

UNIVERSITÀ DEGLI STUDI DI PADOVA

Department of Political Science, Law, and International Studies

Master's degree in European and Global Studies



“Digital migration: The use of digital technologies in border control
and surveillance in the European Union”

Supervisor: Prof. Guido Gorgoni

Candidate: Maria Analuz Piersanti

Matriculation No. 2085463

A.Y. 2024/2025

Abstract

The increasing use of digital technologies and artificial intelligence (AI) in the management of migration flows within the European Union has significantly transformed traditional notions of border control and surveillance. This thesis critically examines the deployment of biometric systems and other digital mechanisms, such as VIS, SIS, EES, ETIAS, Eurodac, and drones, assessing both their operational contributions and their inherent risks. Particular attention is given to the legal and ethical challenges that arise from such practices, with a focus on fundamental rights including human dignity, equality and non-discrimination, privacy and data protection, freedom of movement and the right to an effective remedy and fair trial.

Furthermore, the study addresses structural issues of accountability and transparency in the governance of migration technologies, and critically analyzes the existence of discriminatory practices and racism within European Union border management. Through a normative and critical legal methodology, this research explores whether the current regulatory frameworks adequately safeguard migrants' rights in the face of evolving technological landscapes.

Grounded in a comprehensive literature review and analysis of international, European, and national legal instruments, this thesis underscores the urgent need for a rights-based approach to digital migration governance. It concludes by proposing recommendations aimed at ensuring that technological innovation in migration management does not come at the expense of human rights, dignity, and social justice in the European context.

Acknowledgements

This thesis is the result of the support, guidance, and encouragement of many people and institutions. I would like to take a moment to express my deepest gratitude to all of them.

To my family, for being my unwavering support system throughout every step of this journey. Thank you for encouraging me to embark on this beautiful experience -not only of emigrating, but also of expanding my academic horizons-.

To my partner, Lucas -my confidant and faithful companion-. This final stage in Padova and the writing of this thesis would not have been the same without your presence and encouragement. Thank you for always being there, for your love, your endless patience, and the support.

To my friends -those from back home and those I met over these past three years in Padova-. A special thank you to those with whom I shared a home at Via Tre Garofani. What started as simple cohabitation evolved into a bond of deep friendship. You became fundamental pillars during this intense and often stressful, yet also joyful, period of my life. Thank you, Lu and Bruno, for being unwaveringly supportive. To all of you: thank you for making this chapter one of the most cherished in my life.

To my supervisor, Guido Gorgoni, for his trust, guidance, and dedication. Thank you especially for your patience throughout this process.

To the UNIPD community -students, professors, and staff- thank you for fostering an environment of academic excellence and intellectual growth. This journey has been transformative on both academic and personal levels.

Table of Contents

Abstract	1
Acknowledgements	2
Table of Contents	3
Introduction	5
Hypothesis	6
Research Questions	6
Objectives	7
Methodology	7
Chapter 1: The Foundations of Digital Migration and Border Control in the European Union	10
1.1 Introduction	10
1.2 Definition of Digital Migration and Short Literature Review	12
1.3 Brief Historical Context and Evolution of Border Control Technologies	15
1.3.1 Early Border Control Methods: From Ancient Walls to Modern States	17
1.3.2 The 20th Century: Wars, Migration, and the Evolution of Border Control	18
1.3.3 The Cold War: Borders as Ideological and Technological Frontiers	19
1.3.4 Post-9/11 Border Control: From Surveillance to Digital Biopolitics	20
1.3.5 21st- century technological advancements in border control	24
1.4 Datafication, Digitalization, and Securitization: Digital Borders and Migration Governance in the European Union	28
1.4.1 Datafication: Governing Migration Through Data	29
1.4.2 Securitization: Imagining Migration as a Threat	32
1.4.3 Digitalisation and the Transformation of Migration Governance	35
1.5 Concluding remarks	39
Chapter 2: Digital Migration and Border Control Technologies	41
2.1 Introduction	41
2.2 Biometric Systems	43
2.3 Automated Border Control (ABC) Systems	45
2.3.1 Facial Recognition Technology	47
2.3.2 Fingerprint Recognition	51
2.3.3 Iris Recognition	54
2.4 Surveillance Drones	56
2.5 SIS, Eurodac, VIS, EES, ETIAS	59
2.5.1 Schengen Information System	59
2.5.2 Eurodac	62
2.5.3 Visa Information System	63
2.5.4 Entry/Exit System	65
2.5.5 ETIAS	67
2.6 Concluding remarks	69
Chapter 3: Legal and Ethical Implications	71
3.1 Introduction	71
3.2 Framing the Human Rights dimension	73

3.2.1 Right to Human Dignity	75
3.2.2 Right to Asylum	76
3.2.3 Freedom of movement	79
3.2.4 Right to an Effective Remedy and Fair Trial	81
3.2.5 Prohibition of Torture and Inhuman or Degrading Treatment	83
3.3 Discriminatory Practices and Racism in European Union Border Management	86
3.4 Accountability and Transparency in Digital Migration Management	88
3.5 The evolving regulatory framework	92
3.6 Concluding remarks	96
Final Conclusion	98
Bibliography	103

Introduction

According to the United Nations High Commissioner for Refugees (UNHCR), more than 110 million people were forcibly displaced worldwide by the end of 2023, driven by war, violence, persecution, climate crises, and human rights violations. A significant portion of these movements has involved migration toward and within the European Union. In response, the European Union has progressively strengthened its border management strategies -often under the imperative of security- while increasingly turning to digital technologies to govern migration flows. Biometric databases, AI-based screening tools, predictive risk assessments, and automated surveillance systems now form a growing part of how Europe identifies, monitors, and controls those who cross its borders.

These technological advancements are often presented as neutral tools designed to improve efficiency, interoperability, and security. However, for migrants and asylum seekers, the experience of these systems is rarely so benign. The reliance on biometric registration, facial recognition, and algorithmic profiling not only reshapes how individuals are categorized and processed but can also expose them to significant risks: privacy violations, misidentification, limited access to legal remedies, and even systematic discrimination embedded in the technologies themselves. In many cases, people are subjected to invasive scrutiny without fully understanding how their data is collected, stored, or used -and with few avenues for contesting decisions made by opaque or automated processes-.

This thesis investigates the use of biometric and artificial intelligence technologies in the context of European Union border control, with a particular focus on their implications for migrants' fundamental rights. It seeks to analyze how these systems function as part of a broader digital infrastructure that governs mobility, and to what extent they challenge core principles of human dignity, equality, non-discrimination, and access to justice. Far from being merely technical instruments, these technologies operate within -and often reproduce- structural dynamics of exclusion, securitization, and racialized surveillance.

The first part of the thesis outlines the historical and conceptual foundations of digital migration. It examines the evolution of border technologies from analog documentation practices to today's data-driven, algorithmically managed systems, framing this trajectory within broader trends such as securitization and digital governance. The second part turns to a

critical analysis of the current systems in place -European Asylum Dactyloscopy Database (Eurodac), Visa Information System (VIS), Schengen Information System (SIS), European Entry/Exit System (EES), European Travel Information and Authorization System (ETIAS), and surveillance tools such as drones- unpacking how they operate and what risks they pose for migrants in practice. The final section explores the legal and ethical dimensions of these developments. It assesses the adequacy of existing European Union legal frameworks in safeguarding migrants' rights and interrogates the challenges posed by algorithmic opacity, bias, and a lack of transparency and accountability in digital decision-making.

This work is rooted in a critical perspective on the intersection between technology and migration policy, and it aims to contribute to the urgent conversation about the role of digital infrastructures in shaping who is allowed to move, under what conditions, and at what cost to their rights.

Hypothesis

This thesis hypothesizes that the development of biometric technologies and AI in the European Union border management disproportionately impacts migrants' fundamental rights, and that existing regulatory and legal frameworks are insufficient to effectively address the legal, ethical and structural challenges posed by these technologies.

Research Questions

The main research question that will guide this thesis is: *How does the use of biometric systems and AI in European Union border control affect the protection of migrants' fundamental rights?*

The sub-questions that complement the main one are: *What are the potential benefits and risks associated with the use of biometric and AI-based technologies in European Union border management?* To what extent do existing European Union legal frameworks safeguard migrants from right violations arising from digital surveillance and automation? In what ways do discriminatory practices and structural biases manifest in the design and deployment of these technologies?

Objectives

To address the research question, this thesis pursues the following objectives:

- To critically assess the operational advantages and drawbacks of these digital technologies in the management of migration flows.
- To examine the impact of these technologies on fundamental rights, including human dignity, privacy, equality and non-discrimination, asylum rights, and access to justice.
- To evaluate the adequacy of the current European Union legal and regulatory frameworks in protecting migrants' rights, and to identify existing gaps and challenges.
- To explore issues of discrimination, racism, opacity, and lack of accountability in the deployment and governance of digital border technologies.

Methodology

This thesis employs a qualitative research approach grounded in doctrinal legal methodology, complemented by critical legal analysis. The doctrinal component involves a systematic examination and interpretation of primary legal sources, including European Union regulations and directives relevant to migration and border control, as well as foundational human rights instruments such as the *Charter of Fundamental Rights of the European Union* and the *European Court of Human Rights (ECtHR)*.

The critical legal component engages with these sources to assess their effectiveness in safeguarding migrants' rights in the face of emerging digital technologies, while also questioning the structural assumptions and power dynamics embedded within European Union migration governance.

In addition to legal texts, the research draws on a range of secondary sources, including policy reports and opinions from institutions such as the *European Union Agency for Fundamental Rights (FRA)*, the *European Data Protection Supervisor (EDPS)*, and relevant

United Nations bodies. The analysis is further supported by recent academic literature on digital migration, surveillance technologies, data governance, and human rights law. Together, these sources provide a comprehensive foundation for evaluating both the normative frameworks and the real-world implications of biometric and AI technologies in European Union border management.

Structure of the Thesis

This thesis is organized into three chapters, each addressing a key dimension of the research question regarding the use of digital technologies and AI in European Union migration control and their legal and ethical implications.

The first chapter introduces the research topic by outlining the conceptual foundations of digital migration and tracing the historical development of border control technologies within the European Union. It begins by defining digital migration and exploring its implications for how mobility is governed, monitored, and regulated in a digital age. The chapter then provides a historical overview of border control technologies -from early state-building practices like passports and population registries to the emergence of large-scale biometric databases and predictive surveillance systems-. This foundational analysis situates current technological trends within broader processes of securitization, datafication, and algorithmic governance.

The second chapter offers a comprehensive analysis of the main biometric and digital systems currently employed in European Union border control, including Eurodac, VIS, SIS, EES, ETIAS, and the use of surveillance drones. It examines how these technologies function as part of an interconnected digital infrastructure for migration management, exploring both their operational contributions -such as increased efficiency and data sharing- and the broader legal, ethical, and social implications they raise. Special attention is given to the risks of algorithmic bias, discriminatory outcomes, and the externalization of borders, situating these developments within the European Union's evolving framework of digital surveillance and securitization.

The third chapter engages with the legal and ethical implications of the European Union's growing reliance on digital technologies and artificial intelligence in migration governance. It

critically analyzes the impact of these systems on fundamental rights, particularly regarding data protection, non-discrimination, and access to justice. The chapter addresses concerns related to algorithmic opacity, biometric surveillance, and the structural reproduction of racism and inequality within digital border infrastructures. Furthermore, it explores issues of transparency, accountability, and regulatory oversight, assessing both existing legal frameworks and the ethical challenges faced by researchers and policymakers in this rapidly evolving field.

Finally, the conclusion will present the final reflections arising from the analyses developed throughout the preceding chapters. It will especially emphasize the profound ways in which the use of digital technologies has reshaped the landscape of migration management, putting into question fundamental issues such as inequalities, exclusion and the erosion of established safeguards. By drawing attention to these tensions, the concluding chapter will underscore the urgency of addressing the legal, ethical and social implications posed by the increasing digitalization of borders and migration governance.

It will further synthesize the findings, discussing policy implications, and offer recommendations for a more rights-respecting approach to digital migration governance within the European Union.

Chapter 1: The Foundations of Digital Migration and Border Control in the European Union

1.1 Introduction

The increasing integration of digital technologies into migration governance has transformed how states -and particularly the European Union- conceptualize, monitor, and control human mobility. This shift reflects a broader transition from traditional border enforcement to digitally mediated forms of surveillance, identification, and prediction.

Modern technologies have significantly expanded the capacities of governments to gather and process data, increasing both the variety and the depth of governmental observation and monitoring. “The variety includes data from new technologies such as radar, infrared, and satellite technology (“the eye in the sky”), which enable different forms of observation and detection. Depth is added through technologies like information and communication technology (ICT), biometrics, geographic information systems (GIS), and statistical risk calculation. The more recent development of big data analytics is now also informing public policy making” (Broeders and Dijstelbloem, 2016, p. 1). As these authors point out, the State’s perception of reality becomes increasingly technologically and statistically mediated, or “datafied”. Data of various types and sources are processed, combined, and connected through networked databases. Although policymakers often claim that technology simply performs existing tasks more efficiently, it in fact changes both the substance and the nature of policy by introducing new actors and logics into governance processes.

The application of surveillance technologies and networked databases has been particularly prominent in the management of migration and international mobility. Migration is increasingly framed through the lens of security and risk, including concerns over terrorism, transnational crime, and violations of immigration law. This framing has justified the expansion of surveillance systems and databases aimed at visualizing, registering, mapping, monitoring, and profiling mobile populations (Broeders & Dijstelbloem, 2016, p. 2).

The historical development of these practices can be traced back to the institutionalization of identity documentation in modern state-building, exemplified by the invention of the passport and the spread of population registries (Caplan & Torpey, 2001). In Europe, the evolution of border control technologies accelerated following the Schengen Agreement and the

Maastricht Treaty, leading to the creation of large-scale databases such as SIS, Eurodac, and VIS (Brouwer, 2008; Shields, 2010). These systems were originally intended to enhance intergovernmental cooperation and streamline migration control, but they also laid the groundwork for the externalization of borders and a biometric logic of mobility management (Tazzioli, 2020).

In the 21st century, this infrastructure has expanded to include more complex and predictive forms of control, as will be examined in more detail in Chapter 2 of this thesis. Systems such as EES and ETIAS are designed to preemptively evaluate travelers and migrants through risk-based assessments. The integration of artificial intelligence into these systems raises serious concerns about transparency, accountability, and algorithmic bias, especially when decisions are made based on opaque criteria without effective channels for appeal (Latonero, 2018; Amoore, 2020).

Key debates in the scholarly and policy literature emphasize the securitization of migration through digital means, the erosion of privacy and data protection, and the risks of discrimination and exclusion -particularly for marginalized and vulnerable groups- (Trauttmansdorff, 2022; EPRS, 2022). Critics argue that digital infrastructures are not merely passive tools but active agents in the construction of borders, often reinforcing a logic of suspicion and deterrence (Tazzioli, 2020; Leurs, 2023). As Leurs (2023) notes, “a focus on platforms highlights the complex and shifting landscape of actors, networks, materials and ideas that stitch together places to make migration possible” (p. 32). This underscores the importance of considering the dynamic interactions between human and non-human actors that shape mobility.

Recent research also highlights the experiential and localized dimensions of digital migration. For instance, Lebon (2024) and the European Migration Network (2022) document how municipalities and civil society actors are grappling with the uneven effects of digital systems on migrant communities, especially those with limited digital literacy. Leurs (2023) emphasizes that for many migrants, digital borders are experienced as hostile and exclusionary infrastructures that hinder their ability to access services, understand legal procedures, or challenge automated decisions.

Advancements in the field of digital humanities have also contributed to the study of migration by providing analytical tools that allow researchers to trace migration patterns with

unprecedented depth and accuracy. These include word vector models, discourse-driven topic modeling, place name extraction, visualization techniques (e.g., "Flow toward Europe"), automated text recognition, network analysis, and genre detection. These methodological innovations offer new insights into the forces and dynamics shaping human movement (Viola, L., et. al., 2023, p. 1).

As Ponzanesi and Leurs (2022) point out, “digital migration practices, therefore, emerge as complex negotiations within the digital media sphere -situated between infrastructural bias and agential opportunities-. These practices challenge racialized regimes of control while also enabling digitally mediated bonds of solidarity and intimacy” (p. 103). Moreover, digital migration must be examined through critical lenses that include surveillance capitalism, extractive humanitarianism, datafication, and transnational choreographies of care.

Despite the growing body of critical research, participatory and rights-based frameworks for digital migration governance remain underdeveloped. The technocratic deployment of digital tools -often justified under the banner of “efficiency” or “innovation”- tends to marginalize migrant voices and democratic accountability (Amelung et al., 2020). This has led some scholars to call for a re-politicization of digital migration debates, where questions of ethics, justice, and inclusion take precedence over purely technical or managerial concerns (Amoore, 2020; Magnet, 2011).

1.2 Definition of Digital Migration and Short Literature Review

The increasing integration of digital technologies into migration governance has reshaped how states conceptualize, monitor, and control mobility. In this context, *digital migration* refers to the deployment of information and communication technologies (ICTs), biometrics, AI, databases, and algorithmic tools to manage, assess, and regulate migration flows (Latonero, 2018; Tazzioli, 2020). It encompasses a wide array of practices -from identity verification through fingerprinting and facial recognition to predictive analytics and automated risk profiling- that profoundly affect not only the movement of people but also their access to rights and legal protections.

At its core, digital migration represents the convergence of migration control with digital surveillance infrastructures. Scholars such as Lyon (2007) and Amoore (2020) argue that

these technologies do not merely enhance administrative efficiency but enact new forms of social sorting, control, and ethical tension. Within this broader surveillance paradigm, biometric and algorithmic systems are often normalized as neutral instruments of governance (Guild, 2009; Brouwer, 2008). Digital migration is therefore not only a technical development but also a political and ethical transformation of borders, citizenship, and state power (Magnet, 2011; Torpey, 2018).

From a theoretical perspective, digital migration must be situated within socio-technical frameworks. Amoore (2020) contends that algorithmic systems embedded in border regimes mediate ethical judgments, categorizing individuals as "risky" or "trustworthy". Similarly, Lyon (2007) frames surveillance as "social sorting" that reinforces power differentials. These technologies do not simply collect data, they shape legal outcomes and access to rights through datafied representations of individuals.

Expanding on this approach, Shields (2010) examines how the European Union's integration of ICTs into border surveillance has transformed the logic of control. Systems like Eurosur, SIS II, and VIS function as an interconnected architecture that pre-emptively categorizes individuals before their arrival and continues monitoring afterward. This paradigm of "pre-emptive security" reconfigures migration as a risk to be managed, raising serious concerns about agency, discrimination, and due process.

This dual logic of digital migration is further emphasized by Leurs and Ponzanesi (2018), who define the field as capturing "the expanding and intensifying roles digital technologies play in migration processes, ranging from top-down governmentality to bottom-up practices of everyday meaning-making" (p. 13). Migrants do not merely experience digital infrastructures passively -they also engage with digital tools to navigate, resist, and subvert control systems-. Latonero (2018) affirms that migrants increasingly face "digital borders" that mediate their access to services and mobility.

Meanwhile, concepts such as "e-diasporas," "migrant polymedia", and "information precarity" illustrate the active use of digital media by migrants, while darker notions like "digital deportability" and "networked authoritarianism" highlight the potential for surveillance, exclusion, and algorithmic discrimination. These frameworks illustrate how digital infrastructures can both empower and marginalize migrants, depending on the sociopolitical context (Leurs and Ponzanesi, 2018).

The literature on digital migration has grown significantly since the mid-2010s, partly in response to what Ponzanesi (2016) calls “the first refugee crisis of the digital age” (p. 19). Yet, despite this growing interest, there remains a lack of systematic study on how ICTs affect migrants’ everyday experiences, particularly within the European Union (Leurs & Ponzanesi, 2018). For instance, humanitarian apps like InfoAid¹ or RefAid² may assist migrants in accessing services, but also risk exposing users to surveillance or data breaches in weak regulatory environments.

Legal scholars such as Brouwer (2008) and Molnar (2020) have critically examined the implications of digital systems for fundamental rights. While the General Data Protection Regulation (GDPR) offers a legal framework for data protection, its enforcement within migration governance remains inconsistent. Nalbandian and Dreher (2022) emphasize that the implementation of advanced digital technologies (ADTs) raises significant privacy concerns and requires more robust accountability mechanisms.

Increased migration has driven both state and non-state actors to adopt emerging digital technologies. ADTs -defined as tools that harness digitization (conversion to digital format) and digitalization (enhancement of processes through digital tools)- have become central to migration management. These include AI, biometric recognition, GIS, and predictive analytics. While these technologies are promoted as increasing efficiency and streamlining procedures, they also introduce ethical, legal, and social risks (Nalbandian & Dreher, 2022).

Digital migration studies, as an interdisciplinary field, draw on media studies, migration studies, law, critical data studies, and science and technology studies (STS). Leurs and Smets (2018) note that the field reconfigures the borders of traditional academic domains, calling for a transdisciplinary approach. Scholars stress the importance of understanding how digital infrastructures both reflect and reproduce societal power dynamics.

Trauttmansdorff (2022) adds to this conversation by examining how border infrastructures mediate the relationship between technology and human movement. He writes that these infrastructures “host multiple encounters between technologies and the movements of people,

¹ InfoAid: Launched in Budapest during a major influx of migrants, the InfoAid app provided essential local information—such as train schedules and water safety—in multiple languages, with low-data access and a volunteer-staffed translation chat room; it has since inspired numerous similar apps across Europe (OIM, 2018).

² RefAid: It is a mobile application that shows migrants, refugees, and the social workers assisting them with which nearby services they can access, displayed on a map with a simple interface. The platform ensures that users’ information and location are completely confidential, not stored, and not shared with any authority or law enforcement body (Fundació iSocial, 2025).

who subvert, sabotage, escape, or appropriate them... [and] become tied to the construction of state or trans-national institutions” (p. 144).

In sum, digital migration refers not only to the tools used by states to manage mobility but also to the ways migrants themselves interact with digital systems in their search for safety, rights, and belonging. It spans a spectrum of practices, from smartphone use to algorithmic categorization at borders. This thesis builds on the existing literature to analyze how digital technologies are reshaping European Union migration governance, focusing on surveillance, privacy, rights, and the ethical stakes involved.

1.3 Brief Historical Context and Evolution of Border Control Technologies

Understanding the historical development of border control technologies is crucial to fully grasp the current landscape of digital migration management. These technologies have not emerged in isolation; rather, they are the product of a long evolution shaped by political, legal, technological, and social forces (Caplan and Torpey, 2001). Examining their historical trajectory illuminates how borders have progressively transformed, not only as physical demarcations but also as complex digital systems designed for surveillance, categorization, and control (Brouwer, 2008; Amoore, 2020).

Originally created to regulate trade and assert territorial sovereignty, border control practices have increasingly evolved into mechanisms for managing human mobility, frequently justified in the name of security. This shift is especially pronounced within the European Union, where the Schengen acquis has both abolished internal border checks and simultaneously strengthened external controls through advanced technological infrastructures. Systems such as SIS and Eurodac exemplify the transition from manual, document-based inspections to automated, data-driven monitoring frameworks (Brouwer, 2008).

This modern landscape is deeply embedded in a broader historical process that began with the state’s monopolization of legitimate movement. As Torpey (2018) explains, States have not always exercised full control over individuals’ movements, but over time they have gradually “monopolized the authority to restrict movement vis-à-vis other potential claimants, such as

private economic or religious entities,” which now largely operate “at the behest of states” (p. 6). Torpey further clarifies that:

...“States’ monopolization of the legitimate ‘means of movement’ is [not] a generalization valid for all times and places; the monopolization of this authority by states emerged only gradually after the medieval period in Europe and paralleled states’ monopolization of the legitimate use of violence” (p. 6).

The introduction of passports, visas, and other identification documents throughout the 19th and 20th centuries marked significant milestones in this process. These tools functioned as instruments of both inclusion and exclusion -granting access to some while denying it to others- based on bureaucratic categories such as nationality, race, and legal status (Caplan & Torpey, 2001).

Over the years, surveillance technologies have become central to the governance of mobility. David Lyon (2003) explains that:

“Surveillance happens to us all, every day, as we walk beneath street cameras, swipe cards, surf the Net. Agencies are using increasingly sophisticated computer systems -especially searchable databases- to keep tabs on us at home, work, and play. Once the word surveillance was reserved for police activities and intelligence gathering; now it is an unavoidable feature of everyday life” (p. 1).

Within migration and border control, this pervasive surveillance is far from neutral. Lyon (2003) argues that:

“Surveillance as Social Sorting proposes that surveillance is not simply a contemporary threat to individual freedoms, but that, more insidiously, it is a powerful means of creating and reinforcing long-term social differences. As practiced today, it is actually a form of social sorting -a means of verifying identities but also of assessing risks and assigning worth”- (p. 2).

This logic underpins the deployment of large-scale biometric and algorithmic systems at European borders. Lyon (2003) further notes:

“Everyday surveillance depends increasingly on searchable databases. Even where this is not yet or not fully the case -such as with the predominantly

human-operated CCTV systems- a central aim is social sorting. The surveillance system obtains personal and group data in order to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, access, and so on” (p. 20).

Today’s digital migration technologies -including biometric databases, predictive analytics, and integrated surveillance platforms- represent the latest phase in this ongoing history. However, as Brouwer (2008) cautions, the increasing sophistication of these tools must be accompanied by robust legal safeguards and human rights protections. Without effective remedies and transparent governance, digital borders risk becoming opaque, unaccountable mechanisms that reinforce exclusion instead of promoting justice.

1.3.1 Early Border Control Methods: From Ancient Walls to Modern States

The concept of border control is nearly as old as human civilization itself. Early societies recognized the need to manage who could enter or leave their territories, and although their technologies were rudimentary, their strategies laid the groundwork for today’s complex systems of migration governance. These early practices -ranging from physical fortifications to human surveillance- illustrate how borders have historically functioned as tools not only of security but of identity, control, and state-building.

During the medieval and Renaissance periods, border controls became more localized and fragmented. European feudal lords managed their own domains with toll booths, fortified castles, and watchtowers. Although national borders were virtually nonexistent at the time, the idea of regulating movement was already present through localized permits and checkpoints. As highlighted in *Border Control Evolution: From Historical Narratives to Cutting-Edge Initiatives*, these rudimentary practices reflect an evolving understanding of territoriality and the importance of access control (Topol, 2024).

This period also marked the early development of documentation practices that would later become integral to modern border control. Travelers often carried letters of passage or permits to cross through different territories. These documents foreshadowed the emergence of standardized passports and visas, tools that would later become central to state control over mobility (Topol, 2024).

