, the European Declaration on Digital Rights and Principles[62] further establishes the protection of privacy of personal data as a cornerstone of the attempt to create an EU digital constitution in which European technologies by principle of regulation and technical design protect the digital rights of European citizens. Thus, the EU has pushed for the creation of a wallet under the revision of the EIDAS regulation. [63] We can briefly look at the technical documentation to show how it fosters privacy, data control and data minimization.

The EU Digital Identity Wallet's (EUDI Wallet) architecture employs a robust public-private key infrastructure to manage digital identities securely. Private-public key infrastructure is a mode of managing identity credentials and the identification process that allows for a secure and privacy-preserving transmission of data through cryptographic protocols.[64] This infrastructure involves each user being associated with a unique cryptographic key pair: a private key stored securely in

[59] André Barrinha e G. Christou, «Speaking Sovereignty: The EU in the Cyber Domain», *European Security* 31, Vol. 3 (3 July 2022): 356–76, https://doi.org/10.1080/09662839.2022.2102895.

[60] Patrik Hummel et al., «Data Sovereignty: A Review», *Big Data & Society* 8, Vol. 1 (January 2021): 205395172098201, https://doi.org/10.1177/2053951720982012.but also confront different agents and stakeholders with challenges in retaining control over their data. Our goal in this study is to arrive at a clear picture of what is meant by data sovereignty in such problem settings. To this end, we review 341 publications and analyze the frequency of different notions such as data sovereignty, digital sovereignty, and cyber sovereignty. We go on to map agents they concern, in which context they appear, and which values they allude to. While our sample reveals a considerable degree of divergence and an occasional lack of clarity about intended meanings of data sovereignty, we propose a conceptual grid to systematize different dimensions and connotations. Each of them relates in some way to meaningful control, ownership, and other claims to data articulated by a variety of agents ranging from individuals to countries. Data sovereignty alludes to a nuanced mixture of normative concepts such as inclusive deliberation and recognition of the fundamental rights of data subjects.","container-title":"Big Data & Society","DOI":"10.1177/2053951720982012","ISSN":"2053-9517, 2053-9517","issue":"1","journalAbbreviation":"Big Data & Society","language":"en","page":"205395172098201","source":"DOI.org (Crossref

[61] Alexandra Giannopoulou, «Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity», *Digital Society* 2, Vol. 2 (August 2023): 18, https://doi.org/10.1007/s44206-023-00049-z.{\\i{}Digital Society} 2, fasc. 2 (agosto 2023

[62] European Union, 'European Declaration on Digital Rights and Principles for the Digital Decade', 2022, https://ec.europa.eu/newsroom/dae/redirection/document/94370.

[63] eIDAS Expert Group and European Commission, 'European Digital Identity Wallet Architecture and Reference Framework, Version 1.1.0' (GitHub Pages, 2024), https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/arf/.

[64] Jeongheon Kim et al., 'Service Applicable Blockchain-Based Self-Sovereign Identity Management System', in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dubai, United Arab Emirates: IEEE, 2023), 1–5, https://doi.org/10.1109/ICBC56567.2023.10174875.

a cryptographic device, such as a hardware security module or secure element (Section 3.13), and a public key, which is shared for identity verification and encryption (Section 3.3). The private key never leaves the secure environment, safeguarding it against unauthorized access and tampering. Meanwhile, the public key is used for verifying the user's identity or digital signatures and can be distributed to encrypt sensitive data, ensuring that only the holder of the corresponding private key can decrypt it. This encryption process is crucial for maintaining confidentiality during data exchanges across potentially insecure channel. The wallet collects only the minimum data required to verify identity or perform transactions, giving users complete control over what information is shared and with whom. The path that the regulation and policy on digital identity, privacy, and data have seen in the last 20 years of EU policy making has led to an institutional, technical, and legal landscape that enshrines the principles of privacy-protection, sovereignty, and control over data according to the vision established by the European Commission in the key policy document "A Europe Fit for the Digital Age." Paired with the landmark regulation on data protection, the General Data Protection Regulation (GDPR),[65] which explicitly mandates a special regime of treatment for biometric data, the EU has prioritized the creation of a regulatory landscape that establishes a strong protection of personal and sensitive data for European citizens. This overview of the EU Digital Identity and the principles underlying it is essential to better frame the investigation of the main theme of this paper: the role of migrants concerning the rights to privacy and the ongoing efforts to establish technological solutions that enhance control and sovereignty over data.

As briefly mentioned in the introduction, when we consider the border not merely as a geographical and physical boundary but as a sociopolitical (and for the purposes of this paper, sociotechnical) practice, we can also understand how the creation of the border involves a dynamic of "othering." In this dynamic, the political subject—in this case, the digital subject[66] is granted rights and opportunities based on its position within this process.

In this section, we have briefly touched upon what lies "inside" the digital border: a citizen enjoying a wide array of rights in their digital life, seen as an extension of the rights granted in their physical life. For EU citizens, this is facilitated through European policies aimed at creating a socio-technical environment where the rights established in EU treaties are also applied in a transformed way within the digital realm.[67] Specifically, EU law and policy-making institutions have invested considerable effort in fostering a secure and privacy-preserving digital environment to protect the European digital subject.

