ASSEDEL, 11 Rue de Bruxelles 67000 Strasbourg, France, www.assedel.org,

info@assedel.org

March 2025

Policy Paper

by ASSEDEL

Digital Borders: The Impact of Technology on Migration and Refugee Rights in Europe

Introduction

The increasing reliance on digital technologies in migration management has transformed the European Union's approach to border control and asylum processing. Over the past two decades, governments and institutions across Europe have adopted digital tools such as biometric databases, automated decision-making systems, and artificial intelligence-powered surveillance to enhance efficiency, security, and coordination in migration governance. While these technologies present opportunities to streamline administrative processes, improve data collection, and strengthen security measures, they also introduce significant ethical, legal, and human rights challenges.

The digitization of migration control has evolved alongside broader security concerns, particularly following the 2015 migration crisis. As the EU faces rising asylum applications and irregular migration, policies have increasingly focused on **securitization and automation**, sometimes at the expense of fundamental rights. The **main argument** of this paper is that while digital tools have the potential to make migration processes more efficient, their implementation often prioritizes surveillance and exclusion over human rights and accessibility.

This study explores key digital migration systems, their impact on asylum seekers, and the challenges posed by AI-driven decisions, mass surveillance, and cybersecurity risks. It also examines alternative approaches that balance technological efficiency with ethical migration governance**.**

Biometric Data and Migration Control

The growing integration of biometric data collection, including fingerprint and facial recognition scanning, has become a key component of migration control. The use of databases such as Eurodac, the Schengen Information System (SIS), and the Entry-Exit System (EES) has reshaped the way migrants are identified and tracked across Europe. These databases facilitate border management, help prevent multiple asylum applications, and enhance verification processes. However, they also raise concerns about data privacy, informed consent, and potential misuse, particularly when migrants are compelled to provide biometric information under duress.

A 2023 report by the European Union Agency for Fundamental Rights (FRA) highlighted instances where **asylum seekers were forcibly fingerprinted in Greece and Hungary**, raising serious human rights concerns[1]. Furthermore, Eurodac's retention policies, which store asylum seekers' biometric data for up to 10 years, **blur the lines between migration control and criminalization**.

[1] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-fundamental-rights-report-2023_en.pdf

Artificial Intelligence and Automated Decision-Making

Another critical aspect of digital migration management is the increasing reliance on **artificial intelligence (AI) and algorithm-driven decision-making**. Some countries are employing AI to assess asylum applications, process visa applications, and detect fraudulent claims. While automation speeds up decision-making, it also introduces risks of **algorithmic bias, misinterpretation of refugee narratives, and reduced transparency**.

A 2021 study by the Refugee Studies Centre at the University of Oxford found that AI-driven asylum processing in Germany had an error rate of up to 20%**,** [2]leading to wrongful rejections and prolonged legal battles for asylum seekers**.** AI tools, often trained on **historical** data that reflect past biases, risk perpetuating discrimination against certain nationalities. Critics argue that these systems lack human oversight and fail to account for the complexities of forced migration, trauma, and persecution**.**

As an alternative, some experts advocate for **hybrid decision-making models**, where AI supports but does not replace human judgment in asylum determinations.

The Digital Divide and Barriers to Access

The digital divide further complicates migration policy by creating barriers to access for asylum seekers. Many migrants lack stable internet connections, digital devices, and the necessary digital literacy to navigate online asylum procedures. With some European countries transitioning toward digital-only applications for asylum and legal aid services, refugees who do not have access to online platforms face additional hurdles in seeking protection and legal representation.

According to a report by the International Telecommunication Union (ITU)**,** approximately 43% [3]of displaced persons in refugee camps in Europe have no reliable access to the internet, limiting their ability to apply for asylum or receive legal aid. Language barriers further exacerbate exclusion, as **most government portals are not available in Arabic, Pashto, or other refugee languages**.

Potential solutions include:

- Expanding **free WiFi** in refugee camps and asylum centers.
- Creating **multilingual digital platforms** tailored to the needs of migrants.
- Ensuring **offline alternatives** remain available for asylum applications.

Surveillance Technologies and Migration Control

In addition to data-driven migration systems, European governments are increasingly deploying surveillance technologies, such as facial recognition at border crossings, mobile phone tracking, and social media monitoring of migrants. While these tools are often framed

[2] https://www.rsc.ox.ac.uk/files/files-1/automating-immigration-and-asylum_afar_9-1-23.pdf
[3] https://www.unhcr.org/sites/default/files/legacy-pdf/5dc2e4734.pdf

as necessary for border security and migration control, they raise significant ethical concerns about mass surveillance, discriminatory profiling, and the criminalization of migration**.**

The European Union Agency Asylum organization has documented cases in which **predictive** analytics tools flagged individuals from war-torn regions as potential security threats without clear justification[4]. Additionally, in 2022, **the French government expanded real-time facial recognition use in public spaces**, a move criticized for disproportionately targeting migrant communities.

As a safeguard, legal frameworks such as the EU General Data Protection Regulation (GDPR) must be fully enforced to prevent misuse of migrant data**.**

Cybersecurity Risks in Migration Systems

The cybersecurity risks associated with digital migration policies cannot be overlooked. Large-scale migration databases store sensitive personal and biometric information, making them potential targets for hacking and data breaches.

In 2022, Europol reported a data breach in the Schengen Information System, where unauthorized access led to concerns over the exposure of asylum seekers' data. Additionally, data-sharing agreements between European states and non-EU countries have raised fears that personal information could be misused by regimes with poor human rights records.

Key recommendations to mitigate risks include:

- Implementing **stronger encryption** and **cybersecurity protocols** for migration databases.
- Establishing **independent oversight bodies** to audit data collection practices.
- Ensuring that **asylum seekers have the right to access and delete their data** when no longer needed.

Balancing Technology and Human Rights in Migration Policies

As the European Union continues to expand its digital migration policies, the balance between technological efficiency and fundamental human rights remains a critical concern. While digital tools can enhance border management and improve administrative processes, they must be implemented with strong legal safeguards to prevent rights violations**.**

Potential policy solutions include:

1. **Greater transparency** in digital migration systems, ensuring that AI decisions are explainable and challengeable.
2. **Stronger legal protections** for biometric and personal data, aligning digital migration policies with **human rights law**.

[4] https://euaa.europa.eu/sites/default/files/publications/2023-07/2023_Asylum_Report_EN_0.pdf

3. **Increased human oversight** in asylum decision-making to prevent unjust automated rejections.
4. **Ethical AI guidelines**, requiring fairness audits and accountability for migration-focused algorithms.

Conclusion

Ultimately, digital migration technologies should serve as tools for protection and inclusion rather than instruments of exclusion and control. While automation, biometrics, and AI-driven border security can enhance migration governance, their implementation must be guided by fundamental rights, transparency, and accountability**.**

As the EU continues to refine its digital migration framework, policymakers must prioritize human rights considerations to ensure that digital systems uphold the dignity, privacy, and legal rights of asylum seekers and refugees**.** The challenge remains: can digital transformation in migration be harnessed for efficiency while safeguarding the fundamental freedoms of those seeking protection?

By incorporating these solutions, digital borders can become an ethical migration tool rather than a barrier to asylum and humanitarian protection**.**