For centuries, borders were managed using basic methods such as fortified walls, guard posts, and manual inspections. The Great Wall of China, perhaps history's most famous border defense, exemplifies how ancient societies relied on large-scale physical structures to deter invasions and control movement (Tashji, 2024).

The expansion of European colonial empires in the 16th and 17th centuries brought about a new logic of bordering -one deeply tied to the exercise of imperial domination-. Borders were not only geographic markers but also political instruments used to classify populations, regulate labor flows, and assert control over colonized subjects. According to Caplan and Torpey (2001), the documentation of identity -through permits, passes, and eventually passports- emerged as a crucial means by which states and empires sought to govern mobility.

The 19th century saw the rise of nation-states and the formalization of border control measures. Passport systems and immigration controls became standard, reflecting a growing emphasis on national security (Topol, 2024). At the same time, John Torpey (2018) famously describes this era as the period when states began to “monopolize the legitimate means of movement”, a process analogous to Max Weber's theory of the state's monopoly on violence. By requiring individuals to present authorized identity documents such as passports, the State asserted its exclusive authority over who could move, where, and under what conditions. This marked the formalization of mobility as a state-governed privilege, rather than a natural right (pp. 8-9).

This era also witnessed a rising tension between the goals of security and the principles of individual liberty. As David Lyon (2007) explains in *Surveillance Studies*, surveillance practices have long walked the line between ensuring public safety and infringing on personal freedoms. The industrial age introduced more bureaucratic and invasive methods of population management, which paved the way for modern surveillance infrastructures embedded in today's digital borders.

1.3.2 The 20th Century: Wars, Migration, and the Evolution of Border Control

During the mid-20th century, the role of technology in border control expanded significantly. Equipment initially designed for wartime -such as radar and sonar- was repurposed to monitor movements across land and sea. Surveillance cameras became a common feature in

heavily trafficked border areas, enabling constant observation without the need for direct human oversight. The Cold War period intensified this technological shift, with major powers like the United States and the Soviet Union implementing sophisticated sensor systems to track unauthorized crossings and prevent intrusions. These surveillance methods were often used alongside physical barriers, exemplified by the Berlin Wall, which fused tangible fortifications with state-of-the-art monitoring technology (Tashji, 2024).

Surveillance cameras also began to appear in high-traffic border areas, enabling continuous observation without requiring constant human presence. This marked the beginning of a new era in which technology enabled more remote and efficient forms of border management.

Passports, once simple letters of passage, evolved into standardized, bureaucratic tools of identification. They became central to the establishment of national identity and the regulation of cross-border movement. As Topol (2024) notes, “passport systems and immigration controls became standard, reflecting a growing emphasis on national security” (p. n/d). This shift was not only technological but also institutional, as governments increasingly relied on formal documentation to distinguish citizens from non-citizens and manage migration flows.

The turbulence of the 20th century -including two world wars, decolonization, and large-scale displacement- fundamentally reshaped global mobility. These historical forces contributed to the development of more stringent and technologically sophisticated border control systems, setting the stage for the digital infrastructures of the 21st century (Topol, 2024).

1.3.3 The Cold War: Borders as Ideological and Technological Frontiers

As David Lyon (2007) observes, modern surveillance systems emerged not only to detect threats but to produce legible, classifiable populations. Border control thus ceased to be solely about physical territory; it became increasingly concerned with knowledge, visibility, and risk management.

The development of information and communication technologies (ICTs) for mobility governance can be understood as a continuation of longstanding practices of “remote control”. Since the introduction of passports and immigration controls at the turn of the

nineteenth and twentieth centuries (Torpey, 2018), European governments have sought to extend their border enforcement capabilities beyond their immediate territories, projecting control extraterritorially.

A major milestone in this trajectory was the Schengen Agreement of 14 June 1985, which set the stage for the gradual abolition of identity checks at internal borders between participating states. This development was endorsed by the European Commission, which, in 1988, clarified its position regarding Schengen integration:

“In a separate but parallel and very relevant exercise the five Member States who signed the Schengen Agreement (France, Germany and the Benelux countries) have committed themselves to a process with the aim of abolishing identity controls of individuals at their common land borders. e Commission participates in the work of the Schengen Group which it finds invaluable in formulating its ideas in the wider Community context” (Brouwer, 2008, pp 22-23).

This shift marked a new phase in border governance, characterized by the outsourcing of control to digital and automated systems. In the 1980s, states began to introduce alphanumeric machine-readable passports (MRPs), which allowed for faster and more standardized identity verification. Airports soon adopted computerized entry-exit systems, facilitating the efficient monitoring of cross-border movement.

These innovations foreshadowed the broader digitalization of border security in the 21st century, where automation and data-driven technologies have become central tools of migration management (Broeders and Hampshire, 2013). However, as Tazzioli (2020) argues, these mechanisms also introduced new forms of exclusion. Migrants and asylum seekers are increasingly subjected to intensified surveillance and control -governed not by human officers, but by algorithms, biometric risk scores, and predictive analytics-.

1.3.4 Post-9/11 Border Control: From Surveillance to Digital Biopolitics

Looking at recent shifts in how global risks and security threats are understood -changes that have been significant since the 1970s- new views on societal vulnerabilities have emerged. Although transnational and cross-border crime have long been central to security policies, the

nature of criminal activities has evolved over time. The increased movement of migrants and travelers within and across the supposedly ‘borderless’ Schengen Area has been increasingly securitized and framed as a threat. Major terrorist attacks, such as those in the United States on September 11, 2001, Madrid on March 11, 2004, and London on July 7, 2005, have deeply impacted societies and security agencies, triggering a fundamental shift in security agendas. Political discourse now frequently employs terms like “illegal migration”, “transnational organized crime”, and “terrorism” as blame categories, which serve to justify harsh and sometimes extreme measures aimed at defending states and their populations against perceived threats. These risk categories have specifically contributed to the development and normalization of complex transnational cooperation among police and judicial bodies within the European Union, underpinned by sophisticated technologies using biometric data and extensive cross-border information exchange systems (Amelung et al., 2021, p. 17).

The terrorist attacks of September 11, 2001, marked a watershed moment in the global governance of borders. In the name of national security, governments began developing increasingly data-driven strategies to manage human mobility. This shift materialized most clearly in the expansion of surveillance, biometric identification, and the digital collection of personal data. As Broeders and Hampshire (2013) observe, post-9/11 developments significantly accelerated the deployment of high-tech border controls. Although securitisation may not always dominate political rhetoric, operational practices clearly reflect a counter-terrorism logic. Border infrastructure became increasingly digital and expansive, with the routine collection and repurposing of passenger data for security purposes. Systems originally designed for immigration enforcement were reoriented toward security, reflecting a blurring of boundaries between migration management and counter-terrorism.

The ICT sector played a pivotal role in this transformation. By 2004, the OECD (Organisation for Economic Co-operation and Development), identified a growing “homeland security market” in the European Union, illustrating how security concerns fed into economic and technological developments (Broeders & Hampshire, 2013). Yet, the dominant framing of digital borders as primarily security tools overshadows alternative drivers—such as efficiency, mobility facilitation, and the domestic politicisation of immigration—where governments adopt symbolic measures in response to public opinion or electoral pressure. As Broeders and Hampshire argue, it is important not to conflate

securitisation with politicisation, as the latter often emerges from mainstream party competition rather than extraordinary security discourse.

Torpey's *The Invention of the Passport* (2018) offers a broader historical lens, situating these contemporary developments within the long-standing state ambition to “monopolize the legitimate means of movement.” While states have always sought to regulate mobility, what distinguishes the post-9/11 period is the sophistication and ubiquity of digital controls. The evolution toward biometric databases and algorithmic risk assessments represents a new stage in the “statification of movement,” where access to mobility is increasingly mediated by technological systems.

The United States exemplified this shift through programs such as the Secure Border Initiative and the creation of “virtual fences” (Tashji, 2024), exporting a model of high-tech, anticipatory border control that has since influenced policies across Europe and beyond. These developments underscore how security, technology, and state power have become deeply intertwined in the digital governance of migration.

One of the most significant innovations in this period has been the widespread deployment of biometric identification technologies, including fingerprinting, facial recognition, and iris scans. These tools are often justified as enhancing security and efficiency, yet they also reflect deeper tensions around identity and exclusion (Brouwer, 2008; Magnet, 2011). As Magnet (2011) critically observes that human bodies are not “biometrifiable”. Moreover and despite massive investments based on the assumption that human bodies can be easily translated into biometric data, this premise is flawed. Biometric systems rely on the belief that the body is a fixed, stable source of identity information. However, these technologies often fail -mechanically, in their claim to objectivity, and in their limited understanding of the complex nature of identity-. Even when they malfunction, biometric systems still serve the interests of states and corporations invested in security and control. In this way, they succeed in reinforcing power structures, even as they fail technically. Conversely, when they do function, they can still cause harm -particularly to marginalized groups- by reinforcing exclusion and undermining democratic values. In this sense, they fail even in their apparent success (pp 2-3).

In the European Union, biometric surveillance has been institutionalized through systems such as Eurodac, which stores the fingerprints of asylum seekers, VIS and SIS, which catalog

the personal and biometric data of third-country nationals. These infrastructures, Brouwer (2008) argues, create "digital borders" that can exclude individuals even before they reach the physical frontier, often without clear legal recourse: "given the many shortcomings in relation to the protection of data and the inadequate remedies available to persons, according to the Member of the European Parliament, the current situation would fail to meet the level of protection required by the Charter of Fundamental Rights with potentially serious consequences for citizens" (p. 91).

As Lyon (2007) puts it, this marks a shift from "watching the dangerous" to "watching everyone," as all travelers become potential suspects. In the European context, similar systems are under development, such as ETIAS, which pre-screens visa-exempt travelers to the Schengen Area.

Focusing solely on spatial displacement overlooks the deeper biopolitical effects of contemporary border control. Migrants' movements are not only interrupted and diverted; they are subjected to exhaustion, temporal dislocation, and fragmentation. As Tazzioli (2020) highlights: "disruptive practices such as expulsions and deportations produce existential conditions of precariousness, restlessness and stuckness at the same time" (p. 126). Dispersal also serves to neutralise emerging political collectivities among migrants, undermining solidarity. This digital dispersal intensifies border control while rendering it more opaque, showing how both spatial and algorithmic strategies govern migrant subjectivities beyond physical boundaries.

Amelung et. al. (2021) suggests that following the events of 9/11, two distinct types of bordering became more prominent within the evolving technological frameworks of control and surveillance. First, there is "bordering in society". which is shaped and reinforced by social, cultural, and political divisions among different groups. Second, there are novel 'state practices of bordering' that strengthen state sovereignty over border management through new technologies, which operate not only at physical borders but also extend well beyond them (p. 18).

1.3.5 21st- century technological advancements in border control

In the 21st century, border control has undergone profound transformations due to technological innovation, particularly following the September 11 attacks. As national security concerns surged, governments accelerated the deployment of advanced surveillance, data processing, and biometric systems to monitor and regulate migration flows more effectively. These technologies are now central to what scholars and policymakers refer to as “smart borders” (Broeders and Hampshire, 2013).

According to Tashji (2024) argues, “nations began integrating real-time data collection with centralized systems, enabling more precise control over border activities. For example, radio-frequency identification (RFID) technology allowed vehicles and goods to cross borders faster while maintaining strict oversight” (p, n/d). While biometric passports and e-visa systems have streamlined travel for authorized travelers, they have simultaneously increased the difficulty for irregular migrants to circumvent border controls.

Integrated border management systems have become a cornerstone of European migration governance. The SIS, VIS and Eurodac enable data sharing among European Union Member States, allowing for real-time tracking of visa applicants, asylum seekers, and irregular migrants. Brouwer (2008) notes that these digital infrastructures raise pressing legal and ethical issues. The use of large-scale databases such as SIS II and Eurodac significantly affects the right to privacy and data protection, particularly when individuals are unaware they are being surveilled or cannot challenge erroneous entries.

Surveillance technologies are now embedded in the physical and digital landscapes of borders. Drones, satellite imaging, automated license plate readers, and motion-detecting smart fences are used to monitor border zones, especially remote or difficult-to-access areas. This convergence of military-grade tools with civilian oversight raises concerns about proportionality and accountability (Tashji, 2024). A key example of this is Eurosur, launched in December 2013, which integrates data from satellites, drones, and sensors to monitor irregular migration and criminal activity along the European Union’s external borders. As Tazzioli (2020) explains, Eurosur extends the European border “into the sea”, creating a mobile zone of surveillance that transcends national boundaries. This represents a shift toward a “remote” border control, where sovereignty is enacted through digital infrastructures and data flows rather than physical barriers (pp. 97-98).

These technological developments have also reshaped the internal dynamics of the European Union. The Schengen Area, which allows passport-free travel among 26 European countries, exemplifies regional integration. Yet, this freedom within has come at the cost of increased fortification without. Guild (2009) argues that the European Union's approach to external borders has evolved from a model of territorial defense to one focused on regulating access to rights and resources. Consequently, while borders may be porous for some, they remain rigid and exclusionary for others -especially asylum seekers and irregular migrants-.

Since the early 1990s, scholars have increasingly conceptualized state sovereignty as being exercised well beyond traditional national frontiers, referring to this phenomenon as "bordering". This approach has broadened the analytical scope to include a range of sites where border-related practices occur -both within the territory of the state and in external locations- often in the name of enhancing internal security, as exemplified by the European Union. It also calls attention to more subtle, everyday forms of governance -what some describe as "banal sites"- where bureaucratic and technological mechanisms such as biometric systems play a key role in shaping cross-border cooperation. These extended forms of bordering include not only physical border zones but also the involvement of professionals like security personnel and data analysts who engage in the operationalization of these practices (Amelung et al., 2021, p.18).

The COVID-19 pandemic further accelerated the digitalization of migration governance. New digital health surveillance and mobility-tracking systems were rapidly deployed, showcasing both the flexibility and risks of these infrastructures. As Tazzioli (2020) underscores, "governing migrant mobility through mobility is far from resulting in a less violent borders for the migrants themselves, as it has tangible and dramatic consequences on their lives: being kept on the move and forced to undertake convoluted and diverted routes, migrants are worn out and their material and legal terrain, their spaces of life, are repeatedly undercut" (p. 102). This reveals how forced mobility itself becomes a technique of control -exhausting, delaying, and displacing migrants as a form of discipline..

More broadly, contemporary border security now hinges on the integration of diverse digital technologies. Tashji (2024) notes that AI plays a pivotal role in this context, analyzing large volumes of data to detect irregularities in real-time. AI systems forecast migration patterns by monitoring geopolitical shifts, economic indicators, and environmental changes, enabling more strategic deployment of border resources. Machine learning is also employed to

automate the review of surveillance footage, identifying suspicious behavior and reducing reliance on human oversight. These systems are complemented by sophisticated analytics platforms that consolidate information from drones, sensors, and satellites, creating a comprehensive, real-time overview of border conditions.

Since the late 1990s, European Council policy documents have increasingly emphasized the importance of information exchange between police authorities across Member States. A significant step in this direction was the Treaty of Amsterdam (1997), which established the Area of Freedom, Security and Justice (AFSJ) as part of efforts to build a cohesive European Union approach to Justice and Home Affairs (JHA). Following this, initiatives such as the Tampere Programme (1999), the Hague Programme (2005), and the Stockholm Programme (2010) have shaped the European Union's internal security strategy, reinforcing the need for cross-border information sharing. The Tampere Programme introduced the concept of 'mutual recognition', aiming to foster cooperation and trust among Member States, even in the absence of harmonized legal or administrative frameworks. Building on this, the Hague Programme set forth the principle of 'availability', requiring Member States to grant one another access to relevant information.

These developments reflect a broader trend toward integrating national law enforcement efforts within a shared European security framework (Amelung et al., 2021, pp. 19-20). As a trust-building measure, the degree to which human rights should be protected was spelled out in the Stockholm Programme: "The protection of the rights of suspected and accused persons in criminal proceedings is a fundamental value of the Union, which is essential in order to maintain mutual trust between the Member States and public confidence in the Union" (European Commission, 2010, p. 10).

The different modalities of today's borders intervene in human mobility in complex ways. Even though borders are now "everywhere" there are still lines on the map that separate countries from each other and are patrolled by border guards (Broeders and Dijstelbloem, 2016).

In the Schengen Area, the elimination of internal border controls has shifted the focus to the shared external borders of the European Union. According to the European Parliament, the Schengen Area comprises 27 member states and serves as one of the world's largest areas of free movement, making effective management of its external borders critical for ensuring

security and cooperation. This zone includes roughly 50,000 km of external maritime boundaries and almost 9,000 km of land borders, alongside hundreds of official entry points (European Parliament, 2019). Unsurprisingly, guarding the border has increasingly become a technological affair. Much has been invested in new technologies of border surveillance, driven by both political aspirations to ‘control’ borders and by the “homeland security industry” to create and expand new markets for surveillance technology (Broeders and Dijstelbloem, 2016).

The European Union’s external borders are increasingly managed through a combination of traditional methods and advanced surveillance technologies. Along the eastern land borders, tools such as heartbeat and mobile carbon dioxide detectors are used to detect irregular migrants hidden in carriers or cargo. Also, border controls are supplemented by fixed and mobile document examination systems, CCTV, night vision equipment, thermal cameras and movement detectors. At the Mediterranean’s maritime frontier, the European Union -especially through Frontex and initiatives like EUROSUR- has expanded the use of drones, satellites, and data mining to transform the region into a digital barrier against unauthorized migration. Spain was an early adopter of such technologies, implementing the SIVE maritime surveillance system in 2002. This model later inspired broader European Union strategies, culminating in the 2008 “border package” which outlined a vision for integrated border management through databases, Frontex expansion, and satellite surveillance (Broeders and Dijstelbloem, 2016, p. 7).

In sum, the digitalization of border control in the European Union illustrates a significant transformation in the logic and mechanisms of state sovereignty. The integration of biometric technologies, predictive analytics, and large-scale data infrastructures into migration governance reflects not only a response to technical challenges but a deep-seated reaction to global anxieties and shifting notions of risk. These technologies enable the construction of borders as dynamic, adaptive, and deeply political systems -ones that govern not only who crosses, but who is counted, categorized, and controlled-.

1.4 Datafication, Digitalization, and Securitization: Digital Borders and Migration Governance in the European Union

The digital transformation of migration governance in the European Union is not merely a technological shift -it represents a profound reconfiguration of how mobility, identity, and belonging are conceptualized and managed-. This transformation is best understood through the intersecting dynamics of datafication, infrastructuring, and securitization, each of which exposes the socio-technical and political foundations of the European Union's border regime.

Technological surveillance and datafication have been the focus of extensive critique not only within academic scholarship but also through artistic exploration and intervention. Acting as canaries in a coal mine, artists have generated attention to the harms, hidden injustices, and ethical problems produced by networked surveillance technologies. The artistic interest in this topic expanded following 9/11 and the ensuing securitization period that emerged from the so-called "war on terror" (Wevers and Zhuparris, 2024, p. 89). In recent years, the emergence of biometric surveillance and predictive policing has prompted both artists and researchers to critically examine the algorithmic nature of surveillance and its broader socio-political consequences.

Within this context, it is crucial to distinguish between digitization, digitalization, and datafication. Digitization refers to converting analog materials (such as fingerprints or paper documents) into digital formats; digitalization involves the reorganization of processes and institutions through digital technologies; while datafication goes further, referring to the transformation of social life into quantified, machine-readable data used to inform decisions and automate governance (Witteborn, 2022; Taylor & Broeders, 2015). In migration management, this distinction is not merely semantic: it reflects different levels of abstraction and intervention into the lives of migrants and asylum seekers, and it underpins the creation of what Dijstelbloem (2021) calls borders as infrastructure.

This techno-political shift affects not only how migrants are monitored and registered but also how they are imagined -as data objects, risks, or anomalies within algorithmic systems-. Studies have shown that data-driven approaches to border control often involve opaque decision-making processes, raising questions of accountability, bias, and discrimination (Huysmans, 2006; Latonero, 2018; European Migration Network, 2022). The imaginaries driving digital migration governance are deeply intertwined with broader narratives of

security, efficiency, and technological progress, often sidelining the lived realities and rights of those subjected to these systems (Dijstelbloem, 2021).

As the European Commission's recent strategies show, the European Union is preparing its digital infrastructure not just to manage current migration flows but to preempt and predict future ones, reinforcing a mode of governance where abstraction replaces accountability, and technical efficiency overshadows legal and humanitarian obligations (European Commission, 2024). In this context,

“borders are no longer merely physical checkpoints or static infrastructures for organizing movement; they function as dynamic assemblages deeply entangled in the circulation and control of human mobility. Contemporary border control strategies are designed not only to block or filter entry but also to survey, monitor, and intervene in migratory trajectories well before individuals arrive at geopolitical frontiers. Through digital registration, biometric data collection, and algorithmic risk assessment, borders increasingly operate at a distance, tracking, profiling, and selecting individuals across time and space. They act beyond territorial lines, emerging wherever state authority, technological systems, and mobility intersect, thus reinforcing a regime of anticipatory governance and selective permeability” (Dijstelbloem, 2021, pp. 176-177).

1.4.1 Datafication: Governing Migration Through Data

In recent years, the concept of datafication has become increasingly central in migration research. Defined as the continuous extraction of data from everyday life -data that is then sold to third parties or used for algorithmic profiling, predictive analysis, and automated decision-making- datafication is often portrayed as a universal condition in our networked societies. However, as Nikunen and Valtonen (2024) emphasize, this process is not neutral. It disproportionately impacts racialized, poor, and mobile populations, thereby amplifying existing inequalities and vulnerabilities (p. 343).

In the realm of migration governance, datafication is more than a bureaucratic or technical shift; it is a fundamental instrument of power embedded in regimes of control, security, and surveillance. As Dijstelbloem (2021) and the European Commission (2024) argue, the

European Union's border management systems demonstrate how migrants are surveilled not only at the moment of border crossing, but also long before arrival and long after entry, through the use of predictive technologies, biometric databases, and interoperable information systems. This reflects a broader logic of pre-emptive governance.

Since 2007, the European Union has invested over €3 billion in border security research and infrastructure -especially in the aftermath of the 2015 refugee “crisis”- to expand and integrate large-scale data systems (Nikunen & Valtonen, 2024, p. 343). Key databases such as Eurodac (for asylum seekers’ fingerprints), VIS, SIS II, ETIAS, and EES are now being made interoperable through the Common Identity Repository (CIR), exemplifying a strategy that governs migration through data across borders, systems, and temporalities (EMN, 2022; Witteborn, 2022).

All these systems operate as *identity technologies*, organized around biometrics -typically fingerprints, iris scans, or facial recognition- as unique identifiers tying vast amounts of personal data to individual subjects. This logic turns categorisation into a prerequisite for governance, facilitating a pre-emptive view of migration. Two core trends emerge here: the shift from reactive to anticipatory databases and the technological mediation of categorisation. While traditional migration governance relied on nationality, visas, and country-of-origin assessments, current systems introduce risk-based filtering processes that distinguish between “trusted travellers” and those presumed to be of “bad faith.” Early European Union plans even used the problematic term “bona fide” travellers, revealing embedded biases in data-driven categorisation schemes (Broeders and Dijstelbloem, 2016, pp. 10-12).

Yet these digital systems are far from neutral. Eurodac, for instance, has been criticized for function creep, where data collected for asylum registration is repurposed for criminal investigations -raising serious concerns about legality and fundamental rights- (EMN, 2022). Similarly, the now-defunct iBorderCtrl project, which deployed AI-powered lie detectors and facial recognition at the border, was widely condemned for its pseudoscientific basis and discriminatory effects (Latonero, 2018). These examples underscore the risks of algorithmic migration governance and the urgent need for accountability. In this sense, the increasing reliance on digital technologies does more than manage borders; it transforms them, making data itself an instrument of exclusion and control.

As such, datafication becomes a form of *border violence* -one that is enacted not only through physical exclusion but also through algorithmic profiling and digital categorisation- (Huysmans, 2006). The implications of this datafied governance model extend to how individuals are made “legible” to the state. Tazzioli (2018) points out that the accelerated pace of automated identification eliminates the possibility of interpretation or negotiation, increasing the risk of error and injustice. These seemingly technical decisions can have life-altering consequences.

A growing body of scholarship thus contends that datafication is not merely about documenting pre-existing realities. As Scheel et al. (2019) argue, data practices are performative, they do not passively reflect migration flows but actively constitute and shape them. The assumption that migration data is “raw” or objective obscures the fact that it is always mediated by the instruments, ideas, and institutional agendas that produce it. Data, in this sense, are not neutral artefacts but fragile, contested, and deeply political constructs.

Scheel et al. (2019) challenge the ontological assumption underpinning most datafied governance frameworks -the belief that migration exists as an observable phenomenon "out there" that can be mapped and managed through increasingly sophisticated surveillance systems. Rather, they advocate for a performative understanding of data, one that recognizes how data not only represent but also produce realities in line with institutional power structures and market imperatives. As Gitelman (2013) points out, “raw data is an oxymoron,” reminding us that datafication is never merely a technical affair.

Building on this critique, Fill (2025) proposes a conceptual and methodological compass to analyze the “datafication of mobility” -understood as “the proliferation of data-driven mechanisms targeting people on the move and the reconfiguration of governance through digital means”- (p. 5). This viewpoint offers a valuable lens for examining the legal, political, and ethical shifts that shape today’s border regimes.

Ultimately, datafication reveals a broader shift toward predictive, automated, and abstract forms of migration control, where the logic of efficiency and risk replaces deliberation and rights-based governance. As scholars such as Bigo (2002) and Taylor & Broeders (2015) argue, this evolution signals not just a technological transformation, but a deeper political project—one in which digital infrastructures are not ancillary tools but central mechanisms of migration control and statecraft.

1.4.2 Securitization: Imagining Migration as a Threat

The evolution of digital systems in European migration governance cannot be separated from the broader process of securitization, in which migration is increasingly constructed as a threat to public order, national identity, and European sovereignty. As Bigo (2002) conceptualizes in his critique of the “governmentality of unease,” this framing facilitates the normalization of extraordinary surveillance practices, enabling the expansion of security infrastructures under the guise of necessity. Huysmans (2006) similarly argues that the politics of insecurity justifies a permanent state of exception, allowing technologies of control to be applied not only at the borders but also deep within society.

The sheer numbers of international mobility and the fast developments in modern surveillance technologies have changed the way states register, monitor, and deal with human mobility and migration. The nature of the border has changed drastically and is now “everywhere”, has become “virtual” or has shifted into a “border security continuum”. Many new technologies of visualisation, detection and registration have been added to the policy instruments that governments and international organizations use to manage human mobility at different stages of the migratory process (Broeders and Dijstelbloem, 2016, p. 3).