However, outside the EU digital border, the situation is different. While the development of the EU's digital identity landscape has focused on harmonizing national laws regarding eID to ensure individual control over data, the process has taken a different direction in the case of migrants. As migrants cross EU physical borders, they undergo a sociotechnical practice of biometric identification that establishes their digital subjectivity as "the other". This othering is manifested

[65] 'General Data Protection Regulation (GDPR), Regulation (EU) 2016/679', L 119 Official Journal of the European Union. § (2016).
[66] Olga Goriunova, «Digital Subjects: An Introduction», *Subjectivity* 12, Vol. 1 (March 2019): 1–11, https://doi.org/10.1057/s41286-018-00065-2.
[67] Anu Bradford, 'Europe's Digital Constitution', *Va. J. Int'l L.* 64, no. 1 (2023): 1–69.

through differential treatment concerning personal data, particularly sensitive data such as biometric information, when compared to European citizens.

We argue that the primary mechanism of this othering is the increase in the type of biometric data extracted from migrants for identification and security purposes. While the evolution of EIDAS (in both its versions) and the EUDI Wallet aims to empower EU citizens by minimizing data use and enhancing control over their data, the development of EU regulations on biometric identification at the border follows a different and opposing path, which will be explored in the next section.

4.2 The Second Path: The Evolution of the EURODAC Database

In order to face the challenges posed by the increase in migrations in Europe at the turn of the 21st century, the EU has deployed a battery of regulatory instruments to establish a set of technological tools and databases in order to manage the flows of migrants from third countries. The EU's Large Information System Agency (EU-LISA) is responsible for harmonizing several key databases that collect both alphanumeric and biometric data, such as fingerprints and facial images.[68] EU-LISA is working to make these systems interoperable through the development of a common identity repository and a multiple-identity detector to enhance the accuracy of individual identification.[69] Among the various databases under the EU-LISA (such as the Schengen Information System, the Visa Information System, and the Entry-Exit System), for the purpose of this paper, we will focus on the (European Dactyloscopy) EURODAC database, which collects fingerprints of undocumented migrants and asylum seekers and has been heavily revised and extended in scope since the entry into force of its first version (2003).[70] These databases play a critical role in supporting the daily collaboration and data-sharing activities of various quasi-federal agencies, including FRONTEX, EUROJUST, EUROPOL, and the EU Agency for Asylum (EUAA).

Analyzing the issue of the digital border, taking the case of EURODAC, is key in order to understand how the principles established in the policy documents and main declarations regarding the control over data hardly apply to migrants when it comes to EU management of the (digital) identity of migrants. In fact, in this section, we will show how the route followed by the legislative effort of EU institutions, if compared to what has been achieved in terms of control over data for European citizens, is reversed. In the process of revising the EIDAS regulation and creating a harmonized framework of digital identity for all Europeans, the use of cryptography-based modes of identification in the new European digital wallet exemplifies a step aimed at bolstering the control that EU citizens have on their identity data (increasing the compliance with the spirit of EU Privacy law such as the GDPR). Further to this, as previously stated, the principles of data

[68] Georgios Glouftsios, 'Governing Border Security Infrastructures: Maintaining Large-Scale Information Systems', *Security Dialogue* 52, no. 5 (October 2021): 452–70, https://doi.org/10.1177/0967010620957230.
[69] Paola Regina and Emilio De Capitani, 'Digital Innovation and Migrants' Integration: Notes on EU Institutional and Legal Perspectives and Criticalities', *Social Sciences* 11, no. 4 (23 March 2022): 144, https://doi.org/10.3390/socsci11040144.
[70] 'Council Regulation (EC) No. 2725/2000 of 11 December 2000 Concerning the Establishment of "Eurodac" for the Comparison of Fingerprints for the Effective Application of the Dublin Convention', Official Journal L 316 § (2000).

minimization and data security are entrenched in the EU digital wallet through a security-by-design approach leveraging the private-public key infrastructure.

When it comes to migrants and the policies that deal with the digitalization of borders, the process at the EU level, we argue, has worked following an orthogonal trend. An illustrative case is the development and expansion of the scope and application of the EURODAC database, where we can observe a case of "function creep"[71] in which the original purpose (tracking the movement of migrants in the EU at and between European borders) has been extended to include law enforcement and profiling purposes.

The EURODAC system represents a critical component of the European Union's approach to migration management, functioning as a large-scale biometric database primarily aimed at identifying asylum seekers and irregular migrants. Established in order to strengthen the provisions contained in the Dublin Regulation in 2003, EURODAC's core purpose is to store the fingerprints of asylum seekers and some categories of irregular migrants, facilitating the determination of the Member State responsible for processing an asylum application.

