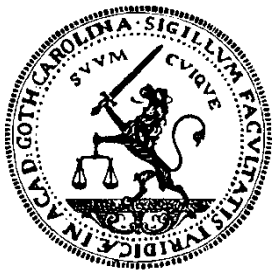


FACULTY OF LAW

LUND UNIVERSITY

Maria-Ecaterina Nistor

Algorithmic Decision-Making in EU Asylum Procedures

JAMM07 Master Thesis

International Human Rights Law

30 higher education credits

Supervisor: Zvezda Vankova

Term of graduation: Spring 2026

Table of Contents

Summary

The increasing digitalization of migration governance has transformed how asylum and migration procedures operate within the European Union. Large-scale databases, biometric identification systems, interoperability frameworks, and algorithmic decision-support tools now play an important role in migration administration. Systems such as Eurodac, SIS, VIS, EES, and ETIAS enable authorities to collect, compare, and circulate large quantities of personal and biometric data across interconnected European infrastructures.

This research examines how these technological developments interact with existing European legal frameworks governing migration and asylum decision-making. The analysis focuses on whether current safeguards under EU migration law, human rights law, and data protection law remain capable of ensuring accountability, procedural fairness, and effective protection once decision-making becomes increasingly mediated through algorithmic systems and interoperable databases. Particular attention is given to the Common European Asylum System, the Charter of Fundamental Rights of the European Union, the GDPR, and the AI Act.

The analysis combines doctrinal legal research with technical explanation in order to examine how algorithmic systems shape evidentiary assessment and administrative reasoning within migration procedures. Biometric and computational systems operate through probabilistic calculations based on datasets, similarity thresholds, and statistical correlations rather than certainty. Yet these outputs may acquire significant evidentiary authority within asylum procedures, despite remaining partially inaccessible to affected individuals and difficult to challenge through ordinary legal mechanisms.

Particular attention is also given to interoperability infrastructures and the growing role of private technology contractors involved in EU migration governance. Accountability becomes increasingly difficult where decision-relevant outputs are shaped through technical systems that remain partially external to visible legal reasoning and judicial scrutiny.

The research concludes that existing legal safeguards provide important protections but remain only partially capable of addressing the structural challenges created by algorithmically mediated migration governance. As migration administration becomes increasingly dependent on biometric systems, interoperable infrastructures, and data-driven forms of assessment, preserving meaningful accountability will require stronger forms of transparency, human oversight, and institutional scrutiny.

Sammanfattning

Den ökande digitaliseringen av migrationsstyrning har förändrat hur asyl- och migrationsförfaranden fungerar inom Europeiska unionen. Storskaliga databaser, biometriska identifieringssystem, interoperabilitetsramverk och algoritmiska beslutsstödsverktyg spelar idag en viktig roll i migrationsadministrationen. System såsom Eurodac, SIS, VIS, EES och ETIAS gör det möjligt för myndigheter att samla in, jämföra och sprida stora mängder personuppgifter och biometrisk data inom sammanlänkade europeiska infrastrukturer.

Denna studie undersöker hur dessa teknologiska utvecklingar samspelar med de europeiska rättsliga ramverk som reglerar migrations- och asylbeslut. Analysen fokuserar på huruvida nuvarande skyddsmekanismer inom EU:s migrationsrätt, mänskliga rättigheter och dataskyddsrätt är tillräckliga för att säkerställa ansvarsskyldighet, rättssäkerhet och effektivt skydd när beslutsfattande i allt större utsträckning påverkas av algoritmiska system och interoperabla databaser. Särskild uppmärksamhet ägnas åt det gemensamma europeiska asylsystemet, Europeiska unionens stadga om de grundläggande rättigheterna, GDPR och AI-förordningen.

Analysen kombinerar rättsdogmatisk metod med tekniska förklaringar för att undersöka hur algoritmiska system påverkar bevisvärdering och administrativt beslutsfattande inom migrationsförfaranden. Biometriska och beräkningsbaserade system fungerar genom probabilistiska beräkningar baserade på dataset, likhetströsklar och statistiska samband snarare än säker identifiering. Trots detta kan sådana resultat få betydande bevisvärde inom asylförfaranden, även om de ofta förblir delvis otillgängliga för de berörda individerna och svåra att ifrågasätta genom vanliga rättsliga mekanismer.

Särskild uppmärksamhet riktas även mot interoperabilitetsinfrastrukturer och den växande rollen för privata teknikföretag inom EU:s migrationsstyrning. Ansvarsskyldighet blir allt svårare att säkerställa när beslutsrelevanta resultat formas genom tekniska system som delvis ligger utanför synligt juridiskt resonemang och rättslig granskning.

Studien drar slutsatsen att befintliga rättsliga skyddsmekanismer erbjuder viktiga garantier men endast delvis kan hantera de strukturella utmaningar som skapas av algoritmiskt medierad migrationsstyrning. I takt med att migrationsadministrationen blir allt mer beroende av biometriska system, interoperabla infrastrukturer och datadrivna bedömningar krävs starkare former av transparens, mänsklig kontroll och institutionell granskning för att säkerställa meningsfull ansvarsskyldighet och skydd för grundläggande rättigheter.

Preface

This thesis marks the conclusion of an incredibly intense, challenging, and deeply transformative journey at Lund University. Writing this work while simultaneously running my own NGO in Sweden, managing a second Master's degree, and maintaining a job has tested the absolute limits of my resilience and willpower. It was a path often walked without a roadmap, but one that has shaped me irrevocably as both a researcher and an individual.

First and foremost, I dedicate this thesis to everyone who has ever had to pack up their life and leave their home behind in the pursuit of safety, a better future, or a higher education. Navigating a foreign system is a long and frequently terrifying journey, especially in a contemporary landscape where media narratives and shifting policies so often alienate and dehumanize us. If nobody has told you this today, let these words find you: *I am incredibly proud of you.* To all the migrants and students reading this who have had to figure things out in the dark because there was no one to guide them: we did it. Congratulations. Please know that if you are ever seeking support or are interested in my research, my door and my inbox will always remain wide open to you.

I owe a profound debt of gratitude to the academic community at the Department of Law at Lund University for believing in my potential, even during the moments I deeply doubted myself.

I am especially grateful to my supervisor, Zvezda Vankova. Thank you for constantly pushing me to make my own decisions and navigate this complex research independently. You taught me a vital life lesson in self-management that I will undoubtedly carry forward into my future PhD journey. I deeply appreciated being treated as a peer and a capable professional throughout this process, especially when managing my responsibilities outside of class.

I would also like to express my sincere thanks to my professors, Valentin, Matthew, Anna, Christine, Christoffer, and Alberto, for their unwavering belief in my capabilities and for helping me develop my legal skills. A special note of gratitude goes to Matthew and Christoffer, whose mentorship and encouragement pushed me beyond the traditional boundaries of a Master's student, giving me the confidence to finally present my research at an international conference and pursue open-access publication.

To my brilliant team and colleagues at The Research Bridge: thank you for believing in my vision, joining my NGO, and helping me build something truly fantastic from scratch in a foreign country. Your dedication has been a constant source of inspiration.

Finally, I wish to express my deepest appreciation to my aunt, Simona. You have been my ultimate inspiration ever since I was a child. At first, it was simply because I loved the stories about your travels across the globe and the airplane food you will always bring to me. Today, it is because I truly understand the immense courage it took for you to move 400 miles away from home, not speaking the language, armed with nothing but your brilliant brain and absolute willpower, and still make it out on top. I know I still have a long path ahead, but with this, I feel one step closer.