The securitization of migration has materialized through highly technological infrastructures that serve to detect, deter, and discipline mobility. A paradigmatic case is the EUROSUR surveillance system operated by Frontex, which integrates satellite imagery, drones, and maritime sensors to track “unauthorized movements” along the European Union’s external frontiers. Despite claims of humanitarian concern, EUROSUR’s primary function has been deterrence rather than rescue, prioritizing state control over migrant safety (Dijstelbloem, 2021). As Taylor and Broeders (2015) argue, such technologies do not merely increase efficiency, they entrench new forms of digital bordering that often exacerbate global inequalities.

This securitarian logic is further evident in the iBorderCtrl. Despite its scientific and ethical flaws, the project was justified on the basis of risk management and security enhancement, reflecting the instrumentalization of experimental technology in managing migration flows (Latonero, 2018). Similarly, the ETIAS system, which screens visa-exempt travelers using pre-travel risk assessments, can preemptively deny entry based on opaque algorithmic criteria

-an example of algorithmic border control where suspicion is automated and contestation is difficult- (Pelizza, 2019; EMN, 2022).

At the policy level, securitization is reinforced through documents like the European Commission's *Strategy Towards a Fully Functioning and Resilient Schengen Area* (2021), which emphasizes "internal security" as a cornerstone of European integration. Technological modernization is positioned as vital to safeguarding European Union citizens' mobility while controlling others. However, as Witteborn (2022) and Tazzioli (2020) point out, this dual regime creates an asymmetric distribution of mobility rights: while freedom of movement is guaranteed for European Union nationals, it is heavily restricted for migrants from the Global South, especially those racialized or undocumented.

These security regimes are not racially neutral. Technologies such as facial recognition and biometric registration -used in places like Melilla and Lampedusa- disproportionately target racialized bodies. Migrants from Africa, the Middle East, and South Asia are more likely to be registered, monitored, and subjected to coercive measures, illustrating how racialized surveillance is embedded in the logics of European border technologies. This echoes Bigo's (2002) idea that security operates not just through territorial control but also through the categorization of bodies and the production of "risky populations."

Infrastructures of migration control are also key to this securitization process. Borders have become infrastructural spaces -as argued by Dijstelbloem (2021)- where biometric data, interoperable databases, and predictive analytics create a dispersed yet powerful regime of governance. These infrastructures are not just neutral tools; they are political actors that enact and materialize the European Union's security priorities. The interoperability of systems like Eurodac, VIS, and SIS II, coordinated through the Common Identity Repository (CIR), is a clear example of how securitization is deeply entangled with technopolitical processes and datafication (EMN, 2022; Taylor & Broeders, 2015).

Approaching the datafication of mobility through an infrastructural lens entails moving beyond a purely technical view of digital systems and engaging with the material realities underpinning border and migration governance. This perspective, influenced by the so-called "materiality turn" in critical security and mobility studies, highlights how infrastructures-composed of institutions, bureaucracies, technologies, regulations, and protocols -actively shape security practices and political outcomes- (Fill, 2025, p. 15). These

infrastructures are not neutral or static; they embody power relations and contribute to the social and political construction of “securityness” around migration. Importantly, they consist of both digital and analogue components that operate in overlapping and sometimes contradictory ways, shaping mobility not just by collecting data, but by actively performing and enacting governance through that data. From this viewpoint, infrastructures become key analytical entry points, not only as physical or technical structures but as dynamic sites of governance and historical sedimentations of power.

By critically examining the infrastructures of datafied mobility -paying attention to access, impact, and disparities- researchers can address broader questions of mobility justice. This lens reveals how infrastructures redistribute rights and vulnerabilities, orchestrating differentiated conditions of movement across legal, physical, and digital layers. It exposes the stratified logic of mobility governance: who is allowed to move, under what circumstances, and with what degrees of freedom or constraint. As Fill (2025) and other scholars suggest, “bordering infrastructures can be seen as systems of ‘sorting out’ and ‘ordering’ alterity through mechanisms that become even more pervasive in the context of datafication” (p. 16). These systems not only process individuals but inscribe them into categories that determine their legitimacy, risk, or eligibility, reinforcing structural inequalities that are central to contemporary migration regimes.

In short, international mobility is deeply intertwined with global power relations, where surveillance operates as a mechanism of *social sorting* -classifying individuals to enable differential treatment-. This sorting can be driven by traditional tools like statistics or by newer digital surveillance systems, but the fundamental goal remains the same: to separate and manage populations based on perceived risk or utility. Surveillance technologies operate along a continuum between care and control, offering both protective and repressive functions depending on policy aims. However, the adoption of digital tools does not just implement policy, it actively transforms it. As Broeders and Dijstelbloem (2016) argue, the rise of risk calculation, algorithmic categorization, and interconnected databases has led to a shift from focusing on people to focusing on data and codes. Migration governance now often takes place in “centers of calculation” -labs, databanks, statistical agencies- where human movement is reduced to traces and documents. In this context, decisions about migrants are increasingly made not by diplomats or legal experts, but by data analysts and algorithm

managers, blurring the line between policy execution and technological design. Thus, digitization fundamentally reshapes the logic, tools, and actors of migration control.

With the digitization of migration policies and new technologies of visualisation, the very nature of policy implementation is transformed. The most significant decisions -such as determining who fits into which migration category- are increasingly made by a new class of policymakers: those managing algorithms and datasets rather than law and diplomacy. In this sense, digitization does not merely support existing policies; it reshapes them (Broeders and Dijstelbloem, 2016).

Ultimately, the securitization of migration through digital means represents a biopolitical strategy: it aims not only to regulate who can enter and stay, but also to categorize, control, and discipline mobile subjects through data, algorithms, and automated suspicion. As Huysmans (2006) warns, this approach risks undermining democratic norms and human rights by turning migration into a problem of security rather than one of justice, care, or solidarity.

1.4.3 Digitalisation and the Transformation of Migration Governance

Digitalisation, broadly understood, refers to “the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business” (EMN, 2022, p. 1). Within the context of migration management, this includes the transformation of asylum and border control systems through the integration of digital infrastructures. However, this shift is not purely technical -it is deeply political and strategic-. Scholars such as Taylor and Broeders (2015) highlight how digitalisation in migration governance intersects with development agendas and power structures, contributing to the datafication of mobility, particularly of people from the Global South. Data produced through surveillance, biometric registration, and predictive analytics is repurposed as both a tool of control and a source of economic and geopolitical value.

Witteborn (2022) identifies digitalisation as part of a broader “Three D” transformation -digitalisation, digitisation, and datafication- which reconfigures forced migration management from a humanitarian imperative into a technologically governed regime- (p. 157). This reconfiguration is not only about the tools deployed, but also about shifting

epistemologies of governance, where data and digital infrastructures increasingly mediate the very terms of legitimacy, risk, and deservingness.

At the institutional level, the European Commission's digital agenda emphasizes the future-oriented development of interoperable databases and smart borders, which are presented as solutions to enhance security and efficiency. However, as Bigo (2002) and Huysmans (2006) argue, the increasing use of technological tools in migration governance is not simply a matter of innovation or efficiency, it is embedded within a broader securitization framework in which migration is primarily perceived as a risk to be managed rather than a human right to be protected. As Bigo (2002) explains, migration as a national security problem derives from a global public discourse that "is the result of a continuum of threats and general unease in which many different actors exchange their fears and beliefs in the process of making a risky and dangerous society" (p. 63). This continuum contributes to a system where digital infrastructures serve not only to monitor borders but also to govern mobility preemptively, reinforcing the idea that migrants constitute a potential threat that must be identified and neutralized before arrival.

Recent scholarship further deepens the critique of digital migration governance by highlighting how digitalisation not only transforms border practices but also reshapes the very concept of sovereignty. Martins et al. (2022) argue that the European Union's effort to control its external borders "increasingly relies on digital systems: from tools for information gathering and surveillance to systems for communicating between different agencies and across Member States", making European Union borders a crucial site for the politics of *digital sovereignty*. These developments demonstrate "the expansion of techniques for governing migration," the "interoperability of European Union databases facilitating the internalisation of borders through domestic policing," and the "extra-territorialization of borderwork beyond the geographic limits of the European Union" (p. 475). In this sense, digital borderwork becomes not simply an act of securing territory, but a broader "enactment of territorial sovereignty that happens both within and beyond territorial lines" (p. 477). Moreover, digital infrastructures are not merely used to "count and oversee the movement of data subjects," but to reconfigure them, transforming migrants into governable entities through algorithmic systems. As they conclude, "data not only shapes our social relations, preferences and life chances, but our very democracies", fundamentally altering both the nature of state power and the subjects it governs (p. 485).

This reconceptualization of governance was further accelerated by the COVID-19 pandemic, which acted as a catalyst for the expansion of AI-based tracking systems, digital health surveillance, and remote registration tools. Real-time mobility data -collected through global dashboards, neighbourhood maps, and wearable technologies- became central to tracking the spread of the virus and regulating human movement. As McAuliffe et al., 2021 observe, “devices producing real-time data aimed to track and monitor the spread of the virus and subsequently the movement of people” became highly significant during the pandemic. This included “mobility monitoring platforms and wearable technology” used to inform “lockdown measures, border closures and other restrictions to movement”. In particular, mobility data at the pre-departure stage was used to “predict population movements, track the spread of the virus, and subsequently implement movement restrictions” (pp. 5-8).

Simultaneously, big data and AI were increasingly leveraged to manage and forecast mobility, with “experiments taking place at European Union borders... to predict population movements and inform automated decision-making in immigration applications”. As such, “big data is currently being leveraged to monitor migrants approaching the border”, and this trend is expected to grow, as “the ways in which big data analytics are being used to monitor movement at border points will continue to intensify” (McAuliffe et al., 2021). While “digitalization and AI are increasingly becoming a common feature of migration and mobility”, they also bring risks. Although these innovations promise to improve ‘migrants’ access to information and services throughout the Migration Cycle³”, their “over-reliance on these technologies... brings about significant challenges”, particularly concerning “the protection of migrants’ human rights” and “the effects on long-term migration trends and the implications for migration corridors”. These developments raise critical ethical and political questions about automation, transparency, and the future of data-driven mobility governance.

However, as Ponzanesi and Leurs (2022) remind us, digitalisation is not solely a top-down process. Migrants themselves actively engage with digital technologies to navigate asylum systems, maintain transnational ties, seek solidarity, and assert agency -even within hostile environments-. These digital tools can offer resilience, empowerment, and access to essential resources. Yet, the same infrastructures also reproduce and intensify existing inequalities, particularly through digital illiteracy, infrastructural limitations, language barriers and constant surveillance. These conditions contribute to digital exclusion and mistrust,

³ AI and the Migration Cycle: The increase in digital capture means that AI has been used throughout the Migration Cycle at all stages: pre-departure, entry, stay and return (see Figure 1) (McAuliffe et al., 2021, p. 3).

demonstrating that digitalisation is a contested and uneven field shaped by both control and resistance.

Complicating this landscape further is the growing involvement of non-state actors (NSAs) in digital migration governance, particularly through externalisation strategies in the Mediterranean. As Belaïd (2022) explains, NSAs -ranging from humanitarian organisations and private tech firms to actors involved in political destabilisation- are now “delegated by European states to exercise ‘remote border control’” (pp. 3-4). This delegation raises serious concerns about accountability and the erosion of state responsibility. Belaïd notes that their role “raises a lot of concerns about accountability for violations of human rights in the process”, particularly as “states remain the primary subjects of humanitarian law, although they have worked towards an externalisation and, to some extent, a privatisation of border operations”. Digitalisation further exacerbates these risks by “adding a layer of opacity,” which makes “the chain of decision-making beyond the level of human beings’ sole rationality more complex” (p. 4). In this increasingly opaque ecosystem of border governance, power and agency are redistributed in ways that often benefit unaccountable actors and undermine democratic oversight.

Finally, as Collins (2023) points out, technological developments in surveillance, biometrics, pre-screening, quarantine, tracing, and associated data collection, aggregation, and analysis have been evolving over several decades. These systems are often presented as neutral tools but are embedded in power structures that shape who is governed, how, and by whom. Within the emerging field of *digital migration studies*, there is a growing recognition of the need for “critical scrutiny of the conditions –political, socio-economic, historical, cultural, technological and ideological, through which migrants are produced as datafied subjects” (Collins, 2023, p. 739). In this context, Collins introduces the concept of *the digital migrant* to describe how AI and automation generate “digital traces that are rendered available to the government”, abstracting migrants from their lived experiences. These traces are not the individuals themselves, but abstract data representations that construct a “techno-centred fantasy of dividualisation, where migrants are endlessly split, reconstructed via data representations and technologies of control” (p. 739). This abstraction supports algorithmic systems of governance that seek to preconfigure migratory futures. As such, it calls into question the very politics and ethics of contemporary border regimes and urges scholars and

practitioners to rethink how solidarity with mobile people can be practiced under data-driven governance.

Therefore, the digitalisation of migration governance must be understood not only through institutional and technological lenses but also through its affective, relational, and lived dimensions. It is precisely in this ambivalence -between control and care, exclusion and agency- that the transformation of migration governance through digital means becomes most visible. Digitalisation is thus not a neutral or universally empowering process; it is a dynamic and stratified assemblage that simultaneously enables, restricts, and shapes the contours of human mobility in the 21st century.

1.5 Concluding remarks

The digitalization of migration governance within the European Union marks a fundamental transformation in the way mobility, identity, and security are conceptualized and operationalized. This chapter has traced the evolution of border control technologies from rudimentary historical practices to today's complex digital infrastructures. The shift from physical to digital borders does not merely reflect technological advancement, but a deeper reconfiguration of state power, where mobility is increasingly regulated through data, algorithms, and surveillance networks. With it, one of the most striking conclusions is that digital technologies do not simply enhance the efficiency of border management; they actively reshape the very logic of control.

What emerges is a border regime that functions beyond geographic boundaries, one that governs mobility remotely, anticipates movement before it occurs, and evaluates individuals through biometric markers and predictive risk assessments. The act of crossing a border is no longer confined to a single point in time or space; it is distributed across databases, sensors, and automated systems that collectively determine access, exclusion, and classification. In this context, borders are not static lines but dynamic and technopolitical infrastructures that embody evolving logics of control.

The chapter demonstrates that datafication -the process of turning human mobility into machine-readable data- has become the cornerstone of European Union border governance. This process introduces new layers of opacity and potential discrimination, as individuals are

translated into algorithmic profiles and risk categories within systems that are often difficult to scrutinize, challenge, or understand. At the same time, this digital architecture is intimately tied to the broader process of securitisation, whereby migration is framed not merely as a policy issue but as a security threat. This framing justifies extraordinary technological measures, expands surveillance, and legitimizes the use of automated decision-making in contexts once governed by human discretion and legal protections.

Digitalisation thus reshapes not only how borders function but also how sovereignty, citizenship, and even humanitarian governance are redefined through algorithmic and infrastructural interventions. These shifts reflect not just operational changes but deeper transformations in how the state enacts control, defines inclusion and exclusion, and assigns legal and moral worth.

Ultimately, the digital turn in border control demands critical reflection. It is not enough to assess technological innovation solely in terms of functionality or policy efficiency. One must also examine the broader ethical, political, and social implications of digital infrastructures -how they shape notions of citizenship, belonging, and human worth-. Crucially, the digital transformation of border management in the European Union should not be viewed as a neutral or purely technical evolution; rather, it represents a profound reconfiguration of sovereignty, legality, and subjectivity. As this thesis will further explore, the future of migration governance in the European Union must balance innovation with accountability, security with justice, and efficiency with humanity. Only then can a more inclusive and equitable approach to mobility be imagined and realized.

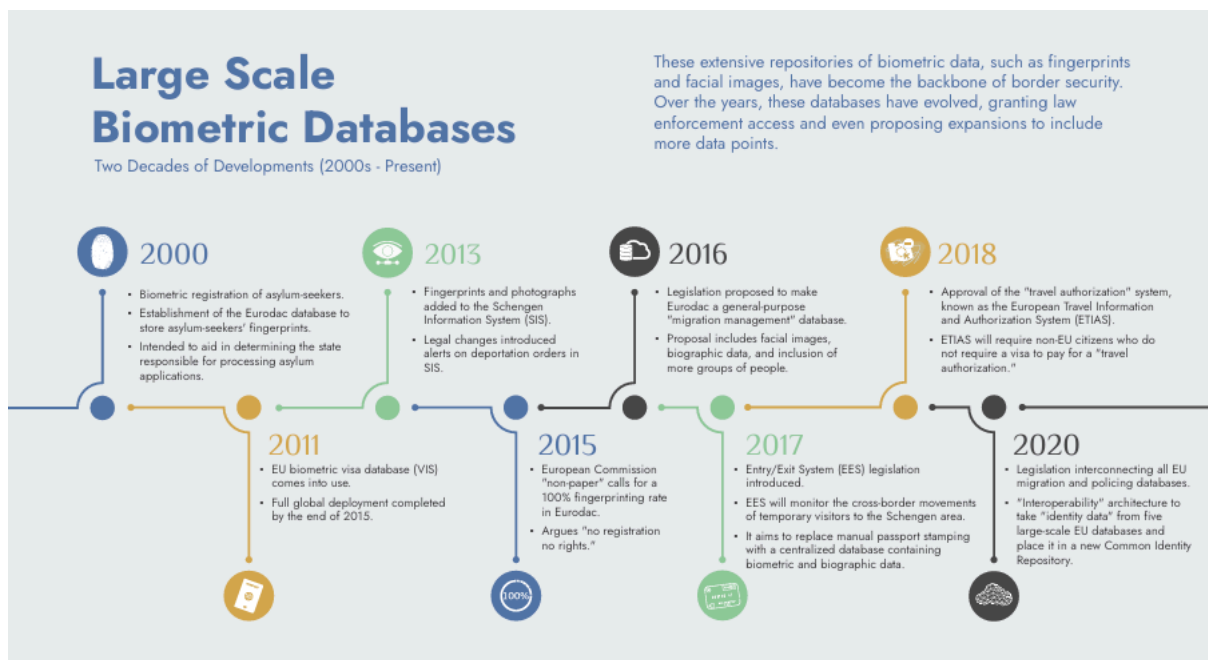
Chapter 2: Digital Migration and Border Control Technologies

2.1 Introduction

Over the last two decades, the use of digital technologies to manage migration at the European Union's borders has become a significant area of debate and transformation. As migration flows rise and the globalized movement of people becomes more complex, the European Union has increasingly turned to cutting-edge digital tools to enhance border security, improve efficiency, and manage migration more effectively (Bellio et. al., 2024)

In this sense, as illustrated in the diagram below, the European Union has developed several centralized databases, including Eurodac, the European Asylum Dactyloscopy Database, which stores fingerprints of asylum seekers; VIS, the Visa Information System, which tracks short-stay visas; SIS, the Schengen Information System, which shares information about wanted persons and stolen property; and EES, the Entry/Exit System, which records the entry and exit of third-country nationals; and ETIAS, the European Travel Information and Authorisation System, which is the new travel authorisation requirement for nationals of 59 visa-exempt countries and territories around the world (eu-LISA, 2025). These systems, built a highly sophisticated and interconnected system designed to track and monitor the movement of individuals across borders, creating digital traces through biometric data and real-time surveillance and enhancing the overall effectiveness of border controls (European Artificial Intelligence & Society Fund, 2023).

Image N° 1: Large scale biometric databases



Source: European Artificial Intelligence & Society Fund, 2023

Biometrics, dataveillance, and automation are key categories for understanding the evolving nature of borders in the digital age. Their application is neither abstract nor uniform, but shaped by national priorities, technological capabilities, and political imperatives. As Everuss (2024) notes, the "smart border" paradigm embodies not just technical efficiency but also a "techno-sovereign" logic that redefines who can move and under what conditions. Across entry points, automated border control systems, biometric gates, and predictive algorithms create variable regimes of inclusion and exclusion.

Biometric systems in particular have become dominant tools for identity verification and risk profiling. Technologies such as facial recognition, iris scanning, and gait analysis are increasingly employed by both national and supranational actors to trace migratory routes and verify legal status (Jain et al., 2004; Kaya, 2023). While these tools are often presented as accurate and impartial, empirical studies have shown that error rates are significantly higher among marginalized and racialized groups, raising concerns about algorithmic bias and discriminatory practices (Amnesty International, 2024; Leslie, 2020).

Moreover, the European Union's reliance on these technologies is tightly interwoven with broader political agendas on security, migration deterrence, and externalization. As Broeders

(2007) observed in the early years of biometric governance, digital borders “extend beyond the territorial frontier” and operate through interconnected databases that condition migrants' legal trajectories before they ever arrive on European soil. This logic has intensified with the proliferation of AI-based risk analysis systems such as ETIAS and the increasing use of surveillance drones and predictive profiling tools (Csernaton, 2018; Bellanova & Glouftsis, 2020).

Recent research has further emphasized that border technologies are not neutral tools but embedded within infrastructural and institutional politics. Dijstelbloem (2021) conceptualizes borders as infrastructures, meaning that technological systems -including sensors, databases, and biometric gates- do not simply reflect political decisions but shape them. In this view, the implementation of digital technologies constitutes a form of governance that is spatially diffuse and often legally ambiguous, especially when deployed at external borders or in collaboration with third countries.

This chapter explores the integration of digital technologies in migration management and border control, examining their implications for surveillance, security, and human rights. It delves into the operation of biometric systems, including facial recognition, fingerprint scanning, and iris recognition, highlighting their role in identifying individuals and regulating cross-border movements. Additionally, the chapter analyzes Automated Border Control (ABC) systems and their impact on efficiency and privacy. The discussion extends to the deployment of surveillance drones, large-scale European databases such as SIS, Eurodac, VIS, EES, and ETIAS, and assesses the broader architecture of digital migration governance. By critically evaluating the technological advancements and their societal consequences, this section aims to provide a comprehensive understanding of how migration is increasingly governed through algorithmic infrastructures and biometric control.

2.2 Biometric Systems

Biometric systems are automated methods for recognizing individuals based on their physiological or behavioral characteristics. These systems rely on unique biological traits such as fingerprints, facial features, iris patterns, and voice recognition to authenticate or identify individuals (Jain et al., 2004). The implementation of biometric technologies has significantly advanced over the past decades, driven by the need for enhanced security,

efficiency, and accuracy in identity verification processes. From civilian applications, such as unlocking smartphones and secure banking transactions, to large-scale governmental implementations, biometric systems have become central to contemporary identity management (Jain et al., 2004).

Biometric systems adapt their operational mode based on the application's specific requirements, functioning either in verification or identification. In verification, the system authenticates an individual's claimed identity by performing a direct comparison between the acquired biometric data and the corresponding template stored within its database. Typically, this process involves the individual providing a form of identification, such as a PIN or username, prompting the system to conduct a one-to-one match, e.g. "Does this biometric data belong to Bob?".

Conversely, identification mode involves the system recognizing an individual by conducting a comprehensive search across all stored templates within its database. This one-to-many comparison aims to determine the individual's identity, or to indicate that the individual's data is not present within the system, without requiring a prior identity claim, e.g. "whose biometrics data is this?". Identification is particularly vital in scenarios demanding negative recognition, where the system's objective is to ascertain whether an individual is falsely denying a particular identity (Guennouni et al., 2019).

Biometric identifiers, including fingerprints, facial recognition, and iris scans, have become an essential component of the European Union's approach to border control and migration management. Initially proposed by the European Commission in 2011, biometric-based "Smart Borders" were designed to distinguish "low-risk" travelers from those deemed a potential security concern, while also streamlining the identification and deportation of irregular migrants. This initiative has emerged alongside a rapidly growing biometric industry focused on developing technological solutions for government systems, such as national ID programs, electronic passports, and other mobility-related security measures (Stenum, 2017).

The intersection between biometric systems and migration is particularly evident in the concept of digital migration, which refers to the use of advanced technologies to monitor, control, and manage cross-border movements. Digital migration encompasses a range of surveillance mechanisms, including biometric data collection at border crossings,

AI-powered risk assessments, and interoperability between national and international databases (Jain et al., 2004).

Therefore, if we want to examine the consequences of biometric technology in migration management we have to put the focus in the perspective of the irregular migration. While possessing official identification has always been vital for border crossings, migrants frequently traverse borders using fraudulent or no documentation. However, within the European Union, many migrants who become undocumented initially entered legally, later overstaying or violating their residency terms. Consequently, documented identity becomes a critical tool for these individuals, both to mitigate the risk of deportation and to access essential services. Acquiring a plausible identity, for example, for health insurance, can offer protection during police checks. Furthermore, it can provide access to spaces restricted to legal residents, such as workplaces or educational institutions. This necessity fosters a practice of “flexible identities” among irregular migrants, adapting to their precarious circumstances (Stenum, 2017).

2.3 Automated Border Control (ABC) Systems

Commonly known as e-Gates, are fully or semi-automated systems designed to verify the identity of travelers crossing international borders, aiming to increase passenger throughput without compromising security or comfort. Essentially, ABC e-Gates automate the border crossing procedure, streamlining the verification of travel documents, traveler identity, and travel authorization. Consequently, these systems are becoming increasingly prevalent at international border crossing points (BCPs) to manage the growing volume of global travel (Frontex, 2012).

According to (Labati et al., 2015), an ABC e-Gate typically encompasses several core components. Firstly, it includes an electronic passport reader to authenticate the travel document, primarily e-Passports. Secondly, it incorporates biometric readers, primarily facial and fingerprint recognition systems, to verify the traveler's identity against the data stored in the document. Thirdly, it features an electronic door to control passenger flow. Finally, it includes a display device to provide visual instructions to guide the traveler through the process.

Indeed, the automated border check process commences with the traveler inserting their e-Passport into the reader. Subsequently, the reader verifies the document's authenticity by checking optical security features, extracting data from the Machine Readable Zone (MRZ), and communicating with the e-Passport chip. Following document verification, a live facial image of the traveler is captured and compared with the image stored on the chip. In some implementations, fingerprint verification is also conducted as an additional biometric identifier (Frontex, 2012).

Furthermore, ABC systems utilize four key subsystems to execute the necessary verification steps. Firstly, the Document Authentication System (DAS) validates the travel document. Secondly, the Biometric Verification System (BVS) captures and compares live biometric samples. Thirdly, the Central Systems Interface (CSI) facilitates communication with external databases. Finally, the Border Guard Maintenance System (BGMS) enables border guards to monitor and manage the ABC system (Donida Labati et al., 2015).