The use of biometric data, such as fingerprints, has become a "technological border" that extends beyond physical frontiers into the digital realm, where the identities of migrants are scrutinized and controlled. Menzes Queiroz[72] argues that the evolution of the EURODAC regulation presents the following issues: (i) The erosion of the purpose limitation principle; (ii) Enhanced accessibility by law enforcement authorities to EU immigration databases; (iii) The increasing digitalization of borders through biometrics. The expansion of scope in the EURODAC database seems to show a tendency in the EU policymaking on migration that blurs the boundaries between migration and crime.[73] Initially instituted in 2000, the EURODAC system became operational in January 2003, serving as a critical tool in determining the Member State responsible for examining asylum claims under the Dublin Regulation.[74]

The primary function of EURODAC has been to prevent "asylum shopping," a practice where asylum seekers submit applications in multiple EU Member States or select a state based on perceived favorable conditions. EURODAC's integration with the Dublin system was fundamental, as the database allowed for the comparison of fingerprints of asylum applicants across Member States, thereby ensuring that claims could be traced back to the country of first entry. EURODAC includes a Central Unit that operates the database and facilitates data transmission between Member States and the central system.[75] The fingerprints collected under this regulation fall into three categories: all asylum applicants aged 14 or older, all non-EU nationals aged 14 or older

[71] Frans W.A. Brom and Michiel Besters, '"Greedy" Information Technology: The Digitalization of the European Migration Policy', *European Journal of Migration and Law* 12, no. 4 (2010): 455–70, https://doi.org/10.1163/157181610X535782.
[72] Benedita Menzes Queiroz, 'The Impact of EURODAC in EU Migration Law: The Era of Crimmigration?', Market and Competition Law Review iii, no. 1 (2019), https://ssrn.com/abstract=4239931.
[73] Oliveira Martins, Lidén, and Jumbert, 'Border Security and the Digitalisation of Sovereignty'.
[74] Niovi Vavoula, Immigration and Privacy in the Law of the European Union: The Case of Information Systems (Brill | Nijhoff, 2022), https://doi.org/10.1163/9789004356115.
[75] Council Regulation (EC) No. 2725/2000 of 11 December 2000 Concerning the Establishment of "Eurodac" for the Comparison of Fingerprints for the Effective Application of the Dublin Convention», Official Journal L 316 § (2000). Art. 1

apprehended for crossing the border irregularly, and non-EU nationals aged 14 or older found to be illegally present in a Member State.[76]

Over time, EURODAC's role has expanded significantly. The second version of the regulation, which entered into force in 2013, also contains clauses for European national law enforcement agencies and EUROPOL to access the database under certain conditions, though requiring the oversight of an independent agency.[77] The European Commission's response to the massive influx of refugees in 2015 highlighted the operational challenges faced by frontline Member States like Greece and Italy, particularly regarding the fingerprinting and registration of migrants. In May 2016,[78] the Commission proposed another version of the EURODAC Regulation as part of a broader reform of the Common European Asylum System. This proposal aimed to further extend the database's scope by including additional biometric identifiers, such as facial recognition and digital photographs. It also proposed the inclusion of more personal data, such as names, dates of birth, and nationality information, to enhance the identification and return of irregular migrants.

The 2016 recast proposal was a response to the challenges of migration management in the EU and reflected the growing emphasis on using EURODAC for broader law enforcement purposes. The proposal included provisions for Member States to store and search data of third-country nationals and stateless persons who were not asylum applicants but were found irregularly staying in the EU, thus facilitating their identification for return and readmission purposes. Subsequent developments in the reform of EURODAC highlight the continued expansion and reinforcement of the system.[79] In 2017, trilogue negotiations between the European Parliament, the Council, and the European Commission resulted in agreements to further lower the age for fingerprinting and facial imaging of minors from 14 to 6 years old, to store more extensive personal and biometric data, and to improve Europol's access to the database for law enforcement purposes.[80]

The past negotiations and eventual agreement on the EURODAC Regulation, culminating in the Council's approval in February 2024, marked another significant step in the evolution of the database. The final act, published in the Official Journal in May 2024, expanded EURODAC's scope to include additional biometric and alphanumeric data and extended its use to new categories of individuals, such as those involved in search and rescue operations.[81] These changes, set to apply from June 2026, represent the latest phase in EURODAC's evolution, reflecting the EU's ongoing efforts to adapt its migration management tools to the complex and changing landscape of asylum and migration in Europe.

The expansion of EURODAC's scope, especially under the new regulations, illustrates a shift

[76] Council Regulation (EC) No. 2725/2000 of 11 December 2000 Concerning the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of the Dublin Convention. Art. 4, 8 and 11
[77] Lehte Roots, 'The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination', *Baltic Journal of European Studies* 5, no. 2 (1 October 2015): 108–29, https://doi.org/10.1515/bjes-2015-0016.
[78] Anita Orav, 'Recast Eurodac Regulation' (European Parliamentary Reaserch Service, June 2024), https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589808/EPRS_BRI(2016)589808_EN.pdf.
[79] Ivi. p.5
[80] Ivi, p.6
[81] Ivi, p.10

towards a more securitized and surveillance-oriented approach to migration. Originally intended solely for asylum purposes, EURODAC's database has been increasingly accessed by law enforcement agencies for criminal investigations, raising significant concerns about the erosion of the principle of purpose limitation.[82] This "function creep" not only undermines the original intent of the database but also poses risks of informal discrimination and stigmatization, as migrants and asylum seekers could be disproportionately viewed and treated as potential criminals.