Thank you.

Abbreviations

AI	Artificial Intelligence
AFIS	Automated Fingerprint Identification Systems
CEAS	Common European Asylum System
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
EES	Entry/Exit System
ETIAS	European Travel Information and Authorisation System
Eurodac	European Asylum Dactyloscopy Database
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems
GDPR	General Data Protection Regulation
sBMS	Shared Biometric Matching System
SIS	Schengen Information System
TFEU	Treaty on the Functioning of the European Union
VIS	Visa Information System

1 Introduction

1.1 Background: Digitalization of Migration Governance in Europe

A person arriving at an external border of the European Union to request asylum may encounter multiple digital systems before speaking in detail to an asylum officer. Upon registration of the asylum application, their fingerprints are collected and entered into the European Asylum Dactyloscopy Database (Eurodac), an EU-wide biometric database established to assist in determining which Member State is responsible for examining an asylum application under the Dublin III Regulation.[1] If the system identifies a prior fingerprint registration in another Member State, this "match" may be used to transfer responsibility for examining the application to that state under the Dublin system, which allocates responsibility for asylum claims between Member States, generally prioritizing the state of first entry[2].

At the same time, authorities may consult the Schengen Information System (SIS), a large-scale database containing alerts relating to border control, return decisions, entry bans, missing persons, and security concerns, as well as the Visa Information System (VIS), which stores biometric and biographical data connected to visa applications. These systems are used to verify identity, determine whether the applicant previously entered or stayed in another Member State, identify prior visa applications or immigration decisions, detect security or return-related alerts, and support the broader allocation of responsibility and border management functions within the Common European Asylum System.[3]

These systems, managed by the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA)[4], do not merely store information. They also shape how identity, movement history, and responsibility for examining asylum claims are interpreted within migration procedures. For example, Eurodac uses biometric technology to compare fingerprints collected across Member States in order to identify previous registrations or border crossings.[5] The system produces a "match" when the similarity between fingerprint records reaches a certain threshold established by the system. As a result, biometric identification does

[1] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 [2013] OJ L180/1.

[2] Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast) [2013] OJ L180/31. From 1 July 2026, the Dublin III Regulation will be replaced by the Asylum and Migration Management Regulation (EU) 2024/1351.

[3] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) [2018] OJ L312/56; Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) [2008] OJ L218/60.

[4] Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) [2018] OJ L295/99.

[5] Eurodac Regulation (n 1).

not operate with absolute certainty, but through probabilistic assessments based on patterns and likelihoods.[6]

In practice, however, these results may be treated as definitive factual findings within legal and administrative procedures, particularly in the application of the Dublin III Regulation. Similar forms of biometric identification and data-linking are increasingly used across systems such as SIS and VIS, especially through new interoperability initiatives and shared digital infrastructures developed with private technology contractors such as IDEMIA and Sopra Steria.[7]

Under EU law, asylum decisions must comply with requirements of individualized assessment, procedural fairness, reason-giving, and effective judicial protection. These safeguards derive in particular from Directive 2013/32/EU (Asylum Procedures Directive)[8], Article 41 of the Charter of Fundamental Rights of the European Union, which guarantees the right to good administration, and Article 47 of the Charter, which guarantees the right to an effective remedy and a fair hearing.[9] The issue is therefore not the absence of legal safeguards, but the interaction between these safeguards and technical systems whose outputs depend on data quality, threshold calibration, and computational design choices that remain partially external to legal scrutiny.

This thesis examines how the integration of system-generated outputs into migration governance affects the structure of legal accountability, focusing on the gap between technical decision processes and the requirements of EU law and fundamental rights.

1.2 Research Problem: Algorithmic Decision-Making and Legal Accountability

The increasing use of algorithmic systems in migration governance exposes a structural gap between existing legal frameworks and how decisions are actually produced in practice. EU migration law, data protection law, and European human rights law set clear safeguards against arbitrary decision-making, discrimination, and fully automated decisions. These rules are built on the idea that decisions rely on identifiable reasoning and evidence that can be explained and reviewed.

This becomes difficult where key elements of a decision are generated through computational processes. Systems such as biometric matching or database correlation[10] produce outputs based

[6] Charles L Wilson, Craig I Watson, Michael D Garris and Austin Hicklin, *Studies of Fingerprint Matching Using the NIST Verification Test Bed (VTB)* (NISTIR 7020, National Institute of Standards and Technology 2004)

[7] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa [2019] OJ L135/27. See also Appendix I.I for further discussion of private contractors and interoperability infrastructures, including IDEMIA and Sopra Steria.

[8] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection [2013] OJ L180/60.

[9] Charter of Fundamental Rights of the European Union [2012] OJ C326/391 arts 41, 47.

[10] Database correlation refers to the automated comparison and linking of information across multiple databases in order to identify connections, matches, or inconsistencies between records.

on similarity scores[11], predefined variables[12], and threshold settings[13]. These outputs can influence the outcome of a case, yet the parameters behind them are not part of the legal reasoning and are not visible to the person affected. In practice, this makes it difficult to understand how a conclusion was reached or to challenge it. The issue is particularly clear in so-called human-in-the-loop systems[14], where a formal decision is still taken by an administrative authority but relies heavily on system-generated results. In these situations, responsibility is spread across different actors, including public authorities, system operators, and private contractors involved in system design. This makes it harder to identify who is accountable and weakens the ability to effectively contest a decision.

The problem is therefore not only whether algorithmic systems produce errors or bias, but how they alter the conditions under which legal accountability operates. When decisions are shaped by technical processes that are not reflected within legal reasoning itself, safeguards such as transparency, reason-giving, and effective remedy become increasingly difficult to apply in practice. Existing scholarship on algorithmic governance in migration has extensively examined issues such as surveillance, discrimination, automated border control, and the implications of emerging legal frameworks including the AI Act and the EU Pact on Migration and Asylum. However, much of this literature remains either primarily doctrinal or focused on broader social and psychological impacts, often without engaging directly with the technical infrastructures through which these systems operate.[15]

At the same time, technical literature frequently explains biometric systems, interoperability mechanisms, and machine learning models in abstract or experimental terms, but rarely examines how these systems interact with legal safeguards, administrative procedures, and the institutional realities of migration governance.[16] In particular, limited attention has been given to the role of private technology companies involved in developing and maintaining large-scale EU migration infrastructures, despite the fact that corporations such as IDEMIA, Sopra Steria, Atos, IBM, and Leonardo increasingly shape the technical architecture through which migration control is operationalized.[17] The rapid development of this sector has created a growing disconnect between legal scholarship, technical scholarship, and the practical realities of migration administration.

[11] Similarity scores are numerical values generated by biometric systems indicating the likelihood that two biometric samples, such as fingerprints, belong to the same person. See Anil K Jain, Arun Ross and Karthik Nandakumar, *Introduction to Biometrics* (Springer 2011).

[12] Predefined variables are specific categories or forms of data selected by a computational system for analysis and comparison, such as nationality, travel history, or biometric identifiers.

[13] Threshold settings refer to predefined confidence levels used by a system to determine when a biometric comparison is treated as a "match". Lower thresholds may increase false positives, while higher thresholds may increase false negatives. See Charles L Wilson and others, *Studies of Fingerprint Matching Using the NIST Verification Test Bed (VTB)* (NISTIR 7020, National Institute of Standards and Technology 2004).