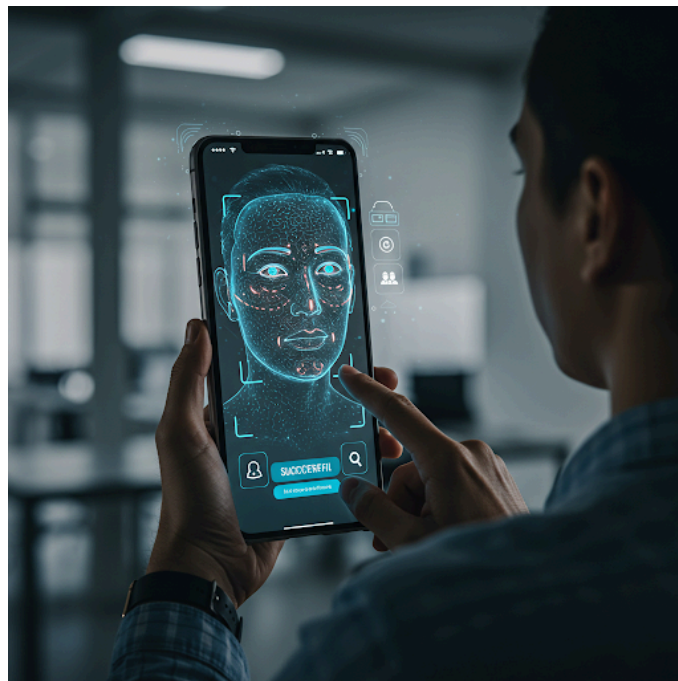
At the same time, ABC systems interface with external systems to verify travel authorization. Specifically, they connect to the Visa Management System (VMS), the Registered Traveler Program (RTP), and the Entry-Exit Management System (EEMS). The EEMS, in particular, plays a crucial role in migration management by tracking traveler movements, detecting overstays, and collecting statistical data. Moreover, ABC systems can operate through three procedural models: one-step, integrated two-step, and segregated two-step. In a one-step process, all verifications occur simultaneously within the e-Gate. In an integrated two-step process, document validity is checked before identity and authorization verification. In a segregated two-step process, verifications can occur at different times and locations (Donida Labati et al., 2015).

The evolution of ABC systems faces several key challenges, in this sense, highlight several challenges and negative aspects associated with their implementation. Some key concerns include accuracy limitations, as facial recognition systems may struggle with variations in lighting, pose, and facial expressions, potentially leading to false rejections or acceptances. Privacy concerns are also emphasized, as the widespread use of biometric data raises ethical and legal questions regarding data security and surveillance. Additionally, the authors discuss operational inefficiencies, noting that factors such as system delays, user errors, and environmental conditions can impact the effectiveness of ABC e-gates. Lastly, regulatory inconsistencies across different jurisdictions pose challenges for standardization and

interoperability, making it difficult to implement a universally effective system (Donida Labati et al., 2015).

2.3.1 Facial Recognition Technology

According to Umoren et al., (2021), facial recognition technology (FRT) is a biometric method that identifies or verifies an individual's identity by analyzing facial features from digital images or video frames. Essentially, FRT systems work by pinpointing and measuring unique facial characteristics, then comparing these measurements against a database of known faces. Specifically, it leverages automated processes to identify individuals based on distinct physical attributes, like facial features, much like fingerprint or voice recognition.

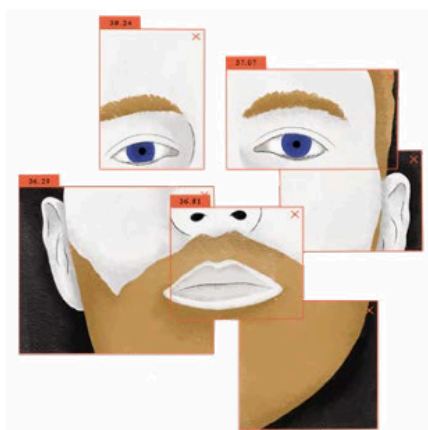


Facial recognition technology has evolved significantly over the decades, transitioning from early manual methods to sophisticated AI-driven systems. In the 1960s, researchers like Woody Bledsoe pioneered semi-automated systems that required human input to identify facial features. By the 1980s and 1990s, mathematical approaches such as Eigenfaces revolutionized the field, allowing computers to recognize faces more efficiently using

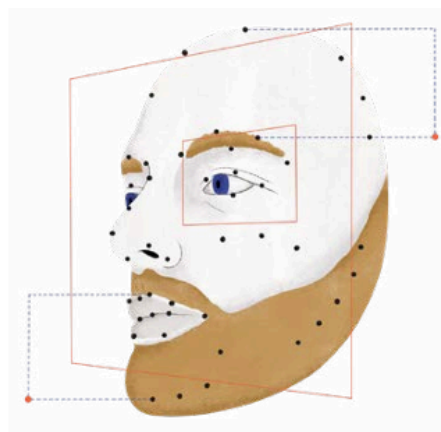
principal component analysis. The early 2000s saw facial recognition enter mainstream applications, particularly in security and law enforcement (Facit, 2024).

In recent years, deep learning and neural networks have propelled facial recognition to new heights, enabling real-time identification with remarkable accuracy. Facial recognition technology has evolved significantly in the 21st century, particularly with the integration of artificial intelligence and deep learning. A major milestone came in 2014 with Facebook's DeepFace, which utilizes a deep learning neural network to identify faces with near-human accuracy. The system processes images through multiple stages, including preprocessing for standardization, feature extraction using convolutional neural networks (CNNs) to capture key facial characteristics, and feature comparison via cosine similarity to determine matches. DeepFace's ability to convert facial images into high-dimensional feature vectors has enabled large-scale face recognition, dramatically improving precision in facial identification and verification (Qinjun et al., 2023).

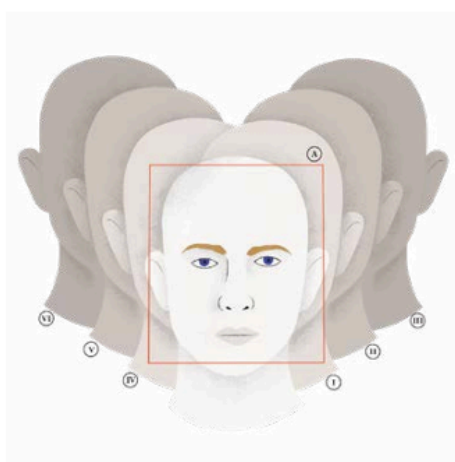
Following the overview of the historical evolution of facial recognition technology, the next section delves into the technical functioning of the recognition process itself. In this context, facial recognition technology follows a structured process involving several key steps, starting with data acquisition, where facial images are captured using cameras designed for 2D, 3D, or thermal imaging. These images can come from surveillance footage, smartphone cameras, or specialized facial recognition devices. Once the image is acquired, the system identifies and detects human faces within it using advanced algorithms that analyze structural elements, colors, and facial shapes. After detection, the next step is feature extraction or face alignment, where unique facial characteristics -such as the distance between the eyes, nose width, and jawline shape- are measured and converted into numerical data. Different systems may focus on either holistic facial features or specific localized elements, depending on their methodology (Qinjun et. al., 2023).



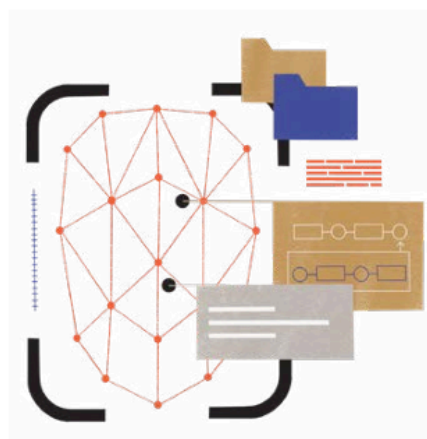
FACE DETECTION



FACE ALIGNMENT



FACE REPRESENTATION



FACE MATCHING

The final stage in the process is matching, where the extracted facial features are compared with stored data in a database. Identification mode searches for potential matches among all stored faces, while verification mode confirms an individual's identity by cross-checking their facial data against previously saved images (International Network of Civil Liberties Organization, 2024).

Facial recognition involves a combination of sophisticated techniques and technologies. Although the core steps -data acquisition, face detection, feature extraction, and matching- form the foundation of all facial recognition systems, the way these steps are implemented can vary significantly. This variation not only affects the system's performance but also plays a crucial role in determining its accuracy and reliability. However, it is important to note, the accuracy of FRT systems is contingent on several factors. Indeed, the reliability of FRT is

determined by algorithmic factors, including the algorithm's design, sophistication, sensitivity to false positives, and the quality of the training data. Moreover, physical conditions like lighting, image quality, and camera motion significantly impact performance. Additionally, individual characteristics, such as age, facial expressions, or hairstyles, can also affect accuracy. These limitations highlight a key disadvantage: the potential for inaccuracies and biases (Santamaria, 2021).

Taking into account the historical process, facial recognition technology has evolved significantly, offering both advantages in security and convenience, but also presenting significant ethical and privacy challenges. Its future development and deployment require careful consideration of these factors, alongside robust regulatory frameworks (Donida Labati et al., 2015). Basing the decision to implement facial recognition technology (FRT) in policing solely on its claimed accuracy fails to acknowledge the broader complexities surrounding its use and the profound implications for fundamental human rights. Even if FRT systems operated with absolute precision, their deployment would still pose serious risks, potentially eroding anonymity, treating individuals as easily trackable entities, and shifting the balance of power in police–civilian interactions further in favor of law enforcement. The consequences extend far beyond technical reliability, necessitating a deeper examination of ethical, legal, and societal impacts (International Network of Civil Liberties Organization, 2024).

Although facial recognition technology has advanced significantly, improving accuracy and expanding its applications, it still faces several challenges and limitations. Issues related to accuracy persist, as variables like lighting, facial expressions, aging, and accessories such as glasses or hats can affect system performance. Moreover, concerns over racial and gender biases in some algorithms raise questions about fairness and reliability. Privacy is another critical issue, as the ability to track individuals in public spaces heightens fears of mass surveillance and potential misuse of sensitive facial data. Additionally, legal and regulatory frameworks often struggle to keep pace with rapid technological advancements, creating inconsistencies across jurisdictions that may lead to misuse or complications for businesses operating internationally. The effectiveness of facial recognition systems also depends largely on the quality of input data, with low-resolution images or images captured at odd angles potentially reducing accuracy. Despite these obstacles, the continuous evolution of the technology, alongside dedicated research, thoughtful regulations, and ethical considerations,

holds promise for overcoming these challenges while maximizing its benefits (Qinjun et. at., 2023).

Dumbrava (2021) highlights that face recognition technologies, although transformative for border management, amplify risks related to fundamental rights, including the disproportionate targeting of specific ethnic groups and mass surveillance. This issue arises from the quality of training datasets used in biometric matching algorithms, which often lack diversity and completeness, resulting in inaccuracies and biases against marginalized groups. The author also underscores that such profiling may lead to discriminatory outcomes based on prohibited grounds, even when biometric data is not the sole basis. The increased reliance on facial images in biometric systems, along with automated profiling, risks unlawful profiling by revealing sensitive attributes, such as ethnic origin. Furthermore, existing safeguards, such as the human-in-the-loop approach and the right to explanation, may prove insufficient to address the broader implications of bias and discrimination embedded in these technologies. These challenges demand heightened transparency and oversight, particularly regarding European Union-funded research in the area, to prevent the erosion of fundamental rights and ensure ethical deployment of biometric systems.

2.3.2 Fingerprint Recognition

Fingerprint recognition is a biometric identification method that utilizes the unique patterns of ridges and valleys on an individual's fingertips to verify or establish their identity (Okta, 2024). Specifically, these patterns, known as minutiae, are highly distinctive and remain constant throughout a person's lifetime. Consequently, fingerprint recognition has become one of the most mature and widely adopted biometric technologies, balancing performance with social acceptance.



Indeed, the process of fingerprint verification typically involves several key steps. The first step is to capture an image of the fingerprint. This is typically done using specialized fingerprint scanners, which may utilize different technologies such as optical, capacitive, or ultrasound. Then, once the fingerprint image is captured, the system extracts specific features from it. These features include ridge endings, bifurcations, and other unique characteristics of the fingerprint. Following this step, the extracted features are then used to create a digital template or representation of the fingerprint. This template is essentially a mathematical model that captures the unique attributes of the fingerprint (Donida Labati et. al., 2015).

When a user attempts to authenticate their identity using their fingerprint, the system captures a new image of the fingerprint. This image is processed to create a new template, which is then compared to the stored templates in the system's database. Following with the process, the system employs pattern-matching algorithms to compare the new template with the stored templates. It looks for similarities and differences between the two templates to determine whether they match. Finally, based on the results of the pattern-matching process, the system decides the authenticity of the fingerprint. If the new template closely matches any of the stored templates, the user is granted access. Otherwise, access is denied (Innovatrics, 2025).

Furthermore, the storage of both facial and fingerprint biometric traits in second-generation European e-Passports allows for multimodal biometric verification, significantly enhancing recognition accuracy. This multimodal approach leverages the distinct strengths of each biometric, providing a more robust and reliable identification process (Oloid Desk, 2024).

Notably, while fingerprints are optional in e-Passports, their use is prevalent in ABC systems globally. In fact, a significant portion of surveyed ABC systems utilize fingerprint recognition, either independently or in conjunction with other modalities. For example, systems like Global Entry in the United States, PARAFE in France, e-Channel in Hong Kong, and the Spanish ABC system exemplify the widespread implementation of fingerprint recognition (Donida Labati et. al., 2015).

To delve deeper, fingerprint recognition relies on analyzing the unique characteristics of ridge endings and bifurcations, collectively known as minutiae. These minutiae points, along with the overall ridge flow, form the basis for creating a digital template that represents the fingerprint. According to the National Institute of Standards and Technology (NIST), Minutiae-based matching is the most common and widely used technique. Minutiae are local ridge characteristics that occur at a ridge ending or a ridge bifurcation (Garris and McCabe, 2000).

Fingerprint recognition, while widely adopted in biometric authentication, faces several obstacles in the context of ABC systems. One significant issue is the quality and reliability of fingerprint scans, which can be affected by factors such as skin conditions, dirt, moisture, or aging. Improving the usability of biometric systems is essential to ensure sufficient image quality, as emphasized by Donida Labati et al. (2015). This underscores the necessity of developing more effective quality analysis algorithms to enhance usability and system performance.

Additionally, cryptographic interoperability between countries remains a crucial challenge. Many authorities employ cryptographic protection for electronic travel document chips, making access to stored fingerprints more complicated. According to the study, “the definition of standards that guarantee the interoperability of the systems could permit easy access to the fingerprints while protecting their integrity and preventing illegal access” (Donida Labati et al. 2015, pp n/d). This highlights the need for standardized protocols to balance security and accessibility across different international systems.

Moreover, fingerprint acquisition speed can sometimes hinder efficiency in border control processes. Proper placement of the finger on the sensor is essential for accurate capture, and some scanners require the user to slide their finger over the sensor for several seconds to ensure a high-quality scan. In this sense, the authors emphasize the importance of developing fingerprint sensors and protocols that can reduce acquisition time, highlighting the need to optimize sensor technology to minimize authentication delays.

In conclusion, fingerprint recognition remains a cornerstone of biometric identification, offering a robust and reliable method for verifying identity. While challenges related to image quality and privacy exist, ongoing advancements in sensor technology and matching algorithms continue to enhance its performance and security. The integration of fingerprint recognition with other biometric modalities further strengthens its utility in diverse applications (1Kosmos, 2024).

2.3.3 Iris Recognition

Iris recognition is a biometric identification technique that utilizes the unique patterns of the iris, the colored ring-shaped diaphragm in the eye, to establish an individual's identity. Specifically, the iris is characterized by its intricate and stable structure, featuring a rich tapestry of furrows, ridges, and pigment spots. Furthermore, the high degree of variability in these patterns among individuals ensures a robust and reliable biometric trait. Consequently, iris recognition stands as a highly effective method for identity verification (Kaya, 2023).



Indeed, iris recognition has found prominent application in border control systems, owing to its exceptional resistance to false matches and rapid matching speed. For example, early implementations of e-Gates, designed for rapid traveler processing (RTP), leveraged iris recognition's strengths. Notably, systems like IRIS in the United Kingdom, Privium in the Netherlands, and those deployed in Canada, Germany, and the United Arab Emirates exemplify this early adoption (Kaya, 2023).

However, a significant drawback to iris recognition in Automated Border Control systems is the absence of iris data in currently circulating e-Passports. Although the iris is an optional biometric for e-Passports, its lack of widespread inclusion necessitates the creation of supplementary backend databases containing iris information. This adds complexity and cost to system implementation (Donida Labati et. al., 2015).

Moreover, while iris recognition boasts high recognition performance, it is perceived as more intrusive compared to other biometric modalities. Consequently, its social acceptance is limited, hindering its widespread adoption in e-Gates. To elaborate, the iris verification process involves several steps: first, guiding the traveler to position their head near the camera; second, using near-infrared light to illuminate the eye, control gaze, and pupil dilation; third, capturing the iris image; and fourth, comparing the live image with stored data.

To further illustrate, iris recognition systems typically employ near-infrared (NIR) illumination to capture detailed iris patterns, as NIR light provides optimal contrast and detail, even in dark irises. Additionally, advanced algorithms analyze the unique textural features of the iris, such as crypts, collarettes, and freckles, to generate a unique iris code. This code is then compared against a database of enrolled iris codes for identification or verification (Donida Labati et al., 2015).

If we think about the challenges, a significant obstacle in the implementation of iris recognition is the substantial financial investment associated with iris capture technologies, which exceed the costs of facial or fingerprint recognition sensors. Moreover, the absence of iris data within current passport infrastructures necessitates the creation of supplementary back-end systems for iris information storage. Furthermore, the perceived intrusiveness and user-unfriendliness of iris scanners pose a challenge to user acceptance. In this sense, the advancement of innovative methodologies aimed at mitigating these issues is crucial for

enhancing the public's receptiveness to ABC systems incorporating iris recognition (Donida Labati et. al., 2015).

Iris recognition, despite its high accuracy, presents several challenges and drawbacks in the context of Automated Border Control (ABC) systems. One significant issue is image quality and environmental dependency, as proper illumination and positioning are essential to ensure reliable identification. According to Sánchez del Río et al., (2016), external factors such as illumination and reflections can significantly impact the quality of iris images, affecting recognition accuracy. Additionally, iris recognition requires user cooperation and precision, since individuals must align their eyes correctly with the scanner, which can be difficult in high-traffic environments. The document highlights that precise eye positioning requirements in biometric systems can impact the speed of verification processes in high-traffic border control environments. Furthermore, interoperability and standardization remain key concerns, as various countries utilize different iris recognition technologies, leading to compatibility issues. The study highlights the importance of standardization in enabling the effective integration of iris recognition technologies across various border control systems.

Donida Labati et al. (2015) further emphasize several challenges associated with implementing iris recognition in Automated Border Control (ABC) systems. One significant limitation is the high cost, as iris capture systems are considerably more expensive than fingerprint or facial recognition technologies. Moreover, since iris biometrics are not currently included in any passport in circulation, ABC systems must develop separate back-end databases to store this biometric data. Another key issue is user perception—many travelers view iris scanners as intrusive and difficult to operate. These factors indicate that enhancing user experience and reducing system costs are essential steps toward the broader adoption of iris recognition technologies in border control contexts.

2.4 Surveillance Drones

The European Union's approach to border surveillance has increasingly incorporated unmanned aerial vehicles (UAVs), or drones, driven by a confluence of state and non-state actors (Loukinas, 2022). Specifically, the Schengen Borders Code outlines the primary objectives of this surveillance: preventing unauthorized border crossings, combating cross-border criminality, and addressing illegal border entries. Consequently, the Council of

the European Union, the European Commission, Frontex, national border and coast guard agencies, the border security industry, and various NGOs have become key stakeholders in the promotion and deployment of drone technology (Csernatoni, 2018).



Indeed, these stakeholders perceive drones as superior to traditional methods, offering a more precise, continuous, and extended view of the European Union's border zones, particularly the vast maritime areas of the southern borders. Furthermore, this emphasis on efficiency aligns with the European Union's "border technology fix," which posits that technological solutions can resolve border security challenges, including distress incidents in the Mediterranean (Loukinas, 2022).

Over the past two decades, the European Union has significantly increased its reliance on surveillance technologies to manage migration flows at its external borders. To this end, substantial investments have been made in large databases, information and communications technologies like Eurosur, and the deployment of advanced aircraft and satellite systems (Topak, 2019). This technological augmentation aims to enhance the European Union's surveillance capacity in order to reduce the number of irregular migrants and, at the same time, to improve situational awareness, with electronic information collection and processing becoming preferred policy options (Loukinas, 2022).

Unquestionably, drones have emerged as pivotal tools in this context, bolstering border-guarding operations and expanding the surveillance system's operational capacity.

Consequently, they are integral to the development of "smart borders" or "technological borders." While the advantages of drone usage are acknowledged, the "dronization" of borders has sparked ongoing debate, particularly concerning humanitarian implications (Val Garijo, 2020).

One of the primary advantages of drones is their ability to perform "3D" tasks-dull, dirty, and dangerous operations. For instance, they can survey extensive and remote areas more efficiently than manned aircraft, with extended flight durations. Moreover, drones enhance operational safety by mitigating risks associated with weather, natural hazards, and pilot fatigue. Additionally, their advanced sensor capabilities facilitate data collection that is going to be transmitted to databases managed by border surveillance authorities (Marin, 2016). Notably, drones enhance transparency, promoting accountability among border guards and agencies. Specifically, they can monitor border guard conduct, including the use of force, and provide evidence in relevant situations (Koslowski and Schulzke, 2018).

Despite the operational advantages of drones, their use in migration governance raises significant ethical and legal concerns, particularly regarding border securitization and the restriction of mobility for irregular migrants. Val Garijo (2020) underscores that drone surveillance reinforces defensive migration policies, enabling states to conduct pull-back operations that prevent migrants from reaching safe territories. These strategies often result in migrants being returned to departure points under legally ambiguous conditions, potentially exposing them to human rights violations (Val Garijo, 2020). Similarly, Loukinas (2022) highlights how drones serve dual purposes; while they support SAR missions, they also enhance border surveillance mechanisms that increase interceptions and pushbacks, limiting asylum opportunities.

Marin (2016) argues that drones contribute to the broader process of techno-securitization, where border surveillance is increasingly militarized through the deployment of advanced technologies. This trend not only reinforces restrictive migration policies but also raises concerns about privacy and data protection, as drones enable mass surveillance and data collection without clear regulatory oversight. Moreover, the "dronization" of borders introduces a military bias into border management, where the dual-use nature of drones blurs the lines between military and non-military domains, reinforcing a defensive logic that prioritizes security over humanitarian considerations (Csernaton, 2018).

Furthermore, the increasing reliance on surveillance technologies raises ethical concerns about the dehumanization of migrants, as drone operations shift the focus from individual human lives to data-driven security measures (Marin, 2016). Additionally, the involvement of private companies in drone operations introduces concerns regarding accountability and transparency, particularly in cases where data collection practices lack regulatory oversight (Loukinas, 2022). This lack of clear regulation increases the risk of misuse and raises questions about how collected data may be leveraged for restrictive migration policies. As Marin (2016) and Csernaton (2018) highlight, drone technology is part of a broader securitization framework that prioritizes border defense over humanitarian considerations. This dynamic underscores the complex implications of drone deployment in border control, emphasizing the need for a balanced approach that integrates ethical migration governance with security objectives.

2.5 SIS, Eurodac, VIS, EES, ETIAS

2.5.1 Schengen Information System

The SIS is one of the major IT systems overseen by eu-LISA to enhance security across Europe. As stated by the Commission (eu-LISA, 2025), it is “the most widely used and largest information-sharing system for security and border management in Europe.” The Schengen countries were pioneers in establishing electronic mail infrastructure, and SIS plays a crucial role in monitoring various cross-border movements. Serving as the "database flagship" of the Schengen Agreement, it stores data on individuals and objects, allowing national authorities, including police and border guards, to enter and consult alerts. The system is composed of a central database, known as C-SIS, and national SISbases across all Schengen states. Located in a secure facility in Strasbourg, C-SIS is designed to uphold public order and security, including State security, and to enforce provisions of the convention concerning the movement of persons within the territories of the contracting parties using information transmitted by the system (Dijstelbloem, 2021).

The SIS became operational on 26 March 1995. By that time, the system was used by seven States: Belgium, the Netherlands, Luxembourg, France, Spain, Portugal and Germany. At the end of 1997 those countries were joined by three other countries: Italy, Austria and Greece. Later, in 2001, SIS I evolved into SIS I+, to include the Nordic countries (eu-LISA, 2025).

In 2013, the second generation of SIS (SIS II) was rolled out, with additional functionalities, such as the possibility of adding fingerprints and photographs to alerts. In this case, access to data within the SIS II system is strictly regulated, confined to national entities responsible for law enforcement, judicial proceedings, and administrative functions. These authorized bodies are permitted to view only the specific SIS II data necessary for their designated duties (European Union, 2013).

To augment the efficacy of counter-terrorism efforts, participating nations have, since March 2021, shared matching search results from SIS alerts pertaining to terrorist offenses with Europol. This collaborative exchange is further facilitated through the SIRENE Bureaux⁴, which handles supplementary information (European Commission, 2025). Moreover, the system extends its protective reach to vulnerable individuals, enabling competent authorities to issue detailed alerts on missing persons and implement preventive alerts for those at risk of abduction, human trafficking, gender-based violence, or involvement in armed conflicts. In terms of migration management, SIS now incorporates the sharing of return decisions to enhance their enforcement, requiring member states to register refusal of entry or stay alerts for individuals illegally residing within the European Union and subject to entry bans. Furthermore, cooperative mechanisms have been expanded to include registration authorities responsible for boats, aircraft, and firearms, allowing them to verify the legal status of these objects through SIS consultations, with access tailored to the specific object type. Lastly, the system grants enhanced access to European Union agencies, with Europol possessing comprehensive access to all alert categories and the European Border and Coast Guard Agency's operational teams currently undergoing integration for SIS access at hotspots (European Commission 2025).