The interoperability of EU information systems, including EURODAC, has raised substantial privacy and data protection concerns. As these systems are increasingly integrated to allow for the cross-referencing and sharing of data among various EU databases, the potential for misuse and overreach grows. Scholars have pointed out that this interoperability exacerbates the challenges of ensuring that the rights to privacy and personal data protection, particularly for third-country nationals, are adequately safeguarded[83], although, as Bellanova and Glouftsios point out, there are limitations in place to regulate cross-databases access rights.[84] The legal framework governing EURODAC and similar systems often struggles to balance the need for security and migration management with the fundamental rights of individuals, leading to tensions and legal ambiguities.

Furthermore, the biometric nature of EURODAC's data collection introduces additional layers of complexity in terms of privacy and data control. Biometric data, unlike other forms of personal data, is inherently sensitive and uniquely tied to an individual's identity, making its protection crucial. However, the current regulatory framework in the EU has been criticized for not fully addressing the specific challenges posed by biometric data.[85] These concerns are compounded by the lack of consistency in data protection practices across EU Member States, which can lead to varying levels of protection and enforcement.

The use of biometric technologies in migration management, as exemplified by EURODAC, also carries significant social and symbolic implications. The database serves not just as a tool for identification but as a mechanism for categorization and control, contributing to the broader phenomenon of "crimmigration," where migration is increasingly framed as a security issue. This framing tends to blur the lines between asylum seekers, irregular migrants, and criminals, reinforcing negative stereotypes and potentially leading to discriminatory practices.[86] Further to this, the socio-symbolic violence that forced biometric identification policy entails led some scholars to frame the issue as a form of "epidermal politics". Those practices have sparked

[82] Brigitta Kuster and Vassilis S. Tsianos, 'How to Liquefy a Body on the Move: Eurodac and the Making of the European Digital Border', in *EU Borders and Shifting Internal Security*, ed. Raphael Bossong and Helena Carrapico (Cham: Springer International Publishing, 2016), 45–63, https://doi.org/10.1007/978-3-319-17560-7_3.
[83] Vavoula, *Immigration and Privacy in the Law of the European Union*., p 2.
[84] Rocco Bellanova and Georgios Glouftsios, 'Formatting European Security Integration through Database Interoperability', *European Security* 31, no. 3 (3 July 2022): 454–74, https://doi.org/10.1080/09662839.2022.2101886.
[85] Annemarie Sprokkereef, 'Data Protection and the Use of Biometric Data in the EU', in *The Future of Identity in the Information Society*, ed. Simone Fischer-Hübner et al. (Boston, MA: Springer US, 2008), 277–84, https://doi.org/10.1007/978-0-387-79026-8_19.
[86] Jelmer Brouwer, Maartje Van Der Woude, e Joanne Van Der Leun, «Framing Migration and the Process of Crimmigration: A Systematic Analysis of the Media Representation of Unauthorized Immigrants in the Netherlands», *European Journal of Criminology* 14, Vol. 1 (January 2017): 100–119, https://doi.org/10.1177/1477370816640136.

resistance among migrants, who may engage in acts of defiance such as mutilating or burning their fingertips to avoid being entered into the system.[87] The act of fingerprinting, for instance, can be seen as a form of bodily subjugation, where migrants are coerced into providing their biometric data under threat of detention or deportation.[88]

As EURODAC continues to evolve, it remains at the center of debates over the balance between security and rights within the EU's migration governance. The system's expansion and increasing entanglement with law enforcement highlight the EU's broader shift towards a more restrictive and surveillance-oriented approach to migration. This shift has significant implications not only for the rights and privacy of migrants but also for the overall trust and legitimacy of the EU's migration policies. Critics argue that the reliance on biometric databases like EURODAC reflects a technocratic vision of migration management that prioritizes efficiency and control over human rights and ethical consideration.[89] The slide toward a securitized ICT migration infrastructure is not solely limited to EU policy and biometrics but creates an ecosystem of privacy-invading technologies that also enables regulation at the national level. The use of data extraction from the smartphones of migrants authorized by law in Germany, Austria, and Switzerland[90] might represent a new frontier of control exercised by state authority in apparent violation of both principles of data control, minimization, and privacy established in EU laws and policy documents.

The process of "digital othering" is established here through a set of regulations and policies that create "datafied migrants" whose digital rights are progressively removed. As we saw, the control over the personal data of European citizens increases through institutional and technical guarantees offered by the new EU Digital Wallet. In contrast, the evolution of the EURODAC database regulation and the presence of national regulations further reduce the autonomy of migrants when it comes to the management of their data, removing agency and autonomy from the digital subject through a securitized practice and discourse at the (digital) border. As the migrant is framed as the "other" which generates suspicion and concern, its data double—the digital replica of an individual through a set of data that identifies them[91]— is equally disempowered.

The contrasting approaches to digital identity and data control for EU citizens and migrants reveal a significant divergence in the application of privacy and data protection principles within the EU. While European citizens are increasingly empowered with tools such as the EU Digital Wallet, which enhances individual control over personal data, migrants experience a different reality. The technological infrastructure that serves to protect and empower citizens simultaneously imposes greater surveillance on migrants. This dichotomy suggests a trend within EU policy that frames the digital identities of migrants more as subjects of control than as bearers of rights.