[14] Human-in-the-loop systems describe decision-making models in which automated systems assist or structure decisions while a human authority formally retains final decision-making power.

[15] *Data Protection, Immigration Enforcement and Fundamental Rights* (PICUM 2019); Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 *Duke Law and Technology Review* 18.

[16] Anil K Jain, Arun Ross and Karthik Nandakumar, *Introduction to Biometrics* (Springer 2011); NIST Special Database 24 (n 6).

[17] Regulation (EU) 2019/817 (n 7); see also Appendix I.I on private contractors and interoperability infrastructures.

As a result, the relationship between technical system design, private technological contractors, migration administration, and legal accountability remains insufficiently explored in an integrated manner. This thesis addresses that gap by combining doctrinal legal analysis with a technical examination of biometric matching systems, interoperability infrastructures, and the private actors involved in developing large-scale EU migration technologies. In doing so, it argues that accountability in contemporary migration governance can no longer be understood solely through legal analysis or technical analysis in isolation. Rather, meaningful analysis increasingly requires engagement across legal, technical, and administrative fields in order to understand how outsourced digital infrastructures shape migration decision-making in practice.

1.3 Research Aim and Questions

The primary aim of this thesis is to assess whether existing European legal frameworks provide adequate safeguards against rights violations arising from algorithmic decision-making in migration governance, and to identify the points at which legal accountability becomes structurally weakened by automation.

To achieve this aim, the thesis is guided by the following research questions:

- How do European human rights law, EU data protection law, and EU migration law regulate the use of algorithmic and data-driven systems in migration and asylum governance?
- How do biometric systems, interoperability infrastructures, and data-driven decision-support tools influence evidentiary assessment and administrative decision-making within EU migration procedures?
- What legal and procedural challenges arise when migration decisions rely on probabilistic classifications, automated matching systems, and computational forms of assessment rather than fully individualized legal reasoning?
- To what extent are existing legal safeguards, including procedural guarantees, transparency obligations, human oversight requirements, and judicial review mechanisms, capable of ensuring accountability in algorithmically mediated migration governance?

These questions are designed to connect doctrinal legal analysis with the technical operation of algorithmic systems, focusing on how legal safeguards function in practice when migration governance increasingly relies on digital infrastructures, biometric technologies, and computational forms of evaluation.

1.4 Methodology: Doctrinal Legal Analysis and Technical Illustration

This thesis adopts a combined methodology based on doctrinal legal analysis and sociotechnical systems modeling. The technical component adopts an explanatory modeling approach commonly used in computer science and biometric systems analysis to illustrate how computational systems generate decision-relevant outputs.[18]

[18] See eg Christopher M Bishop, *Pattern Recognition and Machine Learning* (Springer 2006); Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* (MIT Press 2016).

The doctrinal component examines the legal framework governing decision-making in EU migration contexts. This includes Directive 2013/32/EU (Asylum Procedures Directive),[19] which regulates procedural safeguards in asylum procedures; Directive 2011/95/EU (Qualification Directive),[20] which establishes the criteria for refugee status and subsidiary protection; Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR),[21] particularly Article 22 concerning automated decision-making; and the Charter of Fundamental Rights of the European Union.[22] Particular attention is given to Article 7 of the Charter, protecting private and family life; Article 8, guaranteeing the protection of personal data; Article 21, prohibiting discrimination; Article 41, establishing the right to good administration; and Article 47, guaranteeing the right to an effective remedy and fair trial.

The analysis focuses on how core legal requirements contained in these instruments — such as individualized assessment, non-discrimination, data protection, and the ability to challenge decisions — apply where decision-making is influenced by computational systems. It also considers relevant interpretative guidance issued by the Article 29 Data Protection Working Party, the predecessor body to the European Data Protection Board (EDPB), particularly the *Guidelines on Automated Individual Decision-Making and Profiling under Regulation 2016/679*, which clarify the interpretation of Article 22 GDPR and the requirements for meaningful human oversight in automated decision-making systems.[23] The thesis focuses primarily on the legal and technical framework operating prior to the implementation of the EU Pact on Migration and Asylum, while acknowledging that several of the instruments examined, including the Dublin III Regulation, will undergo substantial modification following the entry into force of the new Pact architecture.[24]

The technical component is used to clarify how these systems operate at a functional level. It draws on established technical literature, including biometric evaluation studies conducted by the National Institute of Standards and Technology (NIST), as well as standard literature on biometric identification and pattern recognition systems.[25] Simplified models are used to illustrate processes such as fingerprint comparison, where biometric images are converted into mathematical feature templates[26] and compared through similarity scoring[27] and threshold-

[19] Asylum Procedures Directive (n 8).

[20] Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection [2011] OJ L337/9.

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.

[22] Charter (n9).

[23] Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* (WP251rev.01, 2018).

[24] Dublin III Regulation (n 2).

[25] NIST Special Database 24 (n 6); Jain, Ross and Nandakumar (n 16).

[26] Feature templates refer to simplified mathematical representations of biometric information, where distinctive fingerprint patterns are converted into numerical data that can be compared automatically by computer systems. For example, instead of storing a fingerprint only as an image, the system identifies specific points where fingerprint lines end or split and converts their position and direction into numerical coordinates. A simplified template may therefore look as follows: Point A (x=24, y=41, angle=62°), Point B (x=31, y=52, angle=15°). The system then compares these numerical patterns with other stored templates in order to estimate how likely it is that two fingerprints belong to the same person.

[27] Similarity scoring refers to the process through which the system calculates how closely two fingerprints resemble each other. For example, a higher score means the system considers it more likely that both fingerprints belong to the same person.

based matching processes[28]. Additional examples demonstrate how classification systems rely on predefined variables and how threshold calibration[29] influences the final classification produced by the system. These illustrations focus on specific mechanisms, including feature selection, similarity metrics, and decision thresholds, that directly affect how outputs are generated. The purpose is to demonstrate how technical parameters shape decision-relevant results that may later be treated as factual elements within legal procedures. This approach allows the legal analysis to engage directly with the technical processes influencing decision-making, rather than relying solely on abstract descriptions of algorithmic systems.

1.5 Scope and Limitations

This thesis examines the use of algorithmic and data-driven systems within European migration governance, with a particular focus on how such systems influence administrative decision-making. While asylum procedures provide a central analytical context, the scope extends beyond asylum law and encompasses the broader digital infrastructures through which migration governance is increasingly organized within the European Union. This reflects the growing integration between asylum, border control, identity management, and return procedures, particularly following the reforms consolidated under the New Pact on Migration and Asylum, which further institutionalize interoperability, data-sharing, and coordinated digital governance across migration management systems.[30] The analysis is confined to systems that support or shape decisions, rather than fully autonomous decision-making, as human authorities remain formally responsible within the current EU framework.

The thesis does not examine in detail systems such as the Entry/Exit System (EES), the European Travel Information and Authorization System (ETIAS), or interoperability infrastructures such as the shared Biometric Matching System (sBMS)[31]. Although these systems form part of the broader digitalization of EU migration governance, they primarily concern border management and infrastructural coordination rather than the direct production of evidentiary outputs within asylum procedures. Nevertheless, they remain relevant as part of the broader shift toward interoperable and data-driven migration governance within the European Union[32].

Geographically, the research is limited to the European legal context, including EU law and relevant human rights standards. It does not undertake a comparative analysis of non-European jurisdictions, nor does it examine differences in implementation across Member States. The focus is instead on the normative legal framework and its capacity to regulate decision-making processes influenced by computational systems.