Within SIS, data is organized into alerts, each detailing specific individuals or objects of interest. These alerts may include biographical details such as an individual's full name, birthdate, gender, and nationality. Additionally, SIS possesses the capability to store biometric data, specifically fingerprints and photographs, linked to these alerts. Authorized member state authorities conduct queries, or searches, within the system to identify potential matches against the stored alerts. Notably, a substantial portion of these alerts pertains to officially issued documents and vehicles, encompassing items such as registration documents,

⁴ SIRENE Bureaux are set up in every Schengen Member State and provide supplementary information on alerts and coordinate activities in relation to alerts in the Schengen Information System. SIRENE Bureaux also exchanges data important for police and judicial cooperation, conducts database queries, and coordinates cross-border operations (European Commission, n.d.).

license plates, and the vehicles themselves. Furthermore, the system processes an average of 20 million search queries daily, reflecting its extensive utilization (eu-LISA, 2025).

To uphold data integrity, all national agencies utilizing SIS II are mandated to verify the accuracy of the information they input into the system. Within the Schengen Area, stringent data protection regulations are enforced. Individuals whose personal data is retained have the entitlement to request access, ensuring the information is precise and legally recorded. Should inaccuracies or unlawful entries be identified, individuals possess the right to demand rectification or deletion of the data. However, access to this data may be denied only when such denial is essential for the execution of a legitimate task related to an alert, or to safeguard the rights and liberties of others (European Union, 2013).

According to eu-LISA (2025), to bolster the operational effectiveness and efficiency of the SIS, a comprehensive reform package was implemented in 2023, introducing a suite of technical and operational enhancements. Specifically, the system now incorporates new alert categories, thereby augmenting the reliability of information distributed among Member States. Moreover, the scope of biometric data has been broadened to include palm prints, fingerprints, facial images, and DNA samples. Furthermore, information exchange concerning individuals and objects linked to terrorism has been intensified, aiding in counter-terrorism efforts. Additionally, proactive alerts have been introduced to safeguard vulnerable individuals, such as missing persons and potential victims of human trafficking or gender-based violence. In terms of migration management, return decisions and entry bans are now shared to improve enforcement. Finally, European Union agencies have been granted expanded access, with Europol accessing all alert categories and Frontex operational teams accessing SIS for tasks conducted at hotspots.

SIS II, while crucial for managing mobility within the Schengen Area, faces significant challenges that affect its reliability and effectiveness. As a complex digital infrastructure, it is prone to technical issues and user-related problems, requiring constant maintenance and monitoring. For the data to be trusted, attention must be given to data quality, system connectivity, and user behavior. The European Commission and eu-LISA address these challenges by implementing corrective measures and training, emphasizing the fragile nature of the system.

This fragility raises important questions about the assumed efficiency of digital border controls. The constant need for maintenance challenges the narrative of flawless digital governance, revealing the vulnerabilities in these systems. By focusing on the upkeep and limitations of infrastructures like SIS II, we can better understand the processes and actors involved in sustaining digital borders and rethink how mobility is governed beyond the technology itself (Bellanova and Glouftsios, 2020).

2.5.2 Eurodac

An acronym for European Asylum Dactyloscopy Database, is a centralized biometric system within the European Union designed to manage asylum applications and address irregular migration. Fundamentally, it operates as a fingerprint database, facilitating the identification of asylum seekers and irregular migrants across member states (eu-LISA, 2025). Specifically, Eurodac was implemented to prevent "asylum shopping," a practice where individuals submit multiple asylum claims in different European Union countries under the Dublin Regulation⁵, and to provide insights into secondary migration movements .

Indeed, the system became operational in 2003 and has been managed by eu-LISA since 2013. Currently, Eurodac is utilized by 31 countries, including the 27 EU member states and four Schengen Area associated countries (Iceland, Norway, Switzerland, and Liechtenstein), as well as Europol. Notably, it stores over seven million fingerprint records and can process up to 24,000 transactions daily (eu-LISA, 2025).

Furthermore, Eurodac's development was driven by the need to establish a system that could determine whether an asylum claimant had previously lodged a claim in another member state (Broeders, 2007). Originally, its scope was limited to asylum seekers, but, in 1998, the German federal government pushed for the inclusion of irregular migrants. At this time, the government criticized the ineffective implementation of the Dublin Convention mechanism claiming that “many asylum seekers enter through the external border but do not submit their application in the first Member State they reach. Instead, they continue their journey to a

⁵ On 23 September 2020, the European Commission adopted the New Pact on Migration and Asylum following consultations with the European Parliament, Member States and various stakeholders. The New Pact covers all the different elements needed for a comprehensive approach to migration. In particular, the New Pact recognises that no Member State should shoulder a disproportionate responsibility and that all Member States should contribute to solidarity on a constant basis (eu.LISA, 2025).

country they personally prefer. By the time they arrive, it is often impossible to determine which part of the external border they initially crossed. As a result, and contrary to the rules outlined in the Dublin Convention, the absence of clear evidence regarding which Member State is responsible means that the country selected by the applicant ends up processing the asylum request” (Aus, 2003: 13).

Notably, Eurodac operates as a hit/no-hit system with limited data storage. Like the SIS, the database contains information such as the member state of origin, place and date of the asylum application, fingerprint data, sex, reference number used by the member state of origin, date of fingerprint capture, among others (Brouwer, 2008).

However, Eurodac is undergoing significant modernization as part of the European Union's New Pact on Migration and Asylum, which entered into force in June 2024. This reform aims to transform Eurodac into a comprehensive database that supports member states in asylum, resettlement, and irregular migration management. The reformed Eurodac will shift its focus from applications to applicants, include new data categories, facilitate relocation, improve return monitoring, and track support for voluntary departure and reintegration (eu-LISA, 2025).

2.5.3 Visa Information System

The VIS is a centralized database designed to support the European Union's common visa policy, facilitating the exchange of visa data between Schengen States and simplifying the application process for travelers. Fundamentally, VIS aims to enhance security, prevent fraud, and streamline visa procedures by centralizing biometric and alphanumeric data related to visa applications. Since 2013, eu-LISA has been responsible for the management of the VIS (eu-LISA, 2025).

Indeed, VIS connects consulates in non-European Union countries with all external border crossing points of Schengen States. Specifically, it processes data and decisions related to short-stay visa applications, enabling border control authorities to verify visa authenticity and traveler identity. Moreover, its biometric matching capabilities aid in detecting multiple applications from the same individual, thereby preventing "visa shopping" (Broeders, 2007).

The implementation of the VIS offers a range of advantages, beginning with simplified and expedited visa processes for travelers entering the Schengen Zone. Furthermore, it enhances security by employing biometric authentication, safeguarding against identity theft and ensuring accurate individual recognition. Enhanced collaboration and information exchange among national visa authorities is also facilitated. The system effectively mitigates the risk of visa fraud and “visa shopping”. Additionally, it enables the identification of individuals who no longer meet the entry or residency requirements within the Schengen Area. The VIS also provides assistance in the adjudication of asylum requests and offers support to national agencies in preempting internal security risks (eu-LISA, 2025).

Furthermore, VIS became operational in October 2011, connecting European Union member states' immigration authorities and consular posts worldwide. The core database within the VIS compiles both personal and biometric records for all individuals applying for European Union visas, alongside a chronological history of each visa's status—application, approval, rejection, cancellation, withdrawal, or extension. Consequently, the VIS facilitates the generation of comprehensive data on visa-related travel patterns across various countries and regions. Specifically, the system manages three distinct data categories: first, alphanumeric details of applicants and visa holders, encompassing biographical information and application specifics; second, digitized fingerprint records of all ten digits, captured and stored by relevant authorities; and third, digital facial images of those seeking Schengen visas (Dijstelbloem, 2021).

Notably, the system generates aggregated data on visa-based mobility trends from specific countries and regions. From a migration management perspective, VIS plays a crucial role in combating irregular immigration. It represents a strategic extension of the evolving European Union database network. Typically, irregular migrants exhibit three distinct 'migration histories': unauthorized border crossing (with or without assistance), overstaying after asylum rejection, or visa expiration. The database network is structured to address these trajectories. While irregular entry inherently resists direct registration, apprehended individuals are recorded in the SIS. Similarly, asylum-related entries are tracked via Eurodac, and future visa-related entries will be managed by the VIS. Identity verification has become a central focus in European Union discourse concerning irregular migration, counter-terrorism, and their perceived interconnections (Broeders, 2007).

However, challenges exist. Firstly, the large-scale use of biometrics raises concerns about privacy and data security. In this sense, the growing reliance on bodily-derived data for identification and registration, such as fingerprints, potentially infringes upon personal privacy and alters perceptions of bodily autonomy. Such practices demand stringent ethical conduct from involved entities, ensuring that overly restrictive data interpretations do not result in unjust decisions. Secondly, the initial implementation and ongoing maintenance of the system can be financially demanding. Thirdly, beyond specific ethical, technical, and financial considerations, a significant critique centers on the systems' tendency to interconnect and expand. Consequently, these systems are often characterized as “greedy” and “machinelike”, particularly in light of European Union proposals to transform them in response to the “migrant crisis” and the convergence of migration and security policies (Dijstelbloem, 2021).

In anticipation of future security and migration complexities, the European Commission has advocated for a modernization of the VIS, focusing on several key enhancements. Initially, security protocols will be reinforced through comprehensive database cross-referencing, automatically scrutinizing all visa applications against European Union-wide information systems to identify individuals employing multiple identities. Secondly, data and information sharing will be expanded to encompass long-stay visas and residence permits used for Schengen Area border crossings, in addition to the current short-stay provisions. Thirdly, return procedures will be made more efficient by integrating copies of applicant travel documents into the VIS, aiding in the identification and repatriation of individuals lacking proper documentation. Lastly, law enforcement and Europol will gain improved, structured access to the VIS, facilitating the prevention, detection, and investigation of terrorist activities and other serious criminal offenses (eu-LISA, 2025).

2.5.4 Entry/Exit System

The EES is an automated IT system designed to digitally record the entry, exit, and refusal of entry of non-European Union nationals traveling to and from the Schengen Area. Essentially, the EES aims to modernize border management by replacing manual passport stamping with electronic records, thereby enhancing security and efficiency (European Commission, 2025).

Scheduled to become operational in October 2025, this system represents a significant shift in how the European Union manages its external borders.

Specifically, the EES will register a traveler's name, travel document type, biometric data (fingerprints and facial images), and the date and place of entry and exit. Furthermore, it will record refusals of entry, providing a comprehensive electronic record of non-European Union nationals' movements within the Schengen Area. Notably, this data collection will be conducted in full respect of fundamental rights and data protection (European Commission, 2024).

According to eu-LISA (2025), the EES offers several benefits, notably the acceleration of border transits through the modernization of inspection processes, thereby minimizing delays and simultaneously improving traveler security and precision. Moreover, it facilitates the monitoring of individuals exceeding authorized stays, thereby assisting European Union Member States in the management of unauthorized migration. The system's biometric data capture and verification capabilities, encompassing fingerprints and facial imaging, effectively counteract identity deception, ensuring accurate traveler authentication. Finally, the EES strengthens domestic security by allowing for the identification of individuals implicated in illicit activities through the cross-referencing of data with other European Union security databases.

The EES is a key component of the European Union's broader efforts to strengthen border security, reflecting the objectives of the Security Union and the European Agenda on Migration and Security (GOV.UK, 2024). The legal framework for the EES was presented on 6 April 2016 as part of the revised Smart Borders Package⁶. Finally, the regulation was adopted in November 2017, which also included targeted amendments to the Schengen Border Code.

The EES applies to all non-European Union nationals traveling for short stays⁷ in Schengen Area countries, regardless of whether they require a visa. However, it's important to note that

⁶ Set of measures consisting of the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and modification to the Schengen Borders Code aimed at improving the management of the external European Union borders by facilitating border crossing for pre-vetted frequent non-European Union travellers, while at the same time fighting against irregular migration and improving internal security by stronger identification of persons at external EU/Schengen borders and detection of overstayers in the European Union's territory (European Commission, 2025).

⁷ 'Short stay' means up to 90 days within any 180-day period. This period is calculated as a single period for all the European countries using the EES (EES, 2025).

Cyprus and Ireland, while European Union Member States, will continue to use manual passport stamping (European Commission, 2025).

As was just mentioned before, the EES, while designed to enhance border management and security within the European Union, raises significant concerns regarding human rights, data protection, and migration management. One critical issue is the potential infringement on the right to privacy and data protection, as the system involves the mass collection and retention of biometric and personal data from non-European Union nationals. According to the European Commission (2025), “the EES will register travelers’ names, biometric data, and travel details, raising concerns about the proportionality and necessity of such extensive data collection”. This extensive data retention, if not adequately safeguarded, could lead to unauthorized access or misuse, thereby compromising individuals' fundamental rights.

Moreover, the EES has been criticized for its potential to exacerbate biases and discrimination in migration management. Amnesty International (2024) highlights that the deployment of digital technologies in migration systems risks perpetuating discriminatory practices, particularly against racialized and marginalized groups.

The reliance on automated systems and biometric data may disproportionately impact vulnerable populations, such as asylum seekers and irregular migrants, who may face challenges in providing accurate biometric information due to physical or environmental factors. Additionally, the system's focus on identifying overstays and irregular migration could lead to the stigmatization of certain groups, further marginalizing them within the broader migration framework. These concerns underscore the need for robust legal and ethical safeguards to ensure that the EES operates in full compliance with human rights standards (Amnesty International, 2024).

2.5.5 ETIAS

The European Commission first introduced the idea of the European Travel Information and Authorisation System in April 2016 in the Communication "Stronger and Smarter Information Systems for Borders and Security". After negotiations with the European Parliament and the Council the ETIAS Regulation (European Union) 2018/1240 was adopted on 12 September 2018 and entered into force on 9 October 2018.

Moreover, ETIAS is implemented within the context of the Security Union initiatives, with the express purpose of contributing to the objectives set forth in the European Agenda on Security⁸ and the European Agenda on Migration⁹. This system is intended to bolster border management practices and serve as a tool for the prevention of transnational crime and terrorism (European Commission, 2024).

The ETIAS system is based on an advanced, largely automated IT infrastructure aimed at pre-screening visa-exempt travelers wishing to enter the Schengen Area. Its main objectives are to identify potential security threats, detect irregular migration patterns, and assess public health risks, while also facilitating border crossings for the majority of low-risk individuals (European Commission, 2024). This intricate system is composed of the ETIAS Central Unit, managed by Frontex, ETIAS National Units distributed across 30 European nations¹⁰, and a comprehensive information network developed and maintained by eu-LISA (Frontex, 2025).

To navigate the intricacies of travel authorization, individuals from 59 visa-exempt countries seeking short stays in one of the aforementioned 30 European nations will be required to obtain ETIAS approval (eu-LISA, 2025). This process mandates the completion of an online application and the payment of a €7 fee. Subsequently, the ETIAS system conducts a thorough cross-examination of applicant data against a consortium of European Union systems, including the Schengen Information System (SIS), the Visa Information System (VIS), the Entry/Exit System (EES), as well as databases maintained by Europol and Interpol. This comprehensive check facilitates the advance verification of potential security, migration, and public health risks (eu-LISA, 2025). Consequently, the majority of applications, approximately 97%, are expected to be processed automatically within minutes, minimizing delays for travelers (Frontex, 2025).

However, in cases where applications raise concerns, a manual review will be conducted by the ETIAS Central Unit and the relevant National Units, potentially extending the processing

⁸ The European Agenda on Security guidees the Commission's work in this area, setting out the main actions to ensure an effective European Union response to terrorism and security threats in the European Union. President Juncker also created a specific Commissioner portfolio for the Security Union to ensure an effective implementation of the commitments made (European Commission, 2017).

⁹ A strategic document of the European Union presented in May 2015 outlining a comprehensive approach to migration management addressing the asylum and migration challenges as well as definition steps to be taken to ensure strong borders, fair procedures and a sustainable system able to anticipate future problems in the context of asylum and migration (European Commission, 2015).

¹⁰ Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland (Frontex, 2025).

timeframe. Once granted, the ETIAS travel authorization permits stays of up to 90 days within the European Union and Schengen Area, valid for a maximum of three years or until passport expiration, whichever occurs first, necessitating a new application upon passport renewal (eu- LISA, 2025). Crucially, border guards at European Union entry points will verify the ETIAS authorization alongside travel documents. This prior verification of visa-exempt non-European Union citizens aims to streamline border checks, reduce bureaucratic obstacles, ensure a coordinated and harmonized risk assessment of third-country nationals, and substantially decrease the incidence of entry refusals (European Commission, 2024).

2.6 Concluding remarks

The increasing reliance on biometric systems within the European Union's migration and border management framework reflects a profound shift in how states perceive and control mobility. These technologies are no longer peripheral tools; they have become central pillars in a broader strategy that prioritizes efficiency, control, and risk assessment. Biometric identifiers such as fingerprints, facial images, iris scans and drones are used not only to authenticate identity but also to classify individuals according to perceived levels of risk. This creates a layered system of mobility, where access and rights are unevenly distributed and determined by algorithmic and biometric calculations.

The chapter has demonstrated how various forms of biometric technology are being applied in different operational modes—verification and identification—to manage vast flows of people at the European Union's internal and external borders. From facial recognition and fingerprint scanning to the more sophisticated but less widespread iris recognition, these systems reflect a technological ambition to automate and secure identity management. However, their functioning is not without challenges. Issues related to accuracy, social acceptance, user cooperation, and data integrity reveal the limitations and unintended consequences of over-relying on such systems, especially in high-stakes contexts like asylum, deportation, or visa denial.

A key point emerging from the analysis is the extent to which biometric systems are embedded into large-scale digital infrastructures. Databases like Eurodac, VIS, SIS, EES, and ETIAS form an interconnected network that not only stores biometric data but actively

shapes the governance of mobility in the European Union. These systems enable real-time surveillance, track historical patterns of movement, and support a pre-emptive logic of border control. While they are often justified through the lens of security and efficiency, their cumulative effect is the normalization of biometric surveillance and the construction of a digital border that is both omnipresent and opaque.

This raises broader ethical and political considerations. As biometric data becomes a prerequisite for legal mobility, the body itself is turned into a passport, a key, and at times, a liability. For many, particularly irregular migrants, the ability to navigate borders depends on negotiating, concealing, or manipulating their biometric trace -often under precarious conditions-. This reality highlights a deeper tension within the European Union's migration regime: the aspiration for smart, seamless borders coexists with practices of exclusion, surveillance, and control. As digital technologies continue to evolve, it is crucial to ensure that their deployment does not come at the expense of dignity, equality, and fundamental rights.

Chapter 3: Legal and Ethical Implications

3.1 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 (FRA, 2020; Amnesty International, 2024).

Recent reports by human rights organizations and European Union institutions have documented discriminatory practices, algorithmic bias, violations of data protection standards, and opaque decision-making systems at the European Union's external borders. These critiques reveal not only the uneven distribution of technological harms across different migrant populations, but also the difficulty of ensuring effective oversight and access to legal remedies in an increasingly digitized border regime (FRA, 2024; Amnesty International, 2021; Human Rights Watch, 2021). Particularly concerning is the role of the European Border and Coast Guard Agency (Frontex), which has faced numerous allegations of involvement in pushbacks and human rights violations, often facilitated through digital surveillance and coordination technologies (Amnesty International, 2021; European Parliament, 2023).

A growing body of scholarship has begun to conceptualize the digital border as a space where power is exercised through datafication, classification, and surveillance. Redpath (2007) argues that digital migration governance exacerbates existing inequalities by embedding surveillance and exclusion into technological infrastructures that claim to be neutral or objective. Similarly, Rinaldi and Teo (2025) emphasize how the integration of AI into migration control introduces a "subtle erosion of human rights", as predictive systems and profiling mechanisms often operate without transparency, clear accountability, or due process safeguards.

The fundamental rights implications of such systems are profound. As the European Union Agency for Fundamental Rights (FRA, 2020) has highlighted, technologies like facial recognition and automated risk assessment can lead to invisible harm -violations that are difficult to detect or challenge because affected individuals are unaware that algorithmic systems have been used to influence decisions about their mobility or asylum claims-. This lack of transparency undermines the right to an effective remedy and raises critical concerns about democratic accountability.

Wachter et al., (2020) stress that fairness cannot be automated and argue that the legal and ethical frameworks governing AI must go beyond technical fixes and address the structural conditions that produce discrimination. In the context of migration, where racialized and socioeconomically vulnerable groups are often targeted, these concerns are particularly acute. The opacity of algorithmic systems -often described as a “black box effect”-makes it difficult to assess whether decisions are lawful, proportionate, or based on accurate data, thus complicating efforts to uphold European Union non-discrimination law and fundamental rights.

Moreover, Amnesty International (2024) has warned that digital surveillance tools deployed at Europe’s borders risk reinforcing a logic of suspicion and deterrence. Their February 2024 briefing highlights cases where migrants and asylum seekers were monitored through biometric and AI systems without meaningful consent, transparency, or the ability to contest data use. The report calls for stronger oversight, human rights impact assessments, and a moratorium on the use of certain high-risk technologies until proper safeguards are in place.

Importantly, the ethical implications of digital migration technologies extend beyond their operational impact. They also raise fundamental concerns about how research is conducted in this field, especially in contexts where migrants face precarity, surveillance, and limited agency. As highlighted in *Research Methodologies and Ethical Challenges in Digital Migration Studies* (2022), investigating these technologies involves complex dilemmas of access, representation, and power. Researchers must navigate opaque systems, protect the dignity and safety of vulnerable individuals, and critically reflect on their own positionality. These methodological challenges are deeply intertwined with the broader ethical landscape and therefore merit inclusion in any comprehensive analysis of digital migration governance (Leurs & Smets, 2018).

Garriga Domínguez (2024) emphasizes that transparency and accountability should be integrated into automated decision-making systems from the outset. She highlights the importance of ensuring that individuals affected by these technologies are provided with meaningful ways to understand how decisions are made, to challenge them when necessary, and to opt out of such processes altogether. Without these safeguards, technological systems risk functioning as tools of exclusion rather than protection.

This chapter examines the legal and ethical dimensions of digital migration technologies in the European Union, highlighting their impact on fundamental rights, data protection, and non-discrimination principles. It explores the risks posed by algorithmic opacity, biometric surveillance, and automated decision-making in migration governance, emphasizing concerns related to fairness, transparency, and accountability. The discussion critically assesses regulatory gaps and the challenges of ensuring effective oversight, while also considering the role of international and civil society actors in advocating for rights-based approaches to digital border management.

3.2 Framing the Human Rights dimension

The legal and ethical implications of digital migration technologies are not confined to isolated policy failures or technical limitations, they reflect a broader systemic shift in how human rights are interpreted, applied, and often undermined at Europe's borders. While legal instruments such as the Charter of Fundamental Rights of the European Union (CFR) and the European Convention on Human Rights (ECHR) remain formally in place, the way digital tools structure access to asylum, mobility, and protection significantly affects how these rights are experienced in practice. As digital infrastructures mediate decisions about who can move, who is visible to the law, and who is rendered a risk, the legal order increasingly privileges operational efficiency over individual rights and legal accountability (Molnar, 2020; FRA, 2020).

A human rights-centered lens makes visible how these technologies affect core principles such as human dignity, non-discrimination, freedom of movement, and access to justice. These are not abstract concerns: they relate directly to how automated decisions are made, how data is collected and shared, and whether people can understand or contest those processes. What emerges is a layered system of control in which migrants are increasingly

evaluated not as rights-holders, but as data profiles -subject to automated classification, surveillance, and preemptive exclusion- (Tazzioli, 2020). The effect is to shift the burden of legality from state action to individual legibility within algorithmic systems (McGregor & Molnar, 2023).

This transformation has significant implications for the right to dignity, which requires that individuals be treated as ends in themselves, not merely as objects of control (Wachter et al., 2020). It also affects the right to asylum, as automated systems and externalized controls risk denying access to procedures altogether (Amnesty International, 2024). Moreover, technologies like facial recognition, predictive analytics, and biometric databases intersect with longstanding forms of racialization and socio-political exclusion, echoing patterns of discriminatory governance. As researchers such as Tazzioli (2020), Molnar (2020), and Leurs (2023) have shown, these tools do not exist in a vacuum, they are embedded in social and institutional frameworks that often reproduce inequality.

In this sense, drawing on the work of Tazzioli (2020), Molnar (2020), and Leurs (2023), this thesis uses the term “digital border” to refer to not only a technical space but a legal one, where fundamental rights are continuously redefined by the capabilities and constraints of technology. As noted by FRA (2020) and McGregor & Molnar (2023), rights such as access to an effective remedy, freedom from degrading treatment, and protection from unlawful data use are often the first to be compromised in automated migration management. Migrants may be subject to decisions they cannot challenge, systems they do not understand, and harms they cannot trace -conditions that erode the normative integrity of human rights protections- (Wachter et al., 2020).

To respond to these challenges, a comprehensive legal and ethical framework must move beyond formal compliance and engage with the structural effects of digitalization. The analysis that follows explores six rights areas most affected by current European Union digital migration practices. These include the right to human dignity, the right to asylum, freedom of movement, the right to an effective remedy and fair trial, the prohibition of inhuman or degrading treatment, and the right to non-discrimination. Each section offers a critical assessment of how digital tools are reshaping the scope, accessibility, and substance of these rights, and what this means for the future of rights-based governance in European migration policy.

3.2.1 Right to Human Dignity

The right to human dignity constitutes the cornerstone of the European Union's legal and ethical order, enshrined in Article 1 of the Charter of Fundamental Rights of the European Union (CFR). It affirms that every individual must be treated as an end in themselves, not merely as a means to an objective, including in the context of migration and border governance. This foundational principle implies that public authorities, including those managing migration, must design and implement policies and technologies in ways that respect and uphold each person's intrinsic worth (European Union, 2000/C 364/01).

However, the increasing automation and depersonalization of migration control processes -such as biometric screening, algorithmic profiling, and AI-powered risk assessments- risk undermining this fundamental right by reducing individuals to data points, risk scores, or categories of suspicion. These practices introduce a logic of control and efficiency that often prioritizes operational goals over the rights and humanity of migrants (McGregor & Molnar, 2023).

As the European Union Agency for Fundamental Rights emphasizes in its report *Getting the Future Right - AI and Fundamental Rights* (2020), technologies deployed in migration contexts must be designed with care to avoid outcomes that dehumanize individuals, particularly vulnerable populations such as asylum seekers. The FRA underlines the importance of ensuring that technological solutions uphold personal dignity and allow for individual consideration, cautioning against systems that risk depersonalizing those they affect.

The principle of human dignity also demands transparency and human oversight, especially when algorithmic systems are used to make or inform life-altering decisions. Migrants subjected to automated assessments are often unaware of how decisions are made or whether they can contest them. Wachter et al. (2020) argue that algorithmic systems challenge the effectiveness of core mechanisms within European Union non-discrimination law, particularly by making traditional detection methods and evidential standards inadequate. This erosion of accountability mechanisms heightens the risk of discrimination, arbitrariness, and rights violations, all of which stand in opposition to the respect for human dignity.