[87] Georgios Glouftsios and Anna Casaglia, «Epidermal Politics: Control, Violence and Dissent at the Biometric Border», *Environment and Planning C: Politics and Space* 41, Vol. 3 (March 2023): 567–82, https://doi.org/10.1177/23996544221144872.
[88] Sanneke Kloppenburg and Irma Van Der Ploeg, «Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences», *Science as Culture* 29, Vol. 1 (2 January 2020): 57–76, https://doi.org/10.1080/09505431.2018.1519534.
[89] Matthias Leese, Simon Noori, and Stephan Scheel, 'Data Matters: The Politics and Practices of Digital Border and Migration Management', *Geopolitics* 27, no. 1 (1 January 2022): 5–25, https://doi.org/10.1080/14650045.2021.1940538.
[90] Ivan Josipovic, 'Digitalising Asylum Procedures: The Legitimisation of Smartphone Data Extraction for Retrospective Border Control', *Geopolitics*, 2 January 2024, 1–24, https://doi.org/10.1080/14650045.2023.2288162.
[91] Minna Ruckenstein, «Visualized and Interacted Life: Personal Analytics and Engagements with Data Doubles», *Societies* 4, Vol. 1 (18 February 2014): 68–84, https://doi.org/10.3390/soc4010068.

The integration of surveillance mechanisms into EU migration management systems could lead to the emergence of a differentiated system of digital rights, where one's ability to exercise data autonomy is influenced by their legal and social status within the EU.

In the context of the use of biometrical data in humanitarian contexts, care must be exercised regarding the collection, storage, and use of biometric data for people on the move. While international organizations extend their reach to provide essential services, this might come at the risk of creating a transactional system where access to fundamental aid is dependent on submitting biometric information. Unlike EU citizens, who benefit from the principle of "data minimization"—as seen in the design of the European Digital Identity wallet—migrants, particularly those in vulnerable situations, often do not enjoy the same protections. Given their reliance on humanitarian aid, migrants cannot opt out of providing biometric data without jeopardizing their access to critical resources.

This disparity underscores the need for heightened attention to data minimization in migration contexts, ensuring that only the minimum necessary data is collected to provide services. Further to this, the collection and centralization of biometric data in large databases might create a single point of failure that, if compromised, could endanger the safety and privacy of individuals and undermine the humanitarian systems designed to protect them.

Beyond security concerns, the widespread use of biometric data can also negatively impact the psychological well-being of migrants. The practice of collecting sensitive biometric information—such as fingerprints—can feel invasive and may contribute to a sense of loss of autonomy. For individuals already grappling with the challenges of displacement and uncertainty, this process may exacerbate feelings of disempowerment and surveillance. While the growing use of biometric data is often justified as a way to ensure the efficient provision of services and prevent fraud—particularly in conflict zones where aid may be misused, as seen in Yemen—it is critical not to overlook the potential drawbacks. The prioritization of data-driven identification systems for migrants, without the corresponding privacy safeguards, risks violating the dignity and rights of the very populations these systems are intended to protect. To address these challenges, humanitarian actors must ensure that biometric data is collected in a way that respects privacy and adheres to the principles of data minimization, even in non-EU contexts. Robust data protection frameworks and alternative identification methods should be explored to mitigate the risks associated with the over-reliance on biometric data. Ultimately, any humanitarian data collection system must balance the need for security and service delivery with the protection of migrant autonomy and human rights.

5. POLICY RECOMMENDATIONS

The decades-long trend in humanitarian efforts to rely on technology to fill capacity and resource gaps is unlikely to be reversed any time soon. Countering technological determinism with an undifferentiated rejection of digital technology in humanitarian efforts and for the betterment of migrants' lives is neither scientifically justified nor logically sound. Possible concrete measures to achieve a balanced outcome between protection and efficiency gains include:

1. The application of data protection and sovereignty rules to all subjects of the respective jurisdiction (in this case largely the European Union) without exception. Loopholes must be closed, and the practice of deliberate opening of strict regulations (i.e. sandboxing) for use cases related to migrants must be ended. Applying equal standards to equal people breaks the cycle of othering, at least in the digital sphere, and ultimately establishes equality as prescribed by the EU Charter of Fundamental Rights.
2. Therefore, a consensus needs to be reached on the proper use of digital technologies with respect to vulnerable groups, an idea that is not new but lacks commitment from state actors and NGOs. As early as 2013, the UN Special Rapporteur on the Human Rights of Migrants proposed the idea of a "firewall" between public services and migration control, whereby public services (health, education, housing, labor inspection, local police) would be instructed not to request migration status information unless it is necessary; and migration control would not have access to migration status information collected by public services.

Emerging technologies and their potential to entrench asymmetrical power relations are a burning issue beyond the realm of humanitarian work. They are high on the agendas of researchers, philosophers, and policymakers, and are often described as neutral tools, their benefit or danger depending on the users and their intentions. Kate Crawford cautions against such an understanding of the dynamics of technology, emphasizing instead that a tool, whether digital or physical, is in fact not neutral, but carries a specific affordance, a term that describes the relationship between an object or environment and the capabilities or actions it enables a user to perform.[92] Maslow's hammer, a commonplace metaphor for the cognitive bias associated with familiar tools, illustrates her reason for caution: "When the only tool you have is a hammer, it is tempting to treat everything as if it were a nail."[93]

Given the ready availability of biometrics and other digital technologies as tools in humanitarian work, all problems begin to appear as computationally solvable, as digital nails. Techno-solutionism and the logic that all life and the processes and problems within it are identifiable, understandable, and algorithmically fixable runs the risk of underrepresenting highly complex and nuanced situations with increased data collection, surveillance, and classification in all spheres. Biometrics and other forms of digital management of migrants and their lives do not appear to

[92] Kate Crawford, *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* (Yale University Press, 2021).
[93] Abraham Harold Maslow, *The Psychology of Science: A Reconnaissance* (Harper & Row, 1966).

offer greater autonomy and agency to their users, but instead reify existing power structures. As currently conceived and implemented, they represent the system from which they emerge, rather than a mutually improving system of governance that treats citizens and migrants alike with dignity and respect for fundamental rights.