The thesis is based on doctrinal legal analysis and desk-based research. It does not include empirical fieldwork, interviews, or access to operational systems or administrative datasets.

[28] Threshold-based matching refers to the minimum score required before the system treats the comparison as a "match."

[29] Threshold calibration refers to the adjustment of the system's internal limits for classification. For example, changing the threshold may determine whether a person is flagged for additional review or treated as presenting a lower level of risk.

[30] European Commission, *Communication on a New Pact on Migration and Asylum* COM (2020) 609 final.

[31] Regulation (EU) 2019/817 (n 7); Regulation (EU) 2019/817 (n 7); Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the field of police cooperation, judicial cooperation, asylum and migration [2019] OJ L135/85.

[32] Valsamis Mitsilegas, 'The Transformation of European Border Controls: The New Architecture of EU Migration Management' (2022) 44 Journal of Ethnic and Migration Studies 1.

The technical component is illustrative rather than empirical, relying on simplified models to demonstrate how algorithmic processes, such as biometric matching, classification, and threshold-based decision rules, function. These examples are used to clarify how technical mechanisms shape decision-relevant outputs, without claiming to represent specific real-world systems.

Given the rapid pace at which artificial intelligence, biometric governance, and digital migration management continue to evolve, both technologically and legally, the analysis presented here reflects the state of the field primarily until 1 May 2026. Consequently, legislative reforms, procurement developments, technical modifications, or operational practices emerging after this date may not be fully reflected within the analysis. This limitation is particularly relevant given the ongoing implementation of the EU Pact on Migration and Asylum and the continued expansion of interoperability frameworks managed through eu-LISA and private technological contractors.

Nevertheless, despite the evolving nature of the field, this research retains analytical and documentary value. Many of the structural issues examined are unlikely to disappear with future technological developments. In addition, the research provides an interdisciplinary examination of legal frameworks, technical mechanisms, and institutional infrastructures at a significant transitional moment in European migration governance. Finally, the annexes included in this research contain detailed technical explanations, simplified system models, and documentation concerning interoperability architectures and private contractors involved in EU migration systems, which may remain relevant for understanding the institutional and historical development of algorithmic migration governance, even as specific technologies continue to evolve.

1.6 Structure of the Thesis

The thesis is structured into five substantive chapters, followed by a conclusion and two appendices.

Chapter 2 establishes the legal framework governing decision-making in EU migration and asylum law. It examines the structure of the Common European Asylum System, procedural guarantees applicable to asylum procedures, fundamental rights protections under the Charter of Fundamental Rights of the European Union, and the role of EU data protection law in regulating automated and algorithmic decision-making.

Chapter 3 examines the digital infrastructures and algorithmic systems used within EU migration governance. It analyzes large-scale databases such as Eurodac, SIS, and VIS, as well as biometric matching systems, interoperability frameworks, and data-driven decision-support mechanisms. Particular attention is given to how these systems generate, structure, and operationalize decision-relevant information within migration procedures.

Chapter 4 explores the structural tensions between algorithmic systems and legal standards. It examines how probabilistic classification, automated matching, and computational forms of assessment interact with legal principles such as individualized assessment, transparency, explainability, procedural fairness, and effective judicial protection. The chapter further analyzes how algorithmic systems may reshape evidentiary assessment and administrative accountability within migration governance.

Chapter 5 evaluates the adequacy of existing European legal frameworks in addressing algorithmically mediated migration governance. It focuses on regulatory gaps, institutional oversight, procedural safeguards, and the limits of current accountability mechanisms under EU migration law, human rights law, data protection law, and the AI Act. The chapter also examines broader questions concerning institutional capacity, judicial review, and algorithmic accountability.

The conclusion summarizes the principal findings of the thesis, reflects on the broader implications of algorithmic governance for migration administration and fundamental rights protection, and identifies areas for future legal and interdisciplinary research.

In addition, the thesis includes two appendices. Appendix I provides technical explanations and simplified illustrative models relating to machine learning systems, biometric matching, threshold calibration, proxy discrimination, fairness metrics, explainability mechanisms, and the role of private technological contractors involved in EU migration governance infrastructures. Appendix II focuses specifically on private contractors and outsourced technological infrastructures involved in EU migration governance, including procurement structures, interoperability systems, biometric infrastructures, and the role of corporations such as IDEMIA, Sopra Steria, Atos, IBM, and Leonardo in the development and maintenance of large-scale EU migration databases and border management systems.

2 Legal Framework Governing Decision-Making in EU Migration and Asylum Law

This chapter examines the legal framework governing decision-making within the European Union asylum and migration system and establishes the doctrinal foundation necessary for the later analysis of algorithmic decision-making. It first outlines the structure of the Common European Asylum System and the principles governing asylum determination procedures. The chapter then examines the procedural guarantees applicable to asylum decision-making, including the rights to good administration, to be heard, and to an effective remedy. It further analyzes the role of fundamental rights constraints under the Charter of Fundamental Rights of the European Union, particularly in relation to equality, non-discrimination, and procedural fairness. Finally, the chapter examines the relevance of EU data protection law and Article 22 GDPR in the context of automated decision-making and algorithmic systems used within migration governance. Together, these sections establish the legal standards against which the use of algorithmic and data-driven systems in migration administration will later be assessed.

2.1 The Structure of EU Asylum Decision-Making

The Common European Asylum System (CEAS) provides the legal framework governing the examination of applications for international protection within the European Union. It regulates how Member States assess claims for refugee status and subsidiary protection, establishing common procedural and substantive standards. Its primary objective is to establish common standards across Member States so that individuals seeking protection are treated in a similar way regardless of the state in which they apply. At the same time, the system allocates responsibility for examining applications and structures cooperation between national authorities.

The development of the CEAS is closely connected to the gradual integration of migration and asylum policy within the European Union. Prior to the late 1990s, asylum regulation remained largely within the competence of individual states, with limited coordination at the European level. This situation changed following the entry into force of the Treaty of Amsterdam in 1999, which incorporated asylum and migration matters into the EU legal framework and created the basis for developing common rules in this area[33]. The process of integration was further consolidated by the Treaty of Lisbon[34], which strengthened the EU's competence in asylum matters and anchored the objective of a Common European Asylum System in primary law under Article 78 TFEU.[35]

The CEAS is structured around several legislative instruments that regulate different aspects of asylum governance. Among the most important are the Qualification Directive[36], which defines the criteria for granting refugee status or subsidiary protection, and the Asylum Procedures Directive[37], which establishes rules governing the examination of asylum applications.

[33] Treaty of Amsterdam [1997] OJ C340/1.
[34] Treaty of Lisbon [2007] OJ C306/1.
[35] Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47, art 78.
[36] Qualification Directive (n 20).
[37] Asylum Procedures Directive (n 8).

Additional instruments, including the Reception Conditions Directive[38], the Dublin Regulation[39], and the Eurodac Regulation[40], address the treatment of asylum seekers during the procedure and determine which Member State is responsible for examining a claim. Together, these instruments form the core of CEAS.

Asylum decision-making under the CEAS is not an open-ended administrative process. It is legally constrained by specific procedural guarantees, including the requirement to carry out an individual assessment of each claim and the obligation to provide an effective remedy under Article 47 of the Charter of Fundamental Rights of the European Union. These safeguards shape both how decisions are taken and how they can be challenged.