A critical example of these tensions can be found in the European Union's biometric and digital identification systems. The collection and processing of biometric data -such as

fingerprints, facial images, and iris scans- are central to European Union initiatives like the SIS, Eurodac, and the EES. While these technologies aim to strengthen border security and migration management, they raise significant human rights concerns particularly related to privacy, data protection, and non-discrimination (FRA, 2020; McGregor & Molnar, 2023).

As Gonçalves and Gameiro (2012) argue in *Security, Privacy and Freedom: The European Union Legal and Policy Framework for Biometrics*, the deployment of biometric systems often shifts the presumption from individual rights to collective security, subtly altering the balance of values at the core of European law. According to the authors, biometric technologies embed a logic of surveillance that privileges state control over personal agency and diminishes the individual's ability to give meaningful consent. They caution that biometric identifiers, once captured, can be reused across databases and institutions, expanding surveillance far beyond the original purpose of collection and entrenching a form of digital tracking that can follow individuals indefinitely. This dynamic undermines dignity by transforming the body into a source of suspicion rather than a bearer of rights.

Furthermore, biometric and algorithmic systems may reinforce social inequalities by embedding racialized and gendered biases. As Browne (2015) argues, surveillance infrastructures often replicate historical patterns of exclusion and domination. Migrants, especially racialized and non-European individuals, are disproportionately subject to invasive technological scrutiny, reinforcing a hierarchy of human worth that contradicts the universality of human dignity.

Respecting human dignity, therefore, demands more than mere procedural safeguards. It requires a reimagining of migration technologies through an ethics of care and justice. This involves foregrounding the lived experiences of migrants, ensuring meaningful consent and transparency, embedding human oversight, and enabling redress. The European Data Protection Supervisor (EDPS) has echoed this stance, emphasizing that dignity must be the guiding principle in all data-driven practices affecting vulnerable populations (EDPS, 2021).

3.2.2 Right to Asylum

The right to asylum, enshrined in Article 18 of the Charter of Fundamental Rights of the European Union and the 1951 *Geneva Convention Relating to the Status of Refugees*,

obligates European Union Member States to ensure that individuals fleeing persecution are granted access to fair and effective asylum procedures. This right is not simply a procedural entitlement, it is a reflection of the European Union's foundational commitment to human rights and the protection of those in vulnerable situations. Yet, the growing deployment of digital technologies in migration management -particularly those involving biometric data, AI, and predictive analytics- can unintentionally undermine this right by creating both digital and physical barriers (FRA, 2020; McGregor & Molnar, 2023).

One major concern is the externalization of asylum procedures, wherein the European Union cooperates with third countries (e.g. Libya, Turkey, Niger) to conduct biometric screenings or risk assessments before migrants reach European territory (Leurs, 2023). These technologies are often enabled by information systems and data-sharing agreements that lack legal clarity and democratic oversight (FRA, 2020). As noted by Lanneau (2023), such practices can shift responsibility and reduce visibility, effectively allowing the European Union to sidestep its legal obligations under the principle of *Non-refoulement*. This principle, codified in Article 33 of the 1951 Refugee Convention, prohibits the return of individuals to countries where they may face persecution or serious harm.

Digital technologies exacerbate this issue by enabling remote filtering mechanisms, often without proper legal safeguards. For instance, asylum seekers may be denied boarding a flight or vessel based on biometric risk scoring or API/PNR (Advance Passenger Information / Passenger Name Record) systems. These preemptive barriers mean that individuals may be denied access to European Union asylum procedures before they have the opportunity to file a claim, effectively creating invisible walls along virtual borders (Guild, 2009).

In this context, the European Court of Human Rights (ECtHR) case *N.D. and N.T. v. Spain* (2020) is highly illustrative. Although the Grand Chamber ultimately ruled that Spain had not violated the applicants' rights, the dissenting opinion warned that collective expulsions without individual assessment -especially when technology is used to automate such decisions- can constitute a breach of the right to seek asylum and of Article 4 of Protocol No. 4 of the ECHR. This case underscores the tension between migration control policies and individual procedural guarantees in an increasingly digital context.

Moreover, automated pre-screening tools and profiling algorithms compound these concerns. These systems often apply generalized assumptions based on nationality, travel history, or

biometric matches in the Eurodac or SIS databases. According to the *Fact Sheet on Digitalisation* (2021), inconsistencies in biometric registration -such as failed finger print captures or poor data quality- can lead to wrongful rejections or excessive delays in processing claims. These operational issues are more than technical flaws; they undermine the fundamental requirement that asylum determinations be individualized, fair and accessible.

In addition, the increasing use of profiling and risk-scoring algorithms presents an even deeper procedural challenge. Many of these systems operate with limited transparency, little to no explainability, and often incorporate socio-political biases present in training datasets (FRA, 2020). As Amnesty International (2021) warns, such tools replicate and intensify existing inequalities by disproportionately categorizing individuals from certain racial or religious backgrounds as risky. These automated systems can have the effect of pre-judging asylum claims, bypassing essential procedural protections such as legal reasoning, human judgement, and appeal rights.

Furthermore, the digitization of asylum procedures -including online applications, automated appointments, and AI-assisted interviews- raises issues of accessibility and equality before the law. Asylum seekers with limited technological literacy or access, including older individuals, unaccompanied minors, persons with disabilities, or those in detention, may face insurmountable barriers (UNHCR, 2021). FRA (2020) have repeatedly emphasized that a technology-mediated system must not exclude those who are already marginalized. The principle of effectiveness -central to the jurisprudence of the European Court of Human Rights- requires that asylum seekers not only formally have access to procedures, but also genuinely be able to use them.

There is also a broader humanitarian and psychological dimension to consider. Digital filtering and surveillance practices can subject asylum seekers to repeated data checks, interviews, and delays that create a climate of uncertainty and anxiety. This prolonged instability has been linked to deteriorating mental health, trauma, and even suicide risk among those seeking protection (UNHCR, 2021). When technological barriers replace face-to-face communication and legal support with automated decision systems, the dignity and agency of asylum seekers are diminished.

Finally, the digitization of asylum processes may disproportionately impact individuals with low digital literacy or limited access to technology, such as children, people with disabilities, and older asylum seekers (FRA, 2020). If asylum applications must be submitted through automated platforms or kiosks with no language support or legal guidance, many may be excluded from the process altogether. Thus, a truly rights-respecting system must integrate human support alongside technology, not replace it (McGregor & Molnar, 2023).

3.2.3 Freedom of movement

Although the freedom of movement primarily protects European Union citizens under Article 45 CFR and Article 2 of Protocol No. 4 to the European Convention on Human Rights, its normative spirit extends to migrants, refugees, and third-country nationals, particularly when technological systems directly limit or shape access to European Union territory. As migration governance becomes increasingly reliant on surveillance technologies, biometric profiling, and automated risk-scoring, freedom of movement is increasingly constrained not by law, but by algorithm -producing opaque and often discriminatory barriers (Molnar, 2020; McGregor & Molnar, 2023).

Contemporary digital migration infrastructures -including systems like ETIAS, the Entry/Exit System, and the Schengen Information System- function as pre-screening regimes. They assess individuals' biometric data, travel history, and even behavioral characteristics before granting border access. These systems do not only expedite border checks; they fundamentally follow the threshold of admissibility by transforming borders into zones of data-driven triage (Amnesty International, 2024; EDRi, 2021).

As the FRA (2020) highlights, predictive analytics used at borders carry the risk of embedding discriminatory biases, especially when relying on incomplete or skewed datasets. This risk is particularly acute in migration contexts, where individuals from conflict-affected or authoritarian countries -who may have legitimate protection claims- can be unfairly flagged as security threats due to their nationality, biometric anomalies, or travel histories. Reports by Amnesty International (2024) and EDRi (2021) have shown that such systems disproportionately flag individuals from Afghanistan, Syria, Somalia, and the Sahel region as "threats", contributing to increased detentions, pushbacks, and denials of entry. These are not abstract concerns. Investigations into Frontex surveillance operations at the Greek-Turkish

border have documented how drone surveillance and automated alert systems were used to intercept and return migrants -without registration or access to asylum procedures- (Sunderland and Pezzani, 2022).

Additionally, AI-driven surveillance tools -such as automated border towers, drone fleets, and thermal imaging cameras- are now deployed along the European Union's southern and eastern frontiers. These technologies are often justified as "neutral" or "efficient," but they facilitate remote monitoring and externalization, shifting migration control from legal frameworks to automated deterrence regimes (Molnar, 2020). As noted in the McGregor & Molnar's report *Digital Border Governance: A Human Rights-Based Approach* (2023), the deployment of digital border technologies can create systems that are both omnipresent and invisible, disproportionately affecting individuals who already face racial and ethnic profiling.

Moreover, the increasing digitization of visa systems and pre-travel authorizations raises access concerns. As highlighted in the European Commission's Ethics Guidelines for Trustworthy AI (2019), automated visa rejection tools may deny applications based on travel history, digital profiles, or indirect risk indicators, often without offering explanation or recourse. The OHCHR (2021) and Amnesty International (2021) document how these platforms exclude migrants with low digital literacy, lack of ID documentation, or inconsistent internet access, effectively replicating pre-existing global inequalities in access to mobility.

One especially concerning example is the deployment of facial recognition technologies at European Union external borders. The FRA (2018) and subsequent studies confirm that such systems have higher error rates when used to identify racialized individuals, women, and children. These inaccuracies result in false positives, leading to unjustified detentions, secondary screenings, or outright denial of entry. Moreover, the use of emotion detection systems -intended to read non-verbal cues during border interviews- has been criticized by scientists and legal experts alike as pseudo-scientific and discriminatory, reinforcing harmful stereotypes about perceived deception or emotional instability (OHCHR, 2021).

These technologies also enable digital profiling and preemptive exclusion. Rather than evaluating migrants on an individual basis, automated tools operate on statistical generalizations that fail to account for lived experiences, socio-political contexts, or specific

legal rights. This kind of algorithmic border control turns freedom of movement into a function of data compatibility, not legal status (Amnesty International, 2021). As Molnar (2020) argues, this shift turns the border into a site of filtration rather than legal reception, reducing freedom of movement to a matter of data compatibility rather than legal entitlement.

Additionally, the privatization of border technologies raises serious concerns about accountability. Many of the surveillance and profiling tools used at European Union borders are developed and maintained by private technology firms. These companies are not subject to the same human rights obligations as public authorities, creating a governance gap. As highlighted in the *Balsillie Papers on Technology at the Borders: Surveillance, Control and Resistance in European Union Migration Governance* (2025), outsourcing border functions to non-state actors undermines transparency and often results in systems that prioritize efficiency over rights.

In essence, while the European Union promotes freedom of movement within its internal borders, it simultaneously constructs digital barriers at its periphery. These barriers are rarely codified in law or policy documents but are implemented through technological infrastructures of exclusion—facial recognition, biometrics, drones, and automated risk assessment systems. For migrants, asylum seekers, and stateless individuals, these tools function as invisible yet impenetrable walls that screen, classify, and deny access before a legal process even begins (McGregor & Molnar, 2023; Amnesty International, 2024).

To uphold freedom of movement as a substantive right, the European Union must ensure algorithmic transparency, prohibit unscientific profiling, guarantee human review, enforce anti-discrimination safeguards, and provide accessible visa and entry systems (FRA, 2020; EDRi, 2021).

3.2.4 Right to an Effective Remedy and Fair Trial

The right to an effective remedy, codified in Article 47 of the Chapter of Fundamental Rights of the European Union and Article 13 of the European Convention Human Rights, ensures that individuals whose rights have been violated have access to a fair, impartial, and competent tribunal. In the migration context, this right is particularly vital given the life-altering consequences of administrative decisions related to deportation, detention, denial

of asylum, and exclusion from European Union territory. As migration governance increasingly incorporates automated decision-making systems (ADM) and AI-driven tools, this fundamental right faces unprecedented threats (UNHCR, 2021; FRA, 2020).

At the heart of this issue lies the opacity and complexity of algorithmic logic. Many asylum seekers, migrants, and stateless persons are unaware that their cases have been evaluated using machine learning models or biometric matching systems. They are rarely informed of the criteria, data sources, or risk profiles used in decision-making. As the OHCHR (2021) warns, the opacity of AI systems can effectively strip individuals of their right to understand and contest decisions that affect them. This denial of explainability effectively renders legal challenge impossible, thereby hollowing out the very notion of effective remedy.

According to Amnesty International (2021), these technological systems often operate without meaningful human oversight and lack clear procedures for appeal or redress. For example, if a traveler or asylum seeker is denied entry at a smart border due to a false positive generated by a facial recognition system, they may be unable to identify the reason, dispute the result, or demand correction. In practice, this removes the legal personhood of the individual and replaces it with a data identity -one governed by inaccessible and unchallengeable rules-.

In this sense, The International Commission of Jurists has raised concerns about the impact of digital border technologies on access to justice, noting that AI-enabled migration tools can undermine principles such as equality of arms and the right to a reasoned decision. In migration procedures where time is critical and the margin of error small, lack of procedural safeguards in digital systems can result in irreversible harm, including deportation to unsafe countries or prolonged arbitrary detention (International Commission of Jurists, 2022).

Moreover, appeal mechanisms, even where they exist formally, are often functionally inaccessible. Many migrants face significant barriers due to lack of language support, legal assistance, digital literacy, or access to the internet. According to EDRI (2021) and ENNHRI (2024), the procedural complexity of challenging an algorithmic assessment far exceeds the capabilities of most individuals -even more so for people in detention, remote camps, or undergoing rapid deportation procedures-. Without legal aid and technological transparency, the right to an effective remedy becomes illusory.

These deficiencies are not merely theoretical. In the *M.S.S. v. Belgium and Greece* case (ECtHR, 2011), the Court found that Greece's asylum system violated Article 13 ECHR due to lack of effective remedies and procedural fairness. Although this case predates the current AI-driven environment, its core finding -that systemic deficiencies in procedural safeguards amount to a human rights violation- applies even more urgently today. If algorithmic systems exacerbate those deficiencies, they may directly contribute to violations of international human rights law.

Further concerns arise from the speed and scale at which automated systems operate. As The Alan Turing Institute (2021) emphasizes, the velocity of ADM in migration control makes it difficult for human actors to intervene before harm occurs. The burden of proof often falls on the migrant, who must somehow prove that a machine was wrong. This reverses traditional due process norms and elevates the state's technological capacity above the individual's legal status.

A remedy is not only a right of last resort, but also a mechanism for accountability and democratic governance. If digital migration systems lack pathways for redress, they also lack legitimacy. According to the ENNHRI Scoping Paper (2024), National Human Rights Institutions across Europe report growing concern that border technologies are being implemented without clear oversight frameworks, legal audit procedures, or channels for complaints. This regulatory vacuum undermines the rule of law and risks fostering forms of unchecked digital control and exclusion at the border.

To comply with Article 47 CFR and Article 13 ECHR, the European Union and its member states must ensure transparency by design, including the right to information on how ADM systems function, guarantee human review of impactful decisions, provide accessible complaint mechanisms, fund legal aid for migrants, and establish public algorithmic audit bodies (FRA, 2020; OHCHR, 2021).

3.2.5 Prohibition of Torture and Inhuman or Degrading Treatment

The absolute prohibition of torture and inhuman or degrading treatment is one of the most fundamental principles of human rights law, enshrined in Article 3 of the ECHR and Article 4 of the Charter of Fundamental Rights of the European Union. Traditionally applied to cases

of physical abuse or detention conditions, this right is now being reinterpreted in light of psychological harm, prolonged uncertainty and digital forms of exclusion and surveillance facilitated by migration technologies (McGregor & Molnar, 2023; UNHRC, 2021).

Asylum seekers may be subjected to prolonged delays, algorithmic misclassifications, and opaque risk assessments that result in wrongful denials or indefinite uncertainty. These conditions can lead to severe mental distress, particularly when individuals are detained or stranded in unsafe border zones without access to legal or humanitarian assistance. According to the United Nations Special Rapporteur on Torture (2020):

“Practices typical of contexts marked by systemic governance failures, or by the persecution of individuals or groups, include sustained institutional arbitrariness that fundamentally betrays the human need for communal trust and, depending on the circumstances, can cause severe mental suffering, profound emotional destabilization, and lasting individual and collective trauma. In the view of the Special Rapporteur, when institutional arbitrariness or persecution intentionally and purposefully inflicts severe mental pain or suffering on powerless persons, it can constitute or contribute to psychological torture. In practice, this question is of particular, but not exclusive, relevance in relation to the deliberate instrumentalization of arbitrary detention and related judicial or administrative arbitrariness (A/HRC/43/49, para. 63, p. 17).”

A key legal precedent is the case of *M.S.S. v. Belgium and Greece* (ECtHR, 2011), where the Court found that the failure of Greece’s asylum system, particularly in providing humane conditions and fair access to procedures, constituted inhuman and degrading treatment under Article 3. While the case did not directly involve digital technologies, the Court emphasized that systemic dysfunction and psychological suffering caused by state negligence can reach the threshold of prohibited treatment. Today, this reasoning is applicable to automated systems that produce arbitrary results or isolate individuals from legal remedies (McGregor & Molnar, 2023).

Similarly, the European Center for Constitutional and Human Rights documented cases of pushbacks at the European Union’s external borders facilitated by thermal cameras, artificial intelligence systems, and drone surveillance coordinated by Frontex. These technologies enabled the covert expulsion of migrants, who were never formally registered and

consequently denied access to asylum procedures. Such practices violated essential procedural safeguards and exposed individuals to serious risks, including violence and abandonment (ECCHR, 2021). Likewise, a 2025 investigation by the European Committee for the Prevention of Torture (CPT) condemned the conditions in Italy's migrant detention centers, where detainees were held in degrading circumstances with insufficient access to medical care and legal support. The report emphasized how digital tools -used to flag individuals based on identity markers or movement histories- often failed to account for the specific needs of each person, thereby reinforcing systemic neglect rather than enhancing protection (AP News, 2025).

Another concern lies in the psychological effects of constant biometric surveillance. Technologies such as iris scanning, gait detection, facial recognition, and emotion analysis are deployed under the logic of "security enhancement," but often reinforce a presumption of guilt. As Amnesty International (2024) warns:

"Digital technologies are reinforcing border regimes that discriminate based on race, ethnicity, national origin, and citizenship status. Inherent racism is deeply ingrained within migration management and asylum systems. These technologies risk perpetuating and concealing racial biases and discrimination under the guise of neutrality and objectivity rooted in historical and colonial practices of racialised exclusion" (p. 4).

This framing not only reduces individuals to data points but also contributes to a broader culture of suspicion and exclusion that disproportionately targets racialized migrants.

Among the most controversial and invasive of these tools are emotion recognition systems. These AI tools claim to detect fear, deception, or aggression in asylum seekers based on facial expressions or vocal cues. But according to Forster (2022), such systems lack scientific credibility and embed racial and cultural bias, posing serious risks of dehumanization. As highlighted in the McGregor & Molnar's (2023) report, the use of artificial intelligence to interpret emotions or intentions during asylum interviews undermines individual agency and poses a serious risk of arbitrary rejection decisions, ultimately compromising the dignity and rights of the persons involved.

The detention of migrants flagged by flawed digital systems also remains a major concern. Many automated border control tools do not provide human oversight or appeal mechanisms,

leading to arbitrary detentions based on faulty classifications. As noted by Tschalaer et al., (2023) and the FRA (2024), migrants flagged as “security threats” often face prolonged confinement without due process, even when there is no evidence beyond the digital profile.

Moreover, long-term confinement in environments of technological opacity and institutional indifference leads to conditions of profound disempowerment, fear, and trauma. These outcomes are not side effects but are increasingly structural in nature -products of systems that prioritize automation over individualized care and security over rights- (Amnesty International, 2024).

To meet its obligations under Article 3 ECHR and Article 4 CFR, the European Union must:

- Prohibit the use of emotion-recognition systems and other unvalidated AI tools in migration contexts.
- Ensure that digital surveillance and biometric tracking are proportionate, rights-compliant, and subject to independent oversight.
- Guarantee that migrants have access to individual assessments, legal aid, and psychological support.
- Implement a moratorium on technologies that facilitate unregistered pushbacks, arbitrary detention, or procedural exclusion. (FRA, 2020).

3.3 Discriminatory Practices and Racism in European Union Border Management

The increasing reliance on digital technologies for migration control in the European Union has raised significant legal and ethical concerns, particularly regarding systemic racism and discriminatory practices embedded in border governance. As noted in the *ENAR Shadow Report: Racism and Discrimination in the Context of Migration in Europe* (2017), African migrants in need of humanitarian protection were frequently misclassified as "economic" or "illegal" migrants without adequate individual assessment. This reflects a systematic

tendency within European Union Migration policy to socialize migrants, treating individuals from specific backgrounds as inherently less worthy of rights and protections.

The *Fundamental Rights Report* by FRA (2024) further underscores that the use of algorithmic systems in border control risks embedding historical biases. These concerns are not hypothetical. For instance, FRA notes that risk profiling mechanisms at several European borders often categorize travelers from North African or Middle Eastern countries as “high risk” solely based on nationality or region of origin, leading to disproportionate targeting for biometric checks and detentions. Automated systems often reflect the biases present in their training data, leading to discriminatory outcomes that disproportionately affect marginalized groups. However, the lack of statistical data concerning traditionally marginalized communities, due to historical and ethical concerns around the collection of sensitive personal data in Europe, makes it difficult to consistently identify and assess these risks. As a result, introducing new requirements for statistical evidence to monitor algorithmic discrimination may paradoxically risk further marginalizing the very groups it seeks to protect (Wachter et. al., 2020).

Concrete parallels can be drawn from the Americas. In *The Everywhere Border: Digital Migration Control Infrastructure in the Americas*, Aizeki et. al., (2023) describe how a Salvadoran migrant was criminalized based on digital surveillance: merely replying “OK” in a WhatsApp group used by a migrant caravan was presented as evidence of smuggling activity. The case exemplifies how digital tools can serve as mechanisms for racialized suspicion and criminalization. While this example comes from Central America, the logic it reveals is not dissimilar to European practices. For instance, in Greece, migrants from racialized groups are regularly subjected to automated screening processes where lack of documents or perceived “inconsistencies” in biometric data -often the result of poor capture or system errors- trigger prolonged detentions (Amnesty International, 2024).

Aizeki et al., (2023) also describe how the United States Department of Homeland Security extends its surveillance reach beyond United States territory through partnerships with countries like Mexico and Guatemala to install biometric databases and checkpoint systems. These infrastructures disproportionately impact Black and Indigenous migrants, whose visibility to digital systems often means enhanced scrutiny. Similarly, in the European Union, the interoperability of border systems -such as Eurodac, SIS II, and the EES- means that

racialized migrants are permanently recorded and tracked across member states, often without clear pathways to challenge or correct this data.

In both contexts, these practices reflect a broader phenomenon that scholars describe as “digital racial borders”. As noted in *Why challenging discrimination at borders is challenging (and often futile)* (2021), this term captures how surveillance infrastructures render racialized migrants hyper-visible as threats, while simultaneously erasing their legal protections and narratives. In the European Union, this manifests not only in profiling at border crossings but also in predictive policing algorithms used to anticipate “migration flows” from African countries, based on opaque data sets that may reinforce colonial assumptions (Molnar, 2020).

Moreover, discriminatory outcomes are often exacerbated by the opacity and permanence of these systems. Amnesty International (2024) documents how digital watchlists and biometric data, once entered into databases like Eurodac, follow individuals for years—regardless of the outcome of their asylum cases. Similarly, in the Americas, Aizeki et al., (2023) highlight how shared biometric systems between governments and private contractors entrench long-term surveillance over specific populations, particularly racialized and undocumented migrants.

In sum, addressing discrimination in European Union migration management requires more than technological reform; it demands a fundamental reevaluation of how digital infrastructures replicate and deepen racial hierarchies. As Leurs (2023) argues, the comparative analysis with the Americas reinforces that the challenges of digital racial profiling and surveillance are transnational. As such, any serious effort to uphold human rights in digital border governance must confront the structural logics of race, colonialism, and exclusion that underpin both policy and technology (Amnesty International, 2021).

3.4 Accountability and Transparency in Digital Migration Management

Transparency and accountability are foundational principles in the ethical and legal governance of digital technologies used in migration management. In the European Union, these principles are codified in legal instruments such as the General Data Protection Regulation (GDPR) and the Law Enforcement Directive. Article 5(1)(a) of the GDPR mandates that personal data must be “processed lawfully, fairly and in a transparent manner

in relation to the data subject” (GDPR, Art. 5(1)(a)). Articles 13 and 14 further require data controllers to inform individuals about “the purposes of the processing for which the personal data are intended,” “the period for which the personal data will be stored,” “the identity and the contact details of the controller,” and “the existence of the right to request access, rectification or erasure” (European Parliament and Council of the European Union, 2016).

Despite these provisions, in practice, significant transparency gaps persist, particularly when viewed from the migrants’ perspective. According to the European Union Agency for Fundamental Rights, many asylum seekers were unaware of why their fingerprints were taken, how their data would be used, or which databases their biometric information would be stored in. In this sense, an apprehended Ivorian migrant interviewed recalled: “When it comes to fingerprints, I have not heard anybody say anything about that, I mean about the purpose. It was afterwards that I heard people who were together with me say that these fingerprints would be used in a European database” (FRA, 2018, p. 35).

In addition to the findings by FRA, similar concerns are raised in the research of Molnar (2019), who conducted fieldwork at several European border regions. Migrants interviewed described being subjected to biometric and surveillance technologies without clear explanations or the ability to give meaningful consent. These accounts reinforce how experimental and often opaque technologies in migration management bypass principles of transparency and accountability, leaving migrants with little understanding of how their data is processed, stored, or shared, and with minimal avenues for contestation.

This lack of awareness is not accidental but symptomatic of broader inconsistencies across European Union databases in how the right to information is implemented. As illustrated in Table N° 1, the legal obligations for informing migrants about data collection, usage, and sharing vary significantly across systems such as Eurodac, SIS II, VIS, and ETIAS. While some instruments contain clear provisions on the right to information, others either omit these entirely or apply them with notable restrictions. The table also shows that many systems fail to ensure that information is presented in an understandable manner or to disclose whether data might be shared with third countries -further undermining informed consent and legal transparency-.