Beyond potential violations of what, at least within the European Union, are largely considered basic digital rights, the practice of digitally othering migrants also has in-group implications. The terminology of “sandboxing,” “experimentation”, or “laboratories” points to a possible trajectory that both humanitarian organizations and civil rights groups warn against the use of digital technologies that monitor, track, and fix the other functions as a testing ground for deployment against the general population. One can posit a future scenario in which we, as citizens, are critical of our governments and therefore subjected to iris scanning, a technology initially tested on migrants. Consequently, we are now situated within an out-group context. Police and other security agencies have an inherent interest in digital technologies that aid in the tracking and apprehension of people of interest. The facial scanners tested and deemed suitable in refugee camps and fed by CCTV footage, or the voice recognition software applied to telephone surveillance, are attractive tools for law enforcement-the privacy implications, especially for the “collateral” data points collected, are immense. This highlights the slippery slope on which biometrics in humanitarianism operate, as well as the potential for “function creep” within and across domains. This includes the fear that data collected, and identities registered to ensure aid distribution will end up in the hands of law enforcement.

Given these risks, the digital othering of migrants is not a marginal issue, but a significant ethical, legal, and social challenge. The differential treatment of migrants in the digital realm reflects and reinforces existing power structures and inequalities, perpetuating their status as eternal outsiders. The increasing reliance on digital and biometric technologies in migration management, while often justified by security and efficiency concerns, raises profound questions about the balance between control and rights, as well as the broader implications for democratic governance and human dignity.

The further development and deployment of these technologies must therefore be accompanied by a cross-sectoral and indeed society-wide debate and consensus on the values that underpin them and how this may limit their scope. Failure to address concerns about the digital othering of vulnerable groups and the erosion of their rights could set a dangerous precedent for the rest of society. In this context, it is important to rethink the frameworks that govern the use of digital and especially biometric technologies, ensuring that they are in line with the EU Charter of Fundamental Rights and that they serve to empower both humanitarian organizations and those in need of their care, rather than further entrench the marginalization and non-belonging of migrants.

6. CONCLUSION

In conclusion, while technology is an integral part of everyday life and can undoubtedly play a role in improving the lives of migrants while enhancing the effectiveness of humanitarian assistance, new technological solutions must be implemented in a way that respects the autonomy, privacy and dignity of those affected by them. Humanitarian organizations have an opportunity to amplify their voices and advocate for their concerns to policymakers and developers, and to work with them to create systems that prioritize the protection of human rights and ensure that vulnerable groups are not treated as mere data points or experimental subjects, but as inherent and integral members of the global community, deserving of equal rights and respect.