The Court of Justice of the European Union has repeatedly emphasized that the operation of the CEAS cannot be detached from fundamental rights obligations. In *Joined Cases N.S. and M.E.*, the Court held that Member States may not automatically transfer asylum seekers under the Dublin system where substantial grounds exist for believing that systemic deficiencies in the responsible Member State create a real risk of inhuman or degrading treatment.[41] Similarly, the European Court of Human Rights in *M.S.S. v Belgium and Greece* confirmed that reliance on mutual trust within the Dublin system does not absolve states of their obligations under Article 3 ECHR.[42] These cases demonstrate that the CEAS cannot operate through purely mechanical allocation rules, but must remain constrained by individualized fundamental rights assessment.

Although these rules are established at the EU level, asylum claims are examined by administrative authorities in each Member State. These authorities conduct interviews, assess evidence, and determine whether an applicant qualifies for international protection. This requires applying EU legal standards while evaluating the specific facts of each case, including the applicant's testimony, available documentation, and country-of-origin information. This process relies heavily on human judgment, particularly in assessing credibility and incomplete evidence, and is subject to a degree of national discretion in its application. Against this background, an important question arises: how might such context-sensitive, judgment-based decision-making be affected by the increasing use of algorithmic systems that structure or influence the evaluation of evidence?

Because asylum seekers frequently flee without documentation, the assessment of credibility plays a central role in the decision-making process. EU law recognizes this and requires authorities to assess applications on the basis of the applicant's statements together with all relevant available information, even in the absence of supporting evidence.[43] Decision-makers must therefore evaluate whether the applicant's account is coherent, plausible, and consistent with known facts. In practice, this is done through personal interviews and the use of country-of-origin information produced by international organizations and specialized bodies.[44] Au-

[38] Directive 2013/33/EU of the European Parliament and of the Council of 26 June 2013 laying down standards for the reception of applicants for international protection (recast) [2013] OJ L180/96.

[39] Dublin III Regulation (n 2).

[40] Eurodac Regulation (n 1).

[41] Joined Cases C-411/10 and C-493/10 *N.S. v Secretary of State for the Home Department* EU:C:2011:865.

[42] *M.S.S. v Belgium and Greece* App no 30696/09 (ECtHR, 21 January 2011).

[43] Qualification Directive (n 20), art 4.

[44] Asylum Procedures Directive (n 8), arts 14–17.

thorities are also required to rely on precise and up-to-date information when examining applications.[45] The Court of Justice has further stressed that credibility assessment must comply with fundamental rights standards and respect human dignity. In *A, B and C v Staatssecretaris van Veiligheid en Justitie*, the Court rejected methods of assessment that disproportionately interfered with applicants' private lives or relied on degrading evidentiary practices.[46] The judgment illustrates that credibility assessment within asylum procedures is but legally constrained by broader fundamental rights obligations. These assessments depend on human interpretation and contextual reasoning, raising questions as to how such evaluation may be affected where elements of evidence assessment are influenced by algorithmic systems.

Another important aspect of asylum decision-making concerns the distribution of the burden and standard of proof. While applicants are expected to present the elements supporting their claim, EU law recognizes that individuals seeking protection may be unable to provide documentary evidence.[47] As a result, authorities must cooperate with the applicant in establishing the relevant facts and assess whether the applicant's statements are credible even in the absence of supporting documentation.[48] This reflects a shared burden of proof and confirms that asylum determination is not a purely mechanical process, but a contextual legal assessment based on both available evidence and the applicant's account.[49]

A central safeguard within the European asylum system is the requirement that each application be assessed on the basis of the individual circumstances of the applicant. This operates as a legal constraint on administrative discretion, requiring authorities to base their decisions on the specific facts of the case rather than on general assumptions about a country situation or a particular social group.[50]

This obligation is grounded in Article 4(3) of the Qualification Directive, which requires that the assessment of an application be carried out on an individual basis and in light of all relevant facts.[51] This includes both the applicant's personal situation and the conditions in the country of origin. Article 4(3) therefore functions as a safeguard against generalized or categorical reasoning in asylum procedures by requiring that protection claims be assessed through an individualized examination of the applicant's circumstances. The provision reflects the broader principle that refugee status determination cannot be reduced to statistical assumptions or group-based classifications detached from the individual applicant's situation. The purpose of this provision is to ensure that the legal criteria for protection, whether a well-founded fear of persecution for refugee status[52] or a real risk of serious harm for subsidiary protection,[53] are applied to the applicant as an individual, rather than through generalized reasoning.

In doctrinal terms, this requirement structures how evidence must be assessed within asylum procedures. Decision-makers are not limited to verifying documentary proof, but must evaluate

[45] Ibid., art 10(3)(b).

[46] Joined Cases C-148/13 to C-150/13 *A, B and C v Staatssecretaris van Veiligheid en Justitie* EU:C:2014:2406.

[47] Qualification Directive (n 20), art 4(1) and 4(5).

[48] Ibid., art 4(5); Asylum Procedures Directive (n 8), art 4(1).

[49] UNHCR, *Handbook on Procedures and Criteria for Determining Refugee Status* (2019), paras 196–204.

[50] Asylum Procedures Directive (n 8), art 10(3)(a).

[51] Qualification Directive (n 20), art 4(3).

[52] Ibid., art 2(d).

[53] Ibid., art 2(f) and art 15.

the applicant's statements together with available country-of-origin information and other relevant contextual elements. Given that asylum claims frequently involve incomplete, unavailable, or difficult-to-verify evidence, the assessment necessarily involves evaluating credibility, consistency, and plausibility in context. As Gregor Noll observes, evidentiary assessment in asylum procedures differs from conventional evidentiary models because it often requires authorities to evaluate uncertain or fragmented factual situations while remaining attentive to the vulnerability of the applicant and the difficulties inherent in obtaining proof in displacement contexts.[54] The legal standard is therefore not one of strict proof, but of establishing whether the applicant's account is sufficiently credible in light of the available information and surrounding circumstances.[55]

This requirement is reinforced by procedural guarantees contained in the Asylum Procedures Directive, including the obligation to conduct a personal interview, ensure access to interpretation where necessary, and provide a reasoned decision capable of judicial review.[56] These safeguards aim to ensure that the applicant's individual circumstances are properly examined and that the reasoning underlying the decision remains transparent and contestable. Together, they give practical effect to the principle of individualized assessment by requiring that asylum decisions remain fact-specific, context-sensitive, and legally justified. Scholarship on procedural fairness within asylum procedures has similarly emphasized that the legitimacy of refugee status determination depends not only on the substantive outcome of a case, but also on the fairness, intelligibility, and reviewability of the process through which the decision is reached.[57]

At the same time, the growing digitalization of migration governance has generated increasing discussion regarding how these procedural standards operate in practice within data-driven administrative environments. Contemporary migration governance relies extensively on large-scale databases, biometric infrastructures, and interoperable information systems that assist authorities in verifying identity, allocating procedural responsibility, and organizing migration-related data. Systems such as Eurodac, SIS, and VIS increasingly structure the administrative management of migration procedures through biometric comparison, database interoperability, and automated data correlation.[58] As recent scholarship has noted, these systems do not merely store information, but increasingly generate decision-relevant outputs that may shape how identity, procedural responsibility, and credibility are interpreted within migration governance structures.[59]

While these systems primarily function as administrative support mechanisms, scholars have noted that the increasing reliance on automated categorization, data correlation, and risk-based processing may gradually influence how information is interpreted and assessed within migration procedures. Vladislava Stoyanova warns that increasing dependence on digital systems

[54] Gregor Noll, *Proofs, Evidentiary Assessment and Credibility in Asylum Procedures* (Martinus Nijhoff 2005) 9–12.