Table N° 1: The right to information when data are collected, existing and planned European Union IT systems

	Eurodac Regulation and proposal	VIS	SIS II Decision and police proposal	SIS II Regulation and borders and return proposals	EES Regulation	ETIAS proposal	ECRIS-TCN proposal	Interop. proposals (BMS, CIR and MID)
Instrument has a provision on the right to information	yes	yes	no	yes, with restrictions	yes	yes	no	yes
Information must be provided in an understandable manner	yes	no	n/a	no	yes	no	n/a	no
Information must include that data determining the Member State responsible for the asylum procedure	yes	yes	n/a	n/a	n/a	n/a	n/a	yes
Information must include that data apprehension and return purposes	no	yes	n/a	yes, with restrictions	yes	n/a	n/a	yes
Information must include that data investigations of serious crimes and terrorism	yes	yes	n/a	yes with restrictions	yes	no	n/a	yes
Data subject must be informed about possible data sharing with third countries	no	yes	n/a	n/a	yes	n/a	n/a	n/a

Note: Proposed systems and proposed changes in *italics*.
n/a = not applicable.

Source: FRA (2018)

The fragmented implementation of the right to information -evident in aforementioned Table- not only creates legal inconsistencies across European Union digital systems but also translates into practical confusion and procedural harm for migrants. These inconsistencies are reflected in the widespread lack of awareness among asylum seekers regarding the collection and use of their biometric data. According to FRA's research, even where legal provisions exist, information is often delivered in inaccessible formats, unknown languages, or during moments of acute distress, undermining any genuine understanding (FRA, 2018).

This disparity is evident across multiple European Union countries, where only a small percentage of migrants recall being clearly informed about fingerprinting procedures. In Greece and Hungary, for instance, fewer than 20% of surveyed individuals reported that they had been told why their biometric data was being collected or how it would be used (FRA, 2018). Firsthand testimonies confirm this lack of transparency and contradictory information:

“An Ethiopian woman interviewed in Sweden explained that she did not understand why the Dutch authorities took her fingerprints and that she was not informed about the purpose or the procedure for which they were collected. The authorities simply told her that she was imprisoned because she had come illegally to the Netherlands and used someone else’s passport” (p. 33).

Furthermore, transparency failures are often compounded by language barriers and institutional negligence. As one Polish female that works at the Asylum and Immigration Agency noted:

“A foreigner, when they have obtained information, very often might confirm that they have understood it when they did not. Even from my personal experience, I know that the language has to be simple and the message has to be straightforward and descriptive. What I mean is, it should be explained why a certain activity has to be conducted. And so on. Because, even if the foreigner admits that they understand, they do not necessarily know what it is about. Even for very basic matters” (FRA, 2018, p. 34).

In such circumstances, what is legally required as informed consent becomes a procedural formality -technically fulfilled, but substantively void of comprehension and dignity-. The effect is a performative transparency regime that offers migrants little in terms of control or clarity, even when their rights are nominally protected.

The issue becomes even more critical with the use of facial recognition technology (FRT) and AI-based risk assessments in border control. These tools often operate as “black boxes”, where the logic behind decisions is opaque -even to those who operate them-. Wachter, et. al., (2020) argue that the opacity of algorithmic systems makes it difficult to establish accountability for decisions, as the logic behind these systems is often inaccessible

This opacity is reflected in concrete instances such as in the Netherlands, where predictive analytics tools have been deployed to assess asylum claims and detect potential cases of “identity fraud”. However, a 2020 ruling by the District Court of The Hague found that the system’s lack of transparency and the potential for racial bias violated fundamental rights. This case underscores the risks posed by opaque algorithmic technologies, particularly when legal safeguards are insufficiently robust or inadequately enforced. Furthermore, the complexity of data flows in automated asylum procedures complicates transparency even

more. Biometric data collected through systems like Eurodac often feed into risk analysis platforms such as ETIAS, which in turn influence decision-making processes. These interconnected systems create multiple points where clarity about how data is used or shared can be lost, making it difficult for migrants or oversight bodies to fully understand or challenge decisions based on algorithmic assessments.

Transparency is not only about informing individuals -it is also essential for fostering public oversight and trust in migration governance-. As McGregor & Molnar (2023) emphasizes, without transparency, individuals are unable to understand or contest how data-driven decisions are made. Similarly, Garriga Domínguez (2024) stresses that transparency must extend beyond policy declarations and include concrete mechanisms such as human rights impact assessments, the creation of public registers of algorithms, and the establishment of avenues for independent audit and appeal. These measures are essential to ensure accountability in the deployment of digital technologies affecting migrants and asylum seekers.

In short, if biometric and AI-driven technologies are to be used in a rights-compliant manner, public authorities must embed transparency and accountability into every layer of design and implementation. This includes accessible information campaigns, real-time translation, consent mechanisms, and independent oversight structures. As the FRA (2019) emphasizes, transparency, oversight, and accountability are essential safeguards in the deployment of such technologies, particularly in law enforcement settings.

3.5 The evolving regulatory framework

While existing European legal instruments -such as the General Data Protection Regulation (GDPR) and the Charter of Fundamental Rights- provide foundational protections, the increasing integration of AI into migration management has exposed deep regulatory and normative gaps. These developments reflect a broader conflict between security-driven legislative agendas and the protection of fundamental rights. As Beduschi and McAuliffe (2021) observe, the deployment of AI in migration systems “risks undermining human rights protections when legal and ethical safeguards are not systematically embedded in system design and implementation” (p. 5). In particular, migrants and refugees often experience

limited ability to understand, contest, or appeal decisions made by algorithmic tools used in identity verification, risk profiling, or border screening.

This tension is heightened by the asymmetrical legal subjectivity imposed on migrants. Unlike European Union citizens, third-country nationals often lack full procedural guarantees under European Union law, meaning they face a double vulnerability: both as targets of securitized digital systems and as legal outsiders (Garriga Domínguez, 2024). Even when remedies exist in theory -such as the right to contest data processing under the GDPR- these rights may be practically inaccessible due to lack of translation, legal aid, or digital literacy. As the Platform for International Cooperation on Undocumented Migrants (PICUM, 2022) emphasizes, migrants are often treated not as rights-holders but as data objects, subject to opaque systems they cannot interrogate or influence.

The European Commission's Regulation on Artificial Intelligence (AI Act, 2021) marked a significant legislative effort to govern AI use across sectors, including migration. It categorizes AI systems used in border control, lie detection, and visa processing as "high-risk" and imposes obligations on risk management, data governance, transparency, and human oversight. However, as FRA (2020) notes, even these high-risk classifications fail to fully account for the vulnerabilities of migrants, who may lack the means to challenge automated decisions or access redress mechanisms, especially when systems operate across multiple jurisdictions and databases, such as SIS, VIS and Eurodac.

The limitations of existing legal regimes are not solely technical but deeply institutional. Beduschi and McAuliffe (2021) emphasize that AI systems often magnify existing power asymmetries in migration governance, and without clear accountability frameworks, "discrimination, opacity, and injustice risk becoming embedded in these new governance tools" (p. 7). While the GDPR remains a cornerstone of the European Union's data protection regime, it was not designed to account for the complexities of algorithmic profiling and real-time biometric surveillance. As Wachter et al., (2020) argue, current regulatory frameworks are not fully equipped to handle the complexities of algorithmic decision-making, particularly in contexts where fundamental rights are at stake.

Garriga Domínguez (2024) similarly emphasizes that the increasing reliance on biometric systems incorporating AI demands specific legal frameworks beyond data protection, including rules on algorithmic explainability, human oversight, and fundamental rights

impact assessments. A rights-based approach requires legal mechanisms that not only regulate technical performance but also uphold accountability and the ability to contest decisions, especially in border settings where individuals often face limited access to remedies.

The expansion of Frontex's mandate through Regulation (European Union) 2019/1896 (2019) intensified these concerns. The regulation empowered Frontex to collect and process vast amounts of personal and biometric data, deploy surveillance drones, and engage in joint operations with third countries. As Amnesty International (2024) has warned, this consolidation of digital surveillance and operational authority often comes at the expense of transparency and fundamental rights. Technologies employed by Frontex -such as facial recognition and data fusion systems- have the potential to function as instruments of exclusion, discrimination, and even violence. This is particularly visible in allegations of illegal pushbacks at sea and land borders, many of which have been digitally coordinated through surveillance infrastructures operated or funded by Frontex¹¹.

Moreover, legal scholars and NGOs have stressed that the current legal landscape is ill-equipped to address the structural discrimination embedded in these technologies. Redpath (2007) argues that the digitization of borders reproduces racialized hierarchies of mobility, stating that digital tools operationalize suspicion and filter access to territory based on algorithmically inferred risk -often correlating with race, nationality, and perceived threat-. Similarly, the European Digital Right Initiative (EDRi, 2020) emphasizes, that “considering the potential data protection, non-discrimination, broader fundamental rights and collective harms at stake from data-driven profiling, automated-decision making in the field of law enforcement and policing, it is vital that the European Commission ensures adequate legal protection and prevention against harms emanating from data-driven profiling and policing” (p. 6-7).

An example that illustrates the consequences of inadequate legal oversight is the deployment of iBorderCtrl, a pilot project funded by the European Union that included emotion detection AI at borders. It aimed to assess the veracity of asylum seekers' statements by analyzing facial micro-expressions, a method heavily criticized for scientific unreliability and ethical dangers (Wachter et al., 2020; McGregor & Molnar, 2023). Despite public backlash and

¹¹ See the European Parliament's decision (2023) on Frontex's failure to ensure accountability in pushback-related surveillance activities.

expert warnings, this system received funding and support under the Horizon 2020 program, raising concerns about how ethical review processes are conducted within European Union institutions.

The problem is not merely technical but also institutional. As the *Platform for International Cooperation on Undocumented Migrants* (2022) underscores, the opacity of border AI systems is compounded by the lack of meaningful consultation with affected communities. Migrants and refugees are often treated as data subjects rather than rights holders, with little involvement in shaping the technologies that govern their lives.

Despite the AI Act's potential, critical gaps remain. The regulation does not address the cumulative effects of multiple surveillance systems nor does it ensure accessibility to remedies across member states. Furthermore, as FRA (2019) points out in its assessment of facial recognition technologies, there is insufficient coordination between law enforcement, border authorities, and data protection bodies, resulting in legal uncertainty and potential rights violations.

In light of these limitations, legal scholars have increasingly called for a reorientation of digital migration governance toward a structural and participatory legal framework. Wachter, et al., (2020) contend that “fairness cannot be automated”, particularly in systems that replicate structural inequalities based on race, nationality, or socioeconomic status. Tazzioli (2020) adds that the datafication of migration embeds colonial logics into contemporary border infrastructures, transforming racialized populations into algorithmic risks. These critiques point toward the need for anti-discrimination law and administrative justice reforms that align with the emerging realities of automated governance.

At present, the AI Act does not ensure cross-border coherence, nor does it provide sufficient clarity on who is accountable when rights are violated by hybrid public-private digital systems. As Leurs (2023) points out, migration control in the European Union is increasingly governed by hybrid assemblages involving tech companies, national authorities, and supranational agencies. Yet, the regulatory framework still primarily addresses state obligations, leaving gaps in areas such as procurement transparency, private sector liability, and public interest litigation.

Ultimately, as Beduschi and McAuliffe (2021) and others argue, the development of AI systems for migration must be guided by principles of legality, necessity, proportionality, and

non-discrimination from the outset—not retroactively addressed through weak accountability mechanisms. Without a structural and anticipatory regulatory model, digital migration systems will continue to deepen inequalities and erode the rights of those most in need of protection.

3.6 Concluding remarks

This chapter has examined the profound legal and ethical implications of the digital technologies currently deployed in European Union migration management. Through a critical lens, it has shown how systems meant to enhance efficiency and security are simultaneously reshaping the experience of rights, often to the detriment of the most vulnerable populations. As digital infrastructures become increasingly central to border governance, core principles such as human dignity, the right to asylum, and access to justice are not only strained but sometimes actively undermined. Far from being neutral or purely technical, these tools carry embedded logics of control, classification, and exclusion that risk turning legal protections into procedural illusions.

One of the most striking outcomes of this analysis is the extent to which digital technologies reconfigure power at the border. Automated decision-making systems, biometric databases, and AI-powered surveillance operate through layers of opacity, making it difficult for migrants to understand, challenge, or even recognize the mechanisms shaping their legal status. In this context, the right to an effective remedy becomes increasingly theoretical, as individuals are transformed into data profiles, assessed and filtered by opaque algorithms with limited avenues for redress. The result is a governance model where accountability is diffused and procedural safeguards are often bypassed in favor of operational objectives.

The deployment of these technologies also amplifies longstanding structural inequalities. Racialized and marginalized groups are disproportionately subject to invasive surveillance and algorithmic suspicion, reinforcing discriminatory patterns under the guise of objectivity. Furthermore, the involvement of private actors and the lack of coherent oversight mechanisms deepen the accountability deficit. Legal instruments such as the GDPR and the proposed AI Act represent important steps forward, but they remain insufficient to fully address the distinct vulnerabilities of migrants within increasingly digitized systems. The

existing regulatory landscape is fragmented, reactive, and often unable to keep pace with technological developments or cross-border data practices.

Ultimately, this chapter underscores that digital migration governance must be approached not solely through the lens of innovation or security, but with a sustained commitment to legality, transparency, and fundamental rights. Addressing the challenges posed by biometric and algorithmic technologies requires more than technical adjustments; it demands a structural rethinking of how migration is governed in the digital age. This involves embedding human rights principles into the very design and deployment of these tools, ensuring meaningful human oversight, and recognizing migrants not as data subjects or risk profiles, but as individuals entitled to dignity, protection, and justice. Only through such an approach can the European Union uphold its legal commitments and foster a migration governance system that is both effective and ethically sound.

Final Conclusion

The digital turn in European Union migration and border governance represents far more than a shift in technological tools. It reflects a profound transformation in the underlying logic through which mobility, identity, and rights are conceptualized and regulated. AI in the fields of migration and mobility is not a recent development, but its role has evolved significantly in recent years. The rise of advanced computational capabilities, breakthroughs in technology, and the growing availability of vast amounts of data have created an ideal environment for its rapid growth and wider application today.

As this thesis has demonstrated, the deployment of digital technologies -biometric systems, algorithmic decision-making, and large-scale data infrastructures- has reconfigured the landscape of migration management in ways that often reinforce exclusion, entrench inequality, and challenge the very foundations of legal protection and democratic accountability.

What began as a historical and conceptual inquiry into the evolution of border control has revealed a structural trend: the normalization of a techno-political regime that operates through opacity, automation, and predictive control. The border is no longer a fixed territorial line but a dispersed, data-driven system embedded in databases, surveillance networks, detention centers, and humanitarian infrastructures. Migrants are increasingly reduced to data points -monitored, categorized, and managed- rather than recognized as individuals with rights, needs, and stories.

The integration of AI in the control of the European Union's external borders has marked a milestone in the management of security and migration. Systems such as SIS, VIS, EES, and Eurodac, together with ETIAS, demonstrate the complexity and diversity of AI-driven tools used to strengthen border security. These systems, backed by Frontex and eu-LISA, have significantly improved efficiency in threat identification and in the management of migratory flows.

Artificial intelligence clearly offers a range of benefits for both policy and operational practice. Its ability to process and analyze large volumes of data can streamline repetitive or resource-intensive tasks, making migration management more efficient. When designed and implemented responsibly, AI tools can also speed up identity verification at border crossings and help authorities detect individuals who may present security concerns.

Examples of promising applications can be found in machine-learning tools that support the placement of refugees by analyzing data to match individuals with suitable resettlement locations, as well as chatbots that provide migrants with accurate information and advisory services in their host countries. In addition, there is growing interest in AI's potential to anticipate displacement patterns and assess which communities may be at risk, allowing authorities to respond more effectively to sudden influxes and to better honor their human rights obligations.

The fundamental rights implications of using biometrics technology vary considerably depending on the purpose, context and scope of the use. Although applications may be designed to be neutral, machine-learning algorithms can be trained to discriminate or can incorporate the biases of the programmer. This can occur due to prior learning or the nature of the dataset used for training. Human migration is too complex to be reduced to an algorithm, and digital border technologies carry certain risks because they can embed racial and gender biases. The use of biometric profiling can lead to unfair practices and discrimination.

At the same time, the use of drones for border surveillance raises its own set of legal and ethical challenges, particularly in relation to the obligation of non-refoulement -a cornerstone of international refugee and human rights law-. The dominant narrative that presents drones as highly efficient, innovative, and precise tools can obscure the fact that certain characteristics of this technology -such as its depersonalization, reduced human presence, and enhanced detection and data-sharing capabilities- do not erase the fundamental humanitarian and human rights dimensions of search and rescue operations at sea. This dynamic carries a serious risk: that the interception of people fleeing persecution, torture, or other forms of inhumane treatment is treated as a routine or neutral event, detached from its legal and human significance.

Technology has become a pervasive and contested element in shaping and implementing state policies on migration and asylum. Its deployment can sustain and intensify systemic racism, discrimination, and social exclusion, often serving to justify xenophobic narratives, policies, and institutional practices. When state policies run counter to their human rights obligations, technological tools can deepen and amplify those breaches. At the same time, the digital platforms and automated systems used in asylum and migration management are themselves

fraught with vulnerabilities -from algorithmic bias and error to threats against privacy, protection from discrimination, and other fundamental rights-.

Biometric and algorithmic systems, central to this digital architecture, are frequently justified in the name of efficiency and security. Yet in practice, they introduce new and deeply consequential forms of vulnerability, especially for those already marginalized by race, legal status, or socioeconomic background. These technologies are not passive tools; they actively shape decisions about who may enter, stay, or be deported, often through mechanisms shielded from public scrutiny and legal challenge. The migrant body becomes both a site of verification and a target of suspicion, and the right to asylum or effective remedy is increasingly mediated by automated processes that many cannot understand or contest.

The digitalization of migration governance, as shown throughout this thesis, is not neutral. It is embedded in a broader securitization narrative that frames migration as a threat rather than as a human and political reality. This framing legitimizes a border regime oriented around deterrence and control rather than justice and solidarity. The deployment of technologies under these narratives not only distorts the role of the state but also erodes the rights-based foundations of the European Union's legal order. Migrants, far from being recognized as rights-bearing individuals, are recast as algorithmically generated risks-preemptively managed and selectively excluded.

Researchers have increasingly turned their attention to the role that digitisation, datafication, automation, and artificial intelligence play in border control and migration governance. These innovations, and the ways they have been examined by geographers and other scholars, build upon long-standing methods of mobility control that have gradually become normalized over time. What characterises the latest phase of migration digitisation is its emphasis on integrating and connecting different technologies and platforms, harnessing advanced computational tools for analysis and decision-making, and employing them not just to respond to migration flows, but also to anticipate and shape them. Recent reviews of this trend trace its emergence within political narratives of crisis, its entanglement with new economic dynamics, and its deep connections to questions of mobility, solidarity, and ethics.

Digitisation and datafication of migration manifest technological infrastructures that articulate with the elaboration of regulatory designs for migration management. So too are digital platforms evidentially becoming part of the intermediated negotiation and

circumvention of migration and border control. Yet, as these technologies evolve and embed themselves in the architecture of migration governance, questions arise about the adequacy of the legal and normative frameworks meant to govern their use.

While legal instruments such as the General Data Protection Regulation (GDPR) and the proposed AI Act provide an initial framework for addressing some of these concerns, they remain fragmented, reactive, and largely insufficient. They often focus narrowly on abstract data protection rather than grappling with the lived realities of those most impacted. Moreover, enforcement mechanisms are generally weak, and binding obligations specific to migration governance are largely absent, leaving significant gaps in accountability. In this context, a more just and equitable approach to digital migration governance must recognize the deeply political nature of technological design and deployment. Technologies are not neutral tools; they carry the assumptions, biases, and priorities of those who create and implement them, and their role in shaping migration is inseparable from the structures of power that govern mobility.

Reimagining the role of digital tools in migration governance, then, requires a fundamental shift, not only in regulation but also in vision. Human rights must be embedded within the very architecture of digital systems, ensuring procedural transparency, meaningful oversight, and accessible mechanisms for those affected. To this end, an independent monitoring mechanism should be established, with access to data, algorithms, and decision-making processes, to review, assess, and recommend changes that uphold fundamental rights. Oversight and redress must be binding and accessible, guaranteeing that automated or digital decisions can be contested, and a human-in-the-loop requirement should be introduced to mitigate discrimination and error. Judicial review must be reasserted, closing the accountability gaps created by externalised and digital controls and making digital borders legible within the rule of law. This means making opaque and extraterritorial practices subject to scrutiny, and embedding robust accountability at the design level of these technologies.

More broadly, this shift demands joint accountability across state and private actors, embedding ‘rule-of-law-by-design’ into digital migration tools to transform surveillance into a rights-centered practice. Such measures can transform digital migration governance from a space of invisibility and structural inequality into one aligned with justice, accountability, and respect for the dignity and agency of those who move, making digital borders an integral part of a democratic and rights-centred legal order. Yet even a human rights-centered approach

faces its own challenges, as the gap between rights, principles, design, deployment, and use can rarely be bridged by regulation alone. Integrating rights into these complex socio-technical environments demands a shift across disciplines and institutional contexts, making AI and its impacts a shared responsibility of technologists, researchers, policymakers, and civil society alike.

Judges, regulators, the private sector, civil society, researchers and migrant-led organizations must work together to hold state and corporate actors accountable, ensuring that digital tools do not deepen discrimination or embed systemic violence. The challenge goes beyond making migration management more efficient; it is about building a governance system that recognizes the full humanity and agency of those who move. The future of European Union migration policy must not be dictated exclusively by imperatives of control, security, or technological optimization. It must be shaped by a renewed commitment to accountability, social justice, and the recognition of migrants as rights-bearing individuals, not merely as profiles, data points, or biometric records.

Bibliography

IKosmos (2024). “Behind Fingerprint Biometrics: How it works and why it matters”. Published 15 April 2024. Available at:

<https://www.ikosmos.com/biometric-authentication/behind-fingerprint-biometrics-how-it-works-and-why-it-matters/>

Aizeki, Mizue; Bingham, Laura & Santiago Narváez (2023). “The Everywhere Border: Digital migration control infrastructure in the Americas”. Transnational Institute. Available at:

<https://search.issuelab.org/resource/the-everywhere-border-digital-migration-control-infrastructure-in-the-americas.html>

Amelung, Nina; Granja, Rafaela & Machado, Helena (2021). A Brief History of the Evolution of Biometrics and Biometric Database Systems Crossing Borders in EU Law Enforcement. In: *Modes of Bio-Bordering*. Palgrave Pivot, Singapore. Available at: https://doi.org/10.1007/978-981-15-8183-0_2

Amoore, Louise (2020). “Cloud Ethics: Algorithms and the Attributes of Ourselves and Others”. Duke University Press. Available at: <https://doi.org/10.2307/j.ctv11g97wm>

Amnesty International (2021). “Amnesty International position on the proposals for a Digital Services Act and a Digital Markets Act”. Available at: https://www.amnesty.eu/wp-content/uploads/2021/04/Amnesty-International-Position-Paper-Digital-Services-Act-Package_March2021_Updated.pdf

Amnesty International (2024). “Defending the rights of refugees and migrants in the digital age”. Available at: <https://www.amnesty.de/sites/default/files/2024-02/Amnesty-Briefing-Migration-Schutzsuchende-Ueberwachung-digitale-Technologien-Februar-2024.pdf>

Amnesty International (2024). “The Digital Border: Migration, Technology and Inequality”. Available at: <https://www.amnesty.de/sites/default/files/2024-02/Amnesty-Briefing-Migration-Schutzsuchende-Ueberwachung-digitale-Technologien-Februar-2024.pdf>

AP News (2025). “Europe's Anti-Torture Watchdog Slams Italy Over Migrant Detention Abuses”. Available at: <https://apnews.com/article/italy-council-of-europe-migration-centers-albania-detainees-violence-0dba82e1f333c60b3bc49a0894970e9d>

Aus, Jonathan P. (2003). “Supranational Governance in an Area of Freedom, Security and Justice: Eurodac and the Politics of Biometric Control”. ARENA, University of Oslo/Sussex European Institute. Available at: <https://www.sussex.ac.uk/webteam/gateway/file.php?name=sei-working-paper-no-72.pdf&site=266>

Beduschi, Ana & McAuliffe, Marie (2021). “Artificial Intelligence, migration and mobility: implications for policy and practice”. In: *World Migration Report 2022*. IOM, Geneva. Available at: <https://publications.iom.int/books/world-migration-report-2022-chapter-11>

Belaïd, J.L. (2022). “The role of non-state actors in digitised migration management: The impacts and limits of digitalisation on the EU’s externalised migration control in the Mediterranean”. IEMed. Available at: <https://www.iemed.org/publication/the-role-of-non-state-actors-in-digitised-migration-management-the-impacts-and-limits-of-digitalisation-on-the-eus-externalised-migration-control-in-the-mediterranean/?lang=es>

Bellanova, Rocco & Glouftsis, Georgios (2020). “Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance”. *Geopolitics*, 27(1), 160–184. Available at: <https://doi.org/10.1080/14650045.2020.1830765>

Bellio, Naiara; Lancho Bances, Carlos; Sánchez Monedero & Valdivia, Ana (2024). “Digital Technologies for Migration Control at the Spanish Southern Border”. EuroMed Rights - AlgoRace. Available at: https://euromedrights.org/wp-content/uploads/2024/10/240826_Euromed_TechBorders_EN.pdf

Bigo, Didier (2002). “Security and immigration: Toward a critique of the governmentality of unease”. *Alternatives: Global, Local, Political*, 27(1), 63–92. Available at: <https://doi.org/10.1177/03043754020270S105>

Brouwer, Evelien R. (2008). “Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System”. Martinus Nijhoff Publishers. Available at: <https://doi.org/10.1163/ej.9789004165038.i-568>

Broeders, Dennis (2007). “The New Digital Borders of Europe. EU Databases and the Surveillance of Irregular Migrants”. *International Sociology*, 22(1), 71–92. Available at: <https://doi.org/10.1177/0268580907070126>

Broeders, Dennis & Dijstelbloem, Huub (2016). “The Datafication of Mobility and Migration Management: The Mediating State and Its Consequences”. In: I. Van der Ploeg & J. Pridmore (Eds.), *Digitizing Identities: Doing Identity in a Networked World* (pp. 242–260). London: Routledge. Available at: <https://doi.org/10.4324/9781315756400-13>

Broeders, Dennis & Hampshire, James (2013). “Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe”. *Journal of Ethnic and Migration Studies*, 39(8), 1201–1218. Available at: <https://doi.org/10.1080/1369183X.2013.787512>

Browne, Simon (2015). “Dark Matters: On the Surveillance of Blackness”. Duke University Press.