7. REFERENCES

1. Achiume, E. Tendayi. ‘Digital Racial Borders’. *AJIL Unbound* 115 (2021): 333–38. https://doi.org/10.1017/aju.2021.52.
2. Barrinha, André, and G. Christou. ‘Speaking Sovereignty: The EU in the Cyber Domain’. *European Security* 31, no. 3 (3 July 2022): 356–76. https://doi.org/10.1080/09662839.2022.2102895.
3. Bellanova, Rocco, and Georgios Glouftsios. ‘Formatting European Security Integration through Database Interoperability’. *European Security* 31, no. 3 (3 July 2022): 454–74. https://doi.org/10.1080/09662839.2022.2101886.
4. Bigo, Didier, Engin F. Isin, and Evelyn Sharon Ruppert, eds. *Data Politics: Worlds, Subjects, Rights*. Routledge Studies in International Political Sociology. London ; New York: Routledge, Taylor & Francis Group, 2019.
5. Bradford, Anu. ‘Europe’s Digital Constitution’. *Va. J. Int’l L.* 64, no. 1 (2023): 1–69.
6. Broeders, Dennis. ‘The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants’. *International Sociology* 22, no. 1 (January 2007): 71–92. https://doi.org/10.1177/0268580907070126.
7. Brom, Frans W.A., and Michiel Besters. ‘“Greedy” Information Technology: The Digitalization of the European Migration Policy’. *European Journal of Migration and Law* 12, no. 4 (2010): 455–70. https://doi.org/10.1163/157181610X535782.
8. Brouwer, Jelmer, Maartje Van Der Woude, and Joanne Van Der Leun. ‘Framing Migration and the Process of Crimmigration: A Systematic Analysis of the Media Representation of Unauthorized Immigrants in the Netherlands’. *European Journal of Criminology* 14, no. 1 (January 2017): 100–119. https://doi.org/10.1177/1477370816640136.
9. Chouliaraki, Lilie, and Myria Georgiou. ‘The Digital Border: Mobility beyond Territorial and Symbolic Divides’. *European Journal of Communication* 34, no. 6 (December 2019): 594–605. https://doi.org/10.1177/0267323119886147.
10. Codagnone, C., G. Liva, L. Gunderson, G. Misuraca, and G. Rebesco. ‘Europe’s Digital Decade and Autonomy’. *Publication for the Committee on Industry, Research and Energy, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg*, 2021. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695465/IPOL_STU(2021)695465_EN.pdf.
11. Council Regulation (EC) No. 2725/2000 of 11 December 2000 Concerning the Establishment of ‘Eurodac’ for the Comparison of Fingerprints for the Effective Application of the Dublin Convention, Official Journal L 316 § (2000).
12. De Gregorio, Giovanni. *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*. Cambridge Studies in European Law and Policy. Cambridge: Cambridge university press, 2022.
13. De Gregorio, Giovanni, and Roxana Radu. ‘Digital Constitutionalism in the New Era of Internet Governance’. *International Journal of Law and Information Technology* 30, no. 1 (15 April 2022): 68–87. https://doi.org/10.1093/ijlit/eaac004.
14. Diener, Alexander C., and Joshua Hagen. *Borders: A Very Short Introduction*. New York: Oxford University Press, 2012.
15. D’Ignazio, Catherine, and Lauren F. Klein. *Data Feminism*. First MIT Press paperback edition. Cambridge, Massachusetts: The MIT Press, 2023.
16. eIDAS Expert Group, and European Commission. ‘European Digital Identity Wallet Architecture and Reference Framework, Version 1.1.0’. GitHub Pages, 2024. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/arf/.
17. European Parliamentary Research Service. ‘The EU’s Strategic Autonomy: Framework for Discussion and Possible Future Developments’. European Parliament, 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf.
18. European Union. ‘European Declaration on Digital Rights and Principles for the Digital Decade’, 2022. https://ec.europa.eu/newsroom/dae/redirection/document/94370.
19. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, L 119 Official Journal of the European Union. § (2016).
20. Giannopoulou, Alexandra. ‘Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity’. *Digital Society* 2, no. 2 (August 2023): 18. https://doi.org/10.1007/s44206-023-00049-z.
21. Glouftsios, Georgios. ‘Governing Border Security Infrastructures: Maintaining Large-Scale Information Systems’. *Security Dialogue* 52, no. 5 (October 2021): 452–70. https://doi.org/10.1177/0967010620957230.
22. Glouftsios, Georgios, and Anna Casaglia. ‘Epidermal Politics: Control, Violence and Dissent at the Biometric Border’. *Environment and Planning C: Politics and Space* 41, no. 3 (May 2023): 567–82. https://doi.org/10.1177/23996544221144872.
23. Goriunova, Olga. ‘Digital Subjects: An Introduction’. *Subjectivity* 12, no. 1 (March 2019): 1–11. https://doi.org/10.1057/s41286-018-00065-2.
24. Gregušová, Daniela, Zuzana Halásová, and Tomáš Peráček. ‘eIDAS Regulation and Its Impact on National Legislation: The Case of the Slovak Republic’. *Administrative Sciences* 12, no. 4 (6 December 2022): 187. https://doi.org/10.3390/admsci12040187.
25. Hölbl, Marko, Boštjan Kežmah, and Marko Kompara. ‘eIDAS Interoperability and Cross-Border Compliance Issues’. *Mathematics* 11, no. 2 (13 January 2023): 430. https://doi.org/10.3390/math11020430.

26. Hummel, Patrik, Matthias Braun, Max Tretter, and Peter Dabrock. 'Data Sovereignty: A Review'. *Big Data & Society* 8, no. 1 (January 2021): 205395172098201. https://doi.org/10.1177/2053951720982012.

27. Iliadis, Andrew, and Federica Russo. 'Critical Data Studies: An Introduction'. *Big Data & Society* 3, no. 2 (December 2016): 205395171667423. https://doi.org/10.1177/2053951716674238.

28. Josipovic, Ivan. 'Digitalising Asylum Procedures: The Legitimisation of Smartphone Data Extraction for Retrospective Border Control'. *Geopolitics*, 2 January 2024, 1–24. https://doi.org/10.1080/14650045.2023.2288162.

29. Kim, Jeongheon, Minji Choi, Chaehyeon Lee, Jongsoo Woo, and James Won-Ki Hong. 'Service Applicable Blockchain-Based Self-Sovereign Identity Management System'. In *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–5. Dubai, United Arab Emirates: IEEE, 2023. https://doi.org/10.1109/ICBC56567.2023.10174875.

30. Kloppenburg, Sanneke, and Irma Van Der Ploeg. 'Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences'. *Science as Culture* 29, no. 1 (2 January 2020): 57–76. https://doi.org/10.1080/09505431.2018.1519534.

31. Krichker, Dina. 'Making Sense of Borderscapes: Space, Imagination and Experience'. *Geopolitics* 26, no. 4 (5 July 2021): 1224–42. https://doi.org/10.1080/14650045.2019.1683542.