[55] Qualification Directive (n 20) art 4(3).

[56] Asylum Procedures Directive (n 8) arts 14–17, 46.

[57] Robert Thomas, 'Assessing the Credibility of Asylum Claims: EU and UK Approaches Examined' (2006) 8(1) *European Journal of Migration and Law* 79, 82–85.

[58] Eurodac Regulation (n 1); SIS Regulation (n 3); VIS Regulation (n 3).

[59] Didier Bigo, Sergio Carrera and Elspeth Guild, 'What Future for the Area of Freedom, Security and Justice? Recommendations on EU Migration and Borders Policies in a Globalising World' (CEPS Policy Brief No 156, 2008) 14–18

within asylum administration may create tensions between data-driven governance and the individualized reasoning required under human rights law.[60] Similarly, scholarship on algorithmic governance and digital migration infrastructures has raised concerns that technical systems may indirectly structure evidentiary evaluation through predefined categories, probabilistic matching, and automated forms of classification.[61] Questions therefore arise as to how individualized assessment and contextual legal reasoning can be maintained where elements of evidentiary evaluation become increasingly structured through digital systems and computational processes. These broader accountability concerns will be examined in greater detail in later chapters.

2.2 Procedural Guarantees in EU Asylum Procedures

European Union asylum law establishes several procedural safeguards intended to ensure fairness, transparency, and accountability in the examination of applications for international protection. These guarantees play a central role in protecting the rights of asylum seekers, particularly because asylum decisions may determine whether an individual receives protection or becomes subject to removal measures[62]. Within the CEAS, procedural safeguards are primarily regulated through the Asylum Procedures Directive and are further supported by broader principles of EU administrative and fundamental rights law.

2.2.1 The Right to Good Administration

One of the key principles governing administrative procedures in the European Union is the right to good administration. This principle is recognized in Article 41 of the Charter of Fundamental Rights of the European Union and requires that public authorities handle cases impartially, fairly, and within a reasonable time.[63] The right to good administration operates not merely as a procedural formality, but as a substantive safeguard intended to ensure that decisions affecting legal status are taken through fair and accountable procedures.

Within asylum procedures, this principle is reflected in the broader requirement that applications for international protection be examined carefully, objectively, and individually. EU asylum law therefore requires authorities to assess the circumstances of each application on the basis of relevant information and appropriate procedural safeguards.[64] The principle of good administration thus supports the broader procedural framework governing refugee status determination by seeking to ensure that asylum decisions remain fair, transparent, and properly reasoned.

The requirement that asylum applications be examined objectively and individually is also closely connected to the principle of equal treatment under EU law. Article 21 of the Charter prohibits discrimination on grounds such as nationality, ethnic origin, religion, or other protected characteristics unless distinctions are legally justified within the framework of EU asylum law. This principle limits the use of generalized assumptions or stereotypical reasoning

[60] Vladislava Stoyanova, *Artificial Intelligence and Asylum Decision-Making: Any Role for Human Rights Law?* (Delmi Report 2026:3, 2025) 6–7.

[61] Edwards and Veale (n 15) 18–20; Jain, Ross and Nandakumar (n 16) 15–21.

[62] Such measures may engage the principle of non-refoulement under art 33 of the 1951 Refugee Convention and art 19 of the Charter of Fundamental Rights of the European Union.

[63] Charter (n 9) art 41.

[64] Asylum Procedures Directive (n 8) art 10(3)(a); Qualification Directive (n 20) art 4(3).

during refugee status determination and reinforces the requirement that decisions be based on the individual circumstances of each applicant.[65]

The principle of good administration also supports a broader set of procedural guarantees that structure asylum decision-making more generally. These include the obligation to provide applicants with the opportunity to present their case, the duty to give reasons for administrative decisions, and the requirement that asylum procedures remain open to effective judicial review.[66] In this sense, the principle functions as an overarching procedural safeguard intended to ensure that asylum procedures remain legally accountable and compatible with fundamental rights standards.

The importance of these safeguards becomes particularly significant within asylum procedures due to the nature of refugee status determination itself. Asylum authorities frequently operate under conditions involving incomplete documentation, complex factual circumstances, and the assessment of credibility and country-of-origin information.[67] The right to good administration therefore seeks to ensure that administrative procedures remain capable of producing decisions that are not only legally correct, but also procedurally fair and properly reasoned.

One of the reasons why digital systems have attracted increasing attention within migration governance is the longstanding difficulty of refugee status determination itself. Scholars have noted that digital databases, biometric systems, and automated tools are often presented as mechanisms capable of improving efficiency, consistency, and administrative coordination within asylum procedures.[68] At the same time, the growing reliance on digital systems within migration administration has generated broader questions regarding how procedural guarantees such as fairness, impartiality, and administrative accountability operate within increasingly digitalized forms of decision-making.[69]

2.2.2 The Right to Be Heard

Another important procedural guarantee within EU asylum law is the right of the applicant to be heard. The Asylum Procedures Directive requires applicants for international protection to be given the opportunity to explain the reasons for their application through a personal interview conducted by the competent authorities.[70] This safeguard reflects the broader principle that individuals affected by administrative decisions should be able to participate meaningfully in the procedure through which those decisions are adopted.

The Court of Justice of the European Union has repeatedly recognized the right to be heard as a general principle of EU law. In *M.M. v Minister for Justice, Equality and Law Reform*, the Court emphasized that applicants for international protection must be placed in a position

[65] Charter (n 9) art 21; A, B and C (n 46).

[66] Charter (n 9) arts 41 and 47; Asylum Procedures Directive (n 8) arts 11 and 46.

[67] UNHCR Handbook (n 49) paras 196–204; Noll (n 54).

[68] Thomas Gammeltoft-Hansen and Rosemary Byrne, 'Digital Evidence in Refugee Status Determination' (2021) *Nordic Journal of International Law* 1, 3–4; Eleni Katsikouli and others, 'Machine Learning and Asylum Adjudications: From Analysis of Variations to Outcome Predictions' (2022) 10 *IEEE Access* 130955, 130955–130956.

[69] Niovi Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill 2022); Rinaldi and Teo, 'The Use of Artificial Intelligence Technologies in Border and Migration Control and the Subtle Erosion of Human Rights' (2025) *International and Comparative Law Quarterly*.

[70] Asylum Procedures Directive (n 8) arts 14–17.

where they can effectively present observations on all elements capable of influencing the administrative decision.[71] This requirement reflects the broader principle that asylum procedures must permit meaningful participation by the applicant in the determination process.

The interview allows applicants to present their experiences, clarify inconsistencies, and provide additional information relevant to their claim. Because many asylum cases rely heavily on personal narratives and contextual explanations, the opportunity to be heard represents a crucial element of procedural fairness.[72]

At the same time, scholars have noted that the increasing use of digital evidence and data-driven technologies within asylum procedures may influence how information is collected and assessed during refugee status determination. Because asylum authorities often have to assess claims with limited evidence and difficult factual circumstances, digital tools are sometimes presented as a way to improve consistency and administrative efficiency.[73] Nevertheless, the growing use of technical systems within asylum procedures raises practical questions regarding how applicants can respond to or challenge information generated through systems they may not fully understand. The increasing use of automated systems in migration governance therefore raises important questions regarding how such systems might interact with procedural safeguards, particularly where elements of risk assessment or credibility evaluation are influenced by algorithmic tools.[74]

2.2.3 Reasoned Decisions and Explainability

Closely connected to the right to be heard is the obligation for authorities to provide reasoned decisions. Under EU asylum law, applicants must receive a written explanation of the legal and factual grounds on which their application has been accepted or rejected.[75] This obligation is closely linked to the right to an effective remedy under Article 47 of the Charter, since judicial review becomes difficult where the reasoning underlying an administrative decision cannot be properly examined.

The obligation to provide reasons serves several important functions within asylum procedures. It allows applicants to understand why a decision was reached, ensures a degree of transparency within administrative decision-making, and enables courts to review whether the relevant facts and legal standards were properly considered. Reasoned decisions also help limit arbitrary decision-making by requiring authorities to explain how they reached their conclusions on issues such as credibility, risk, and eligibility for protection.[76]

Within refugee status determination, this safeguard becomes particularly important because asylum decisions frequently involve complex factual assessments and uncertain evidentiary situations. Authorities are often required to evaluate personal testimony, country-of-origin information, and other contextual evidence in order to determine whether an applicant faces a

[71] Case C-277/11 *M.M. v Minister for Justice, Equality andLaw Reform* EU:C:2012:744 para 87.

[72] UNHCR Handbook (n 49) paras 196–204; Noll (n 54).

[73] Gammeltoft-Hansen and Byrne (n 68); William Hamilton Byrne and others, 'Data-Driven Futures of International Refugee Law' (2024) 37(4) *Journal of Refugee Studies* 915–937.

[74] Maya Ellen Hertz, Thomas Gammeltoft-Hansen and William Hamilton Byrne, 'What "Real Risk" Means For AI-Assisted Refugee Status Determination' (2025) *Verfassungsblog*; Sebastiano Antonio Piccolo and others, 'On Predicting and Explaining Asylum Adjudication' (2023) ICAIL Proceedings 217–226.

[75] Asylum Procedures Directive (n 8) art 11; Charter (n 9) art 47.

[76] Charter (n 9) arts 41 and 47.

real risk of persecution or serious harm.[77] The obligation to provide reasons therefore helps ensure that such assessments remain transparent, reviewable, and connected to the individual circumstances of the applicant.

The increasing use of digital systems and automated tools within migration governance has nevertheless generated broader discussions regarding transparency and explainability within administrative procedures. Scholars have raised concerns that technical systems may make it more difficult for applicants, lawyers, and courts to fully understand how certain conclusions or assessments were reached, particularly where administrative decisions rely upon complex forms of data processing or automated evaluation.[78] While asylum procedures formally remain subject to human decision-making, questions have emerged regarding how transparency and procedural accountability can be maintained where technical systems increasingly influence administrative reasoning and evidentiary assessment.[79]

2.2.4 The Right to an Effective Remedy

Another central procedural safeguard within EU asylum law is the right to an effective remedy before a court or tribunal. Article 47 of the Charter of Fundamental Rights of the European Union guarantees that individuals whose rights and freedoms under EU law are violated must have access to effective judicial protection.[80] Within the asylum context, this principle is reflected in Article 46 of the Asylum Procedures Directive, which requires Member States to ensure that applicants for international protection have access to an effective remedy against decisions concerning their application.[81]

The right to an effective remedy plays an important role in ensuring accountability within asylum procedures. It allows applicants to challenge errors in factual assessment, credibility findings, or the interpretation and application of asylum law. Judicial review also functions as an important safeguard against arbitrary decision-making by requiring administrative authorities to justify the legality and reasoning of their decisions before an independent body.[82]

Within refugee status determination, access to an effective remedy becomes particularly important because asylum decisions may have serious and irreversible consequences for the individuals concerned. European courts have repeatedly emphasized the importance of procedural safeguards and effective judicial protection within asylum procedures. In *M.S.S. v Belgium and Greece*, the European Court of Human Rights highlighted the importance of access to meaningful remedies within asylum systems, particularly where deficiencies in the procedure may expose individuals to a risk of ill-treatment.[83] Similarly, in *N.S. and M.E.*, the Court of Justice recognized that Member States may not transfer asylum applicants where systemic deficiencies within the receiving State create a real risk of inhuman or degrading treatment.[84]

[77] UNHCR Handbook (n 49) paras 196–204; Noll (n 54); Thomas (n 57) 82–85.
[78] Edwards and Veale (n 15) 18–20; Hertz, Gammeltoft-Hansen and Byrne (n 74).
[79] Stoyanova (n 60) 6–7; Piccolo and others (n 74); Vavoula (n 69).
[80] Charter (n 9) art 47.
[81] Asylum Procedures Directive (n 8) art 46.
[82] Charter (n 9) arts 41 and 47.
[83] *M.S.S. v Belgium and Greece* (n 42).
[84] *N.S. and M.E.* (n 41).

The increasing use of digital systems within migration governance has nevertheless generated broader discussions regarding transparency and accountability within judicial review processes. Scholars have raised concerns that technical systems may make it more difficult for applicants and courts to fully assess how certain administrative conclusions were reached, particularly where decisions rely upon complex forms of automated processing or data analysis.[85] This may create practical challenges for applicants seeking to effectively challenge decisions influenced by technical systems that are not always fully transparent or easily understandable within legal proceedings.[86]

Together, these procedural guarantees form an essential part of the legal framework governing asylum decision-making in the European Union. They ensure that asylum procedures remain transparent, accountable, and consistent with fundamental rights principles. At the same time, the increasing integration of digital infrastructures and automated decision-support tools within migration governance raises new legal questions regarding whether these safeguards can be effectively maintained when administrative decisions are partially shaped by algorithmic systems.

2.3 Data Protection and Automated Decision-Making

The increasing digitalization of migration governance has led to a growing reliance on large-scale databases, biometric identification systems, and digital administrative tools. Asylum procedures now routinely involve the collection, storage, and analysis of personal data, including biometric information and highly sensitive personal details related to an applicant's identity, background, and personal history.[87] As a result, data protection law has become an essential component of the legal framework governing migration decision-making within the European Union. The protection of personal data within migration governance is also closely connected to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, which protect the rights to privacy and data protection.[88]

The primary legal instrument regulating the processing of personal data in the European Union is the General Data Protection Regulation (GDPR).[89] The regulation establishes a set of fundamental principles that must guide all processing of personal data by both public authorities and private actors. These include the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality.[90]

These safeguards are particularly relevant within migration and asylum procedures. The examination of international protection claims frequently requires the processing of special categories of personal data under Article 9 GDPR, including information relating to ethnic origin, religion, political opinions, health status, or sexual orientation.[91] In addition, migration governance increasingly relies on digital infrastructures such as biometric databases and cross-

[85] Stoyanova (n 60) 6–7; Vavoula (n 69).

[86] Rinaldi and Teo (n 69); Hertz, Gammeltoft-Hansen and Byrne (n 74).

[87] Vavoula (n 69); Evelien Brouwer, 'Large-Scale Databases and Interoperability in Migration and Border Policies' (2020) 26 *European Public Law* 71.

[88] Charter (n 9) arts 7 and 8.

[89] GDPR (n 21).

[90] Ibid., art 5.

[91] GDPR (n 21) art 9.

border information systems designed to support identity verification and administrative coordination between Member States.[92] While these technologies can enhance administrative efficiency and cooperation, they also raise important questions regarding privacy, transparency, and individual rights.

The Court of Justice of the European Union has repeatedly emphasized that large-scale processing of personal data by public authorities engages serious fundamental rights concerns under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. In Digital Rights Ireland, the Court invalidated EU data retention legislation on proportionality grounds due to the scale and sensitivity of the data processing involved.[93] Similarly, in La Quadrature du Net, the Court stressed that generalized and indiscriminate data retention measures interfere seriously with the rights to privacy and data protection guaranteed under EU law[94]. Although these cases arose outside the asylum context, they are highly relevant for understanding the legal limits applicable to large-scale migration databases and interoperable information systems.

Within this framework, Article 22 GDPR plays a particularly significant role in regulating automated decision-making. Article 22 establishes that individuals have the right not to be subject to a decision based solely on automated processing, including profiling, where such a decision produces legal effects or similarly significant consequences for the individual.[95] Decisions concerning asylum status, residence rights, or removal from the territory clearly fall within this category, as they directly affect the legal position, safety, and fundamental rights of the person concerned.[96]

The GDPR does not entirely prohibit automated decision-making. Instead, it permits such processing in limited circumstances, including where it is authorized by law or based on the explicit consent of the individual. However, even when automated decision-making is allowed, the regulation requires the implementation of appropriate safeguards to protect the rights and freedoms of the affected person. These safeguards include the right to obtain human intervention, the possibility to express one's point of view, and the right to contest the decision.[97]

Further clarification regarding the interpretation of Article 22 has been provided through guidance issued by the Article 29 Data Protection Working Party. According to the Working Party, a decision can only be considered lawful under Article 22 if meaningful human involvement remains part of the decision-making process. A decision will still be regarded as automated if the human reviewer simply approves the algorithmic output without critically assessing it. In order for human oversight to be meaningful, the person reviewing the automated decision must

[92]Regulation (EU) 2019/817 (n 7); Regulation (EU) 2019/818 (n 31).

[93] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* EU:C:2014:238.

[94] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others*EU:C:2020:791.

[95] GDPR (n 21), art 22(1).

[96] Article 29 Working Party, Guidelines on Automated Decision-Making (n 23)21–22; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation'

[97] GDPR (n 21), art 22(3).

have the authority and competence to interpret the result, evaluate its relevance to the individual case, and modify or reject the outcome where necessary.[98]

Recent case law has reinforced the significance of Article 22 GDPR in contexts involving algorithmic assessment and probabilistic outputs. In SCHUFA Holding AG, the Court of Justice held that automated score-based assessments capable of substantially influencing legal decisions may fall within the scope of prohibited solely automated decision-making under Article 22 GDPR.[99] Although the case concerned credit scoring rather than asylum procedures, its reasoning is highly relevant in situations where algorithmic systems generate outputs that significantly shape administrative decisions affecting legal status.

The guidelines also emphasize the importance of transparency in automated decision-making. Individuals must receive meaningful information about the logic involved in the processing, as well as the significance and potential consequences of the decision. These requirements are intended to ensure that individuals can understand how decisions affecting them are made and can challenge those decisions when necessary.

These safeguards become particularly significant in the context of migration governance. Decisions concerning asylum applications often involve complex assessments of credibility, risk, and country-of-origin information. Traditionally, these assessments have relied on the professional judgment of administrative decision-makers who evaluate the evidence presented in each individual case.[100] If algorithmic systems are introduced to support or influence these assessments, questions arise regarding whether such technologies might alter how evidence is interpreted, how credibility is evaluated, or how risk is assessed.

Algorithmic systems frequently rely on probabilistic models and large datasets rather than individualized legal reasoning. As a result, they may generate classifications or predictions that influence administrative decisions without providing transparent explanations for how those outcomes were produced[101]. In such circumstances, ensuring meaningful human oversight becomes particularly challenging. If decision-makers rely heavily on algorithmic outputs without fully understanding their underlying logic, the requirement of individualized assessment and procedural fairness may be undermined. A more detailed technical explanation of probabilistic matching systems, biometric comparison processes, and algorithmic classification methods used within migration governance is provided in Annex I.

For this reason, the interaction between EU migration law and EU data protection law forms a crucial component of the legal framework governing algorithmic decision-making in migration governance. While the GDPR establishes safeguards intended to prevent harmful automated decisions, the practical implementation of these protections within migration procedures remains uncertain. Assessing whether existing legal frameworks are capable of maintaining transparency, accountability, and effective human oversight when algorithmic tools are introduced into migration administration therefore constitutes an important part of the broader analysis developed in this thesis.

[98] Article 29 Working Party, Guidelines on Automated Decision-Making (n 23).
[99] Case C-634/21 *SCHUFA Holding AG* EU:C:2023:957.
[100] Noll (n 54).
[101] Edwards and Veale (n 15) 18–20; Piccolo and others (n 74); Stoyanova (n 60) 6–7.

3 Digital and Algorithmic Systems in EU Migration and Asylum Governance

This chapter examines the technical and administrative infrastructures through which algorithmic and data-driven processes operate within EU migration and asylum governance. While the previous chapter focused on the legal framework governing asylum decision-making, the present chapter analyzes how digital systems structure the production, organization, and interpretation of information used within those procedures. The chapter first examines the principal large-scale databases underpinning EU migration governance, including Eurodac, SIS, and the VIS. It then analyzes broader categories of algorithmic tools used in migration administration, including classification systems, automated verification technologies, and data-driven decision-support mechanisms. Finally, the chapter examines the internal architecture of these systems and the operation of human-in-the-loop governance structures, focusing on how computational outputs become integrated into legal decision-making processes.

3.1 Digital Infrastructure in European Border and Migration Systems

This section examines the digital infrastructure underpinning EU migration decision-making, with a focus on systems that generate data directly used within legal procedures. The analysis centers on the Eurodac, SIS, and VIS[102], as these systems do not merely store information but produce data capable of shaping legal determinations concerning identity, responsibility allocation, admissibility, and credibility assessment. As already mentioned above, within the Dublin III framework, for example, Eurodac fingerprint matches may determine which Member State is responsible for examining an asylum application[103], while SIS alerts and VIS records may influence identity verification and the interpretation of movement history.[104] These systems are therefore significant not simply because they digitalize migration administration, but because their outputs acquire evidentiary and procedural relevance within legal decision-making processes.[105]

These systems introduce a form of technically mediated evidence into migration decision-making. Their outputs are generated through biometric comparison, database querying, and cross-system data linking, and are subsequently used within legal reasoning. Within Eurodac, this primarily occurs through biometric fingerprint matching, within SIS, through alerts and identity-based queries circulated between Member States, and within VIS, through visa records, travel histories, and identity verification data**.** While formally regulated under EU law, including data protection and fundamental rights, the reliability of these outputs depends on technical parameters such as similarity thresholds, data quality, and system calibration, which are not reflected in legal standards of proof.[106] A more detailed technical explanation of biometric matching, threshold calibration, probabilistic classification systems, and interoperability infrastructures is provided in Appendix I.**[107]**

[102] Eurodac Regulation (n 1); SIS Regulation (n 3); VIS Regulation (n 3).
[103] Dublin III Regulation (n 2).
[104] Vavoula (n 69) 87–112.
[105] Brouwer (n 85) 74–78.
[106] GDPR (n 21).
[107] Appendix I.A–I.D.

3.1.1 Eurodac and Biometric Matching

Eurodac operates through Automated Fingerprint