Caplan, Jane & Torpey, John (Eds.) (2001). “Documenting Individual Identity: The Development of State Practices in the Modern World”. Princeton University Press.

Cinnéide, Colm O. (2021). “Why challenging discrimination at borders is challenging (and often futile)”. *AJIL Unbound*, 115, 362–367. Available at: <https://doi.org/10.1017/aju.2021.53>

Collins, Francis L. (2023). “Geographies of migration III: The digital migrant”. *Progress in Human Geography*, 47(5), 738–749. Available at: <https://doi.org/10.1177/03091325231157709>

Csernaton, Raluca (2018). “Constructing the EU’s high-tech borders: Frontex and dual-use drones for border management”. *European Security*, 27(2), 175–200. Available at: <https://doi.org/10.1080/09662839.2018.1481396>

Delioglu, Fatmanur (2025). “Technology at the borders: Surveillance, control and resistance in EU migration governance”. *Balsillie Papers*, 6(6). Available at:

<https://balsilliepapers.ca/bsia-paper/technology-at-the-borders-surveillance-control-and-resistance-in-eu-migration-governance/>

Dijstelbloem, Huub (2021). *Borders as Infrastructure: The Technopolitics of Border Control*. MIT Press.

District Court of The Hague (Rechtbank Den Haag) (2020). “Netherlands: Court Prohibits Government’s Use of AI Software to Detect Welfare Fraud”. *Library of Congress*. Available at: [Netherlands: Court Prohibits Government’s Use of AI Software to Detect Welfare Fraud | Library of Congress](#)

Donida Labati, Ruggero; Genovese, Angelo; Muñoz, Enrique; Piuri, Vincenzo; Scotti, Fabio and Sforza, Gianluca (2015). “Advanced design of automated border control gates: Biometric system techniques and research trends”. In: *Proc. of the 2015 IEEE Int. Symp. on Systems Engineering (ISSE)*, Rome, Italy.

Donida Labati, Ruggero, Genovese, Angelo, Muñoz, Enrique, Piuri, Vincenzo, Scotti, Fabio, and Sforza, Gianluca (2015). “Automated border control systems: Biometric challenges and research trends”. In *Proceedings of the IEEE International Symposium on Systems Engineering (ISSE)* (pp. 1–7). IEEE.

Dumbrava (2021). “Artificial Intelligence at EU Borders: Overview of Applications and Key Issues”. EPRS. Available at: <https://doi.org/10.2861/91831>

eu-LISA (2025). “EES. Enhancing Border Security in the Schengen Area”. European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. Available at: <https://www.eulisa.europa.eu/activities/large-scale-it-systems/ees>

eu-LISA (2025). “Eurodac. Supporting Asylum and Migration Policies across Europe”. European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. Available at: <https://www.eulisa.europa.eu/activities/large-scale-it-systems/eurodac>

eu-LISA (2025). “SIS. Europe's Largest Internal Security Database”. European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom,

Security and Justice. Available at:
<https://www.eulisa.europa.eu/activities/large-scale-it-systems/sis>

eu-LISA (2025). “VIS. Streamlining the Visa Application Process”. European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. Available at: <https://www.eulisa.europa.eu/activities/large-scale-it-systems/vis>

European Artificial Intelligence & Society Fund (2023). “AI in Border Control and Surveillance. Current and Future Implications”. *Euromed Rights*. Available at: <https://euromedrights.org/wp-content/uploads/2023/07/AI-in-border-control-and-surveillance.pdf>

European Asylum Support Office (2021). “Fact sheet on digitalisation” (EASO/IAS/2021/3). Available at: <https://shre.ink/xNsr>

European Commission (n.d.). “SIRENE cooperation”. Migration and Home Affairs. Available at: https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system/sirene-cooperation_en

European Commission (2010). “The Stockholm Programme — An open and secure Europe serving and protecting citizens” (2010/C 115/01). Available at: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF>

European Commission (2015). “A European Agenda on Migration”. Available at: https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/european-agenda-migration_en

European Commission (2017). “A European Agenda on Security: State of Play”. Available at: https://home-affairs.ec.europa.eu/system/files/2020-09/20170907_a_european_agenda_on_security_-_state_of_play_en.pdf

European Commission (2019). “Ethics guidelines for trustworthy AI”. Available at: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

European Commission (2021). “Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)”. COM (2021) 206 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

European Commission (2021). “A strategy towards a fully functioning and resilient Schengen area”. Available at: <https://www.europarl.europa.eu/legislative-train/carriage/future-schengen-strategy/report?sid=9201>

European Commission (2024). “Getting the EU's digital infrastructure ready for the future”. Available at: https://commission.europa.eu/news-and-media/news/getting-eus-digital-infrastructures-ready-tomorrows-world-2024-02-21_es

European Commission (2025). “European Travel Information and Authorisation System (ETIAS)”. Directorate-General for Migration and Home Affairs. Available at: https://home-affairs.ec.europa.eu/policies/schengen/smart-borders/european-travel-information-authorisation-system_en

European Commission (2025). “Entry/Exit System (EES)”. Directorate-General for Migration and Home Affairs. Available at: https://home-affairs.ec.europa.eu/policies/schengen/smart-borders/entry-exit-system_en

European Commission (2025). “What is SIS and how does it work?” Directorate-General for Migration and Home Affairs. Available at: https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system/what-sis-and-how-does-it-work_en

European Commission (2025). “What is the EES?” Directorate-General for Migration and Home Affairs”. Available at: https://travel-europe.europa.eu/ees/what-ees_en

European Court of Human Rights (ECtHR) (2011). “M.S.S. v. Belgium and Greece” Application No. 30696/09. Grand Chamber judgment. Available at: <https://hudoc.echr.coe.int/eng/?i=001-103050>

European Court of Human Rights (ECtHR) (2020). “N.D. and N.T. v. Spain”. Applications Nos. 8675/15 and 8697/15. Grand Chamber judgement. Available at: <https://hudoc.echr.coe.int/eng?i=001-201353>

European Data Protection Supervisor (EDPS) (2021). “Opinion 2/2021 on the European Commission’s Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)”. Available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-artificial-intelligence-act_en

European Digital Rights (EDRi) (2020). “Structural Racism, Digital Rights and Technology”. Recommendations to inform the European Commission Action Plan on Structural Racism. Available at: https://edri.org/wp-content/uploads/2020/09/Structural-Racism-Digital-Rights-and-Technology_Final.pdf

European Digital Rights (EDRi) (2021). “Uses of AI in Migration and Border Control: A Fundamental Rights Perspective”. Available at: https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf

European Migration Network (EMN) (2022). “The Use of Digitalisation and Artificial Intelligence in Migration Management”. Available at: https://home-affairs.ec.europa.eu/system/files/2022-02/00_EU_EMN_Digitalisation%20infor%20m%20February%202022_EN_0.pdf

European Network Against Racism (2017). “ENAR Shadow Report: Racism and Discrimination in the Context of Migration in Europe”. European Network Against Racism. Available at: <https://www.enar-eu.org/wp-content/uploads/shadow-report-migration-2015-16.pdf>

European Network of National Human Rights Institutions (ENNHRI) (2024). “Technologies, Migration and Human Rights: The Role of European NHRIs” – Scoping Paper. Available at: <https://ennhri.org/wp-content/uploads/2024/09/Technologies-migration-and-human-rights-the-role-of-European-NHRIs-an-ENNHRI-scoping-paper.pdf>

European Parliament (2019). Schengen: “A guide to the European border-free zone”. Available at: <https://www.europarl.europa.eu/topics/en/article/20190612STO54307/schengen-a-guide-to-the-european-border-free-zone>

European Parliament (2023). “European Parliament resolution on the annual report on the activities of the European Ombudsman in 2021” (2022/2141(INI)). Official Journal of the European Union, C/2023/397. Available at: [EUR-Lex - 52023IP0070 - EN - EUR-Lex](#)

European Union (2013). “SIS II Schengen Information System II. Helping you move freely, Helping you live safely”. Available at: https://www.minv.sk/swift_data/source/mv_sr_sport/schengen_pictures/HOME%20-%20SIS%20II%20-%20Leaflet%20V1.0.HR.EN.pdf

European Union Agency for Fundamental Rights (FRA) (2019). “Facial recognition technology: Fundamental rights considerations in the context of law enforcement”. Available at: <https://doi.org/10.2811/524628>

European Union Agency for Fundamental Rights (FRA) (2020). “Getting the future right – AI and fundamental rights”. European Union Agency for Fundamental Rights. Available at: <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights>

European Union Agency for Fundamental Rights (FRA) (2024). “Primer: Defending the Rights of Refugees and Migrants in the Digital Age”. Available at: <https://www.amnesty.de/sites/default/files/2024-02/Amnesty-Briefing-Migration-Schutzsuche-nde-Ueberwachung-digitale-Technologien-Februar-2024.pdf>

Everuss, Louis (2024). “Digital Mobilities and Smart Borders. How Digital Technologies Transform Migration and Sovereign Borders”. De Gruyter. Contemporary Social Sciences. Volume 5.

Facit (2024). “Milestones in Facial Recognition Technology: A Historical Overview”. Published 4 November 2024. Available at: <https://facit.ai/insights/evolution-of-facial-recognition-technology>

Fill, Alice (2025). “The datafication of mobility: Reading across legal and socio-technical infrastructures”. MOBILE Working Paper Series, no. 65, University of Copenhagen, Faculty of Law.

Forster, Madeleine (2022). “Refugee protection in the artificial intelligence era: A test case for rights”. Chatham House. Available at: <https://www.chathamhouse.org/2022/09/refugee-protection-artificial-intelligence-era>

Fundación iSocial (2025). “RefAid, una app para los refugiados que llegan a Europa”. Available at: <https://isocial.cat/es/refaid-una-app-para-los-refugiados-que-llegan-a-europa/>

Frontex (2012). “Best Practice Operational Guidelines for Automated Border Control (ABC) Systems”. Research and Development Unit. European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. Available at: https://www.frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_for_Automated_Border_Control.pdf

- Frontex (2025). “ETIAS/EES”. Available at: <https://www.frontex.europa.eu/what-we-do/etias-ees/about-etias/#:~:text=ETIAS%20will%20further%20strengthen%20Europe%27s,whether%20they%20pose%20a%20security%2C>
- Garriga Domínguez, A. (2024). “Rights in the Face of Biometric Systems Incorporating Artificial Intelligence”. *Derechos y Libertades*, 51(II), 117-149. Available at: <https://doi.org/10.20318/dyl.2024.8585>
- Garris, Michael D. & McCabe, Michael R. (2000). “Fingerprint Minutiae from Latent and Matching Tenprint Images”. NIST Special Database 27. National Institute of Standards and Technology. Gaithersburg, MD. Available at: <https://doi.org/10.6028/NIST.IR.6534>
- Gitelman, Lisa (2013). “Raw Data’ Is an Oxymoron”. MIT Press. Available at: <https://doi.org/10.7551/mitpress/9302.001.0001>
- Gonçalves & Gameiro (2012). “Security, Privacy and Freedom: The European Union Legal and Policy Framework for Biometrics”. Available at: https://www.researchgate.net/publication/294860286_Security_privacy_and_freedom_2012
- GOV.UK (2024). “Guidance. EU Entry/Exit System”. Foreign, Commonwealth & Development Office. Available at: [EU Entry/Exit System - GOV.UK](https://www.gov.uk/guidance/eu-entry-exit-system)
- Guenouni, Souhail; Mansouri, Anass and Ahaitouf, Ali (2019). “Biometric Systems and Their Applications”. IntechOpen. Available at: <https://www.intechopen.com/chapters/65920>
- Guild, Elspeth (2009). “Security and Migration in the 21st Century”. Polity Press.
- Human Rights Watch (2021). EU: “Artificial intelligence regulation threatens social safety net”. Available at: <https://www.hrw.org/news/2021/11/10/eu-artificial-intelligence-regulation-threatens-social-safety-net>
- Huysmans, Jef (2006). “The Politics of Insecurity: Fear, Migration and Asylum in the EU”. Routledge. Available at: <https://doi.org/10.4324/9780203008690>
- Innovatrics (2025). “Iris Recognition Technology”. Available at: <https://www.innovatrics.com/iris-recognition-technology>

International Commission of Jurists (2022). “Digital Technologies and Human Rights”. Available at: <https://www.icj.org/wp-content/uploads/2022/05/Digital-Technologies-and-Human-Rights-Briefing-Paper-FINAL-VERSION-May-2022.pdf>

International Network of Civil Liberties Organization (2024). “Eyes on the Watchers: Challenging the Rise of Police Facial Recognition”. Principles to reduce the human rights harms of facial recognition technology”. INCLO. Available at: <https://inclo.net/wp-content/uploads/2024/03/INCLO-FRT-Principles-Final.pdf>

IOM (2018). “Tech for Change: How Digital Tools Are Fostering Integration and Inclusion”. Medium. UN Migration. Available at: <https://medium.com/@UNmigration/tech-for-change-e2cd1483854b>

Jain, Anil K.; Ross, Arun & Prabhakar, Salil (2004). “An Introduction to Biometric Recognition”. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20. Available at: <https://doi.org/10.1109/TCSVT.2003.818349>

Kaya, Seyit A. (2023). “Real-Time Border Crossing with Iris Recognition”. *Border Security Report*. The Journal of border security and transnational crime. 15 December 2023. Available at: <https://www.border-security-report.com/real-time-border-crossing-with-iris-recognition/>

Koslowski, Rey & Schulzke, Marcus (2018). “Drones Along Borders: Border Security UAVs in the United States and the European Union”. *International Studies Perspectives*. <https://doi.org/10.1093/isp/eky002>

Lanneau, Romain (2023). “Digital rights and the protection of the right to asylum in the Charter of the European Union”. Statewatch. Available at: https://www.statewatch.org/analyses/2023/digital-rights-and-the-protection-of-the-right-to-asylum-in-the-charter-of-the-european-union/?utm_source=chatgpt.com

Latonero, Mark (2018). “Governing artificial intelligence: Upholding human rights & dignity”. *Data & Society*. Available at: https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf

Lebon, Léa (2024). “Cities and migrants’ rights in the era of digitalisation: Implications of the digital regulations in the new Pact on Migration and Asylum”. *Friedrich-Ebert-Stiftung*. Available at: <https://library.fes.de/pdf-files/a-p-b/21463.pdf>

Leslie, David (2020). “Understanding bias in facial recognition technologies: An explainer”. *The Alan Turing Institute*. Available at: <https://doi.org/10.5281/zenodo.4050457>

Leurs, Koen (2023). “Digital Migration”. Sage Publications.

Leurs, Koen & Ponzanesi, Sandra (2018). “Connected migrants: Encapsulation and cosmopolitanization”. *Popular Communication*, 16(1), 4–20. Available at: <https://doi.org/10.1080/15405702.2017.1418359>

Leurs, Koen & Smets, Kevin (2018). “Five Questions for Digital Migration Studies: Learning From Digital Connectivity and Forced Migration In(to) Europe”. *Social Media + Society*, 4(1), 1–16. Available at: <https://doi.org/10.1177/2056305118764425>

Loukinas, Panagiotis (2022). “Drones for Border Surveillance: Multipurpose Use, Uncertainty and Challenges at EU Borders”. *Geopolitics*, 27(1), 89–112. Available at: <https://doi.org/10.1080/14650045.2021.1929182>

Lyon, David (2003). “Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination”. Routledge.

Lyon, David (2007). “Surveillance Studies: An Overview”. Polity Press.

Magnet, Shoshana A. (2011). “When Biometrics Fail: Gender, Race, and the Technology of Identity”. Duke University Press.

Marin, Luisa (2016). “The deployment of drone technology in border surveillance. Between techno-securitization and challenges to privacy and data protection”. In: S. Carrera, J. Faure Atger, N. Hernanz, & A. Kostakopoulou (Eds.), *The Changing Dynamics of Security in an Enlarged European Union* (pp. 108–133). Routledge. Available at: <https://doi.org/10.4324/9781315619309-7>

Martins Oliveira, Bruno; Lidén, Kristoffer and Jumbert Gabrielsen, Maria (2022). “Border security and the digitalisation of sovereignty: insights from EU borderwork, European Security”, 31:3, 475-494, Available at: <https://doi.org/10.1080/09662839.2022.2101884>

McAuliffe, M., Blower, J. & Beduschi, A. (2021). “Digitalization and Artificial Intelligence in Migration and Mobility: Transnational Implications of the COVID-19 Pandemic”. *Societies*, 11, 135. <https://doi.org/10.3390/soc11040135>

McGregor, L. & Molnar, Petra (2023). “Digital Border Governance: A Human Rights Based Approach”. OHCHR & University of Essex. Available at: <https://www.ohchr.org/sites/default/files/2023-09/Digital-Border-Governance-A-Human-Rights-Based-Approach.pdf>

Molnar, Petra (2019). “Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective”. *Cambridge International Law Journal*, 8(2), 305–330. Available at: <https://doi.org/10.4337/cilj.2019.02.07>

Molnar, Petra (2020). “Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up”. EDRi & Refugee Law Lab. Available at: <https://km4s.ca/wp-content/uploads/Technological-Testing-Grounds-2020.pdf>

Nalbandian, Lucia & Dreher, Nick (2022). “Advanced Digital Technologies in Migration Management: A Review of Emerging Literature”. Toronto Metropolitan Centre for Immigration and Settlement (TMCIS) & CERC in Migration and Integration. *Working Paper No. 2022/11*.

Nikunen, Kaarina & Valtonen, Sanna (2024). “Undocumented and datafied: Anticipation, borders, and everyday life”. In K. Leurs & S. Ponzanesi (Eds.), *Doing Digital Migration Studies: Theories and Practices of the Everyday* (pp. 343–361). Amsterdam University Press.

Okta (2024). “Fingerprint biometrics: Definition & how secure it is”. Available at: <https://www.okta.com/identity-101/fingerprint-biometrics-definition-how-secure-it-is/>

Oloid Desk (2024). “Beyond Fingerprints: The Power of Multimodal Biometric Authentication”. Available at: <https://www.oloid.com/blog/beyond-fingerprints-the-power-of-multimodal-biometric-authentication>

Pelizza, Annalisa (2021). “Processing Alterity, Enacting Europe: Migrant Registration and Identification in EU Border Technologies”. *Science, Technology, & Human Values*, 46(2), 208–229. Available at: <https://doi.org/10.1177/0162243919827927>

Ponzanesi, Sandra (2016). “Connecting Europe: Postcolonial mediations”. Utrecht, The Netherlands: Utrecht University.

Ponzanesi, Sandra & Leurs, Koen (2022). “Digital Migration Practices and the Everyday”. *Communication, Culture and Critique*, 15(2), 103–121. Available at: <https://doi.org/10.1093/ccc/tcac016>

Platform for International Cooperation on Undocumented Migrants (PICUM, 2022). “Digital Technologies and the Rights of Undocumented Migrants”. Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Platform_for_International_Cooperation_on_Undocumented_Migrants.pdf

Qinjun, Li; Tianwei, Cui; Yan, Zhao & Yuying, Wu (2023). “Facial Recognition Technology: A Comprehensive Overview”. School of Electronic Information and Artificial Intelligence, Shaanxi University of Science & Technology, Xi'an, China. *Academic Journal of Computing & Information Science*, 6(7), 15–26. Available at: <https://francis-press.com/uploads/papers/qd2810eEIhPDLdXhBQjSWXVTJW4SrZ7iCUtQqZfs.pdf>

Redpath, Jillyanne (2007). “Biometrics and International Migration”. *Ann Ist Super Sanità*, 43(1), 27–35. Available at: https://www.iss.it/documents/20126/45616/STAMPA+ANN_07_05+Redpath.1180428351.pdf/e54f0d03-7008-46f9-5855-a73e54fb9d75?t=1581103273012

Rinaldi, Alberto & Teo, Sue A. (2025). “The Use of Artificial Intelligence Technologies in Border and Migration Control and the Subtle Erosion of Human Rights”. *International and Comparative Law Quarterly*. Available at: <https://doi.org/10.1017/S0020589325000090>

Sandberg, Marie; Rossi, Luca; Galis, Vasilis & Bak Jørgensen, Martin (Eds.) (2022). “Research Methodologies and Ethical Challenges in Digital Migration Studies: Caring For (Big) Data?” Palgrave Macmillan. Available at: <https://doi.org/10.1007/978-3-030-81226-3>

Sánchez del Río, José; Moctezuma, Daniela; Conde, Cristina; de Diego, Martín D. & Cabello, Enrique (2016). “Automated Border Control E-Gates and Facial Recognition Systems”. *Computers & Security*, 62, 49–72. Available at: <https://doi.org/10.1016/j.cose.2016.07.001>

Santamaria, Kelsey Y. (2021). Facial recognition technology and law enforcement: Select constitutional considerations. In W. Lambert (Ed.), *Issues with facial recognition technology*, 1–46. Nova Science Publishers.

Scheel, Stephan; Ruppert, Evelyn & Ustek-Spilda, Funda (2019). “Enacting Migration Through Data Practices”. *Environment and Planning D: Society and Space*, 37(4), 579–588. Available at: <https://doi.org/10.1177/0263775819865791>

Shields, Peter (2010). “ICTs and the European Union's Evolving Border Surveillance Architecture: A Critical Assessment”. *Observatorio (OBS) Journal*, 4(1), 255–288. Available at: <https://doi.org/10.15847/obsOBS412010331>

Stenum, Helle (2017). “The Body-border: Governing Through Biometric Technology”. *Journal for Digital Cultures. Spheres*, 4. Media and Migration. Available at: https://www.academia.edu/89024652/The_Body_Border_Governing_Irregular_Migration_through_Biometric_Technology

Sunderland, Judith & Pezzani, Lorenzo (2022). “EU’s Drone Another Threat to Migrants and Refugees”. Human Rights Watch & Border Forensics. Available at: <https://www.hrw.org/news/2022/08/01/eus-drone-another-threat-migrants-and-refugees>

Tashji, David (2024). “Smart Borders: How Technology is Tracking You”. Posted on December 9, 2024. Available at: [Smart Borders: How Technology is Tracking You |](#)

Taylor, Linnet & Broeders, Dennis (2015). “In the Name of Development: Power, Profit and the Datafication of the Global South”. *Geoforum*, 64, 229–237. Available at: <https://doi.org/10.1016/j.geoforum.2015.07.002>

Tazzioli, Martina (2018). “The Temporal Borders of Asylum: Temporality of Control in the EU Border Regime”. *Political Geography*, 64, 13–22. Available at: <https://doi.org/10.1016/j.polgeo.2018.02.002>

Tazzioli, Martina (2020). “The Making of Migration: Biopolitics of Mobility at Europe’s Borders”. *Society and Space*. SAGE Publications, Inc. Available at: <https://doi.org/10.4135/9781526492920>

The Alan Turing Institute (2021). “Artificial Intelligence, Human Rights, Democracy, and the Rule of Law”. Available at: https://www.turing.ac.uk/sites/default/files/2021-03/cahai_feasibility_study_primer_final.pdf

Topak, Özgün E. (2019). “Humanitarian and Human Rights Surveillance: The Challenge to Border Surveillance and Invisibility?” *Surveillance & Society*, 17(3–4), 382–404. Available at: <https://doi.org/10.24908/ss.v17i3/4.10779>

Topol, Tom (2024). “Border Control Evolution: From Historical Narratives to Cutting-Edge Initiatives”. Available at: <https://www.linkedin.com/pulse/border-control-evolution-from-historical-narratives-tom-topol-rgric/?trackingId=Rsx5R5hLTgWiIP%2Bqv4Cx5Q%3D%3D>

Torpey, John (2018). “The Invention of the Passport: Surveillance, Citizenship, and the State”. Second Edition. Cambridge University Press. <https://doi.org/10.1017/9781108664271>

Trauttmansdorff, Paul (2022). “Borders, Migration, and Technology in the Age of Security: Intervening with STS”. *Tecnoscienza - Italian Journal of Science & Technology Studies*, 13(2), 133–154. Available at: <https://doi.org/10.6092/issn.2038-3460/17584>

Tschalaer, M., Xanthaki, A. & Xanthopoulou, E. (2023). “Migration Flows Prediction Tools and Asylum Policy Commitments in Alignment with Human Rights” (Policy Brief No. 5, Deliverable D8.1). ITFLOWS Project, Brunel University London. Available at: <https://www.itflows.eu/wp-content/uploads/2022/06/ITFLOWS-Policy-Brief-5-D8.1.pdf>

Umoren, Imeh; Inyang, Saviour & Silas, Abasiama (2021). “Intelligent Surveillance and Facial Recognition System for Efficient Border Monitoring and Threats Prediction Using Machine Learning Approaches”. *Researchers Journal of Science and Technology (REJOST)*, 1(1), 47–63. Available at: <https://rejost.com.ng/index.php/home/article/view/6/3>

United Nations General Assembly (2020). “Report of the Special Rapporteur on Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment” (A/HRC/43/49). Available at: <https://undocs.org/A/HRC/43/49>

United Nations High Commissioner for Refugees (UNHCR) (2021). “Global Report 2021”. Available at: https://www.unhcr.org/wp-content/uploads/sites/27/2022/06/UNHCR_global-report-2021.pdf

United Nations Human Rights Office (OHCHR) (2021). “The right to privacy in the digital age” (A/HRC/48/31). United Nations Human Rights Council. Available at: <https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high>

Val Garijo, Fernando (2020). “Drones, Border Surveillance and the Protection of Human Rights in the European Union”. National Distance Education University, Madrid, Spain. Available at: <http://dx.doi.org/10.13165/PSPO-20-25-09>

Viola, Lorella; Venkel, Machteld & Verheul, Jaap (2023). “Migration Studies and the Digital: Datafication, Implications, and Methodological Approaches”. *Frontiers in Human Dynamics*, 5, Article 1337817. Available at: <https://doi.org/10.3389/fhumd.2023.1337817>

Wachter, Sandra; Mittelstadt, Brent & Russell, Chris (2020). “Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-discrimination Law and AI”. *Computer Law & Security Review*, 41. Available at: <https://ssrn.com/abstract=3547922>

Wevers, Rosa & Zhuparris, Ahnijili (2024). “Undocumented and datafied: Anticipation, borders, and everyday life”. In K. Leurs & S. Ponzanesi (Eds.), *Doing Digital Migration Studies: Theories and Practices of the Everyday* (pp. 343–361). Amsterdam University Press.

Witteborn, Saskia (2022). “Digitalization, Digitization and Datafication: The ‘Three D’ Transformation of Forced Migration Management”. *Communication, Culture and Critique*, 15(2), 157–172. Available at: <https://doi.org/10.1093/ccc/tcac007>