32. Kuster, Brigitta, and Vassilis S. Tsianos. 'How to Liquefy a Body on the Move: Eurodac and the Making of the European Digital Border'. In *EU Borders and Shifting Internal Security*, edited by Raphael Bossong and Helena Carrapico, 45–63. Cham: Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-17560-7_3.

33. Latonero, Mark, and Paula Kift. 'On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control'. *Social Media + Society* 4, no. 1 (January 2018): 205630511876443. https://doi.org/10.1177/2056305118764432.

34. Leese, Matthias, Simon Noori, and Stephan Scheel. 'Data Matters: The Politics and Practices of Digital Border and Migration Management'. *Geopolitics* 27, no. 1 (1 January 2022): 5–25. https://doi.org/10.1080/14650045.2021.1940538.

35. Lips, Silvia, Natalia Vinogradova, Robert Krimmer, and Dirk Draheim. 'Re-Shaping the EU Digital Identity Framework'. In *DG.O 2022: The 23rd Annual International Conference on Digital Government Research*, 13–21. Virtual Event Republic of Korea: ACM, 2022. https://doi.org/10.1145/3543434.3543652.

36. Mejias, Ulises A., and Nick Couldry. 'Datafication'. *Internet Policy Review* 8, no. 4 (29 November 2019). https://doi.org/10.14763/2019.4.1428.

37. Menzes Queiroz, Benedita. 'The Impact of EURODAC in EU Migration Law: The Era of Crimmigration?' *Market and Competition Law Review* iii, no. 1 (2019). https://ssrn.com/abstract=4239931.

38. Metcalfe, Philippa, and Lina Dencik. 'The Politics of Big Borders: Data (in)Justice and the Governance of Refugees'. *First Monday*, 1 April 2019. https://doi.org/10.5210/fm.v24i4.9934.

39. Mocanu, Stefan, Ana Maria Chiriac, Cosmin Popa, Radu Dobrescu, and Daniela Saru. 'Identification and Trust Techniques Compatible with eIDAS Regulation'. In *Security and Privacy in New Computing Environments*, edited by Jin Li, Zheli Liu, and Hao Peng, 284:656–65. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-21373-2_55.

40. Oliveira Martins, Bruno, Kristoffer Lidén, and Maria Gabrielsen Jumbert. 'Border Security and the Digitalisation of Sovereignty: Insights from EU Borderwork'. *European Security* 31, no. 3 (3 July 2022): 475–94. https://doi.org/10.1080/09662839.2022.2101884.

41. Orav, Anita. 'Recast Eurodac Regulation'. European Parliamentary Reaserch Service, June 2024. https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589808/EPRS_BRI(2016)589808_EN.pdf.

42. Ploeg, Ymkje Hilda, and Jason Pridmore. *Digitizing Identities: Doing Identity in a Networked World*. Routledge Studies in Science, Technology and Society 30. New York: Routledge, 2016.

43. Regina, Paola, and Emilio De Capitani. 'Digital Innovation and Migrants' Integration: Notes on EU Institutional and Legal Perspectives and Criticalities'. *Social Sciences* 11, no. 4 (23 March 2022): 144. https://doi.org/10.3390/socsci11040144.

44. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, L 1183 Official Journal of the European Union § (2024).

45. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, L 257 Official Journal of the European Union § (2014).

46. Roots, Lehte. 'The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination'. *Baltic Journal of European Studies* 5, no. 2 (1 October 2015): 108–29. https://doi.org/10.1515/bjes-2015-0016.

47. Ruckenstein, Minna. 'Visualized and Interacted Life: Personal Analytics and Engagements with Data Doubles'. *Societies* 4, no. 1 (18 February 2014): 68–84. https://doi.org/10.3390/soc4010068.

48. Sharif, Amir, Matteo Ranzi, Roberto Carbone, Giada Sciarretta, Francesco Antonio Marino, and Silvio Ranise. 'The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes'. *Applied Sciences* 12, no. 24 (10 December 2022): 12679. https://doi.org/10.3390/app122412679.

49. Sprokkereef, Annemarie. ‘Data Protection and the Use of Biometric Data in the EU’. In *The Future of Identity in the Information Society*, edited by Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, and Leonardo Martucci, 277–84. Boston, MA: Springer US, 2008. https://doi.org/10.1007/978-0-387-79026-8_19.

50. Turculet, Georgiana. ‘Data Feminism and Border Ethics: Power, Invisibility and Indeterminacy’. *Journal of Global Ethics* 19, no. 3 (2 September 2023): 323–34. https://doi.org/10.1080/17449626.2023.2278533.

51. Vavoula, Niovi. *Immigration and Privacy in the Law of the European Union: The Case of Information Systems*. Brill | Nijhoff, 2022. https://doi.org/10.1163/9789004356115.

52. Von Der Leyen, Ursula. State of the Union Address by President von der Leyen at the European Parliament Plenary, 16 September 2020.

53. Weigl, Linda, Alexandre Amard, Cristiano Codagnone, and Gilbert Fridgen. ‘The EU’s Digital Identity Policy: Tracing Policy Punctuations’. In *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*, 74–81. Guimarães Portugal: ACM, 2022. https://doi.org/10.1145/3560107.3560121.

INTERSOS

HUMANITARIAN AID

INTERSOS

Humanitarian Organisation

www.intersos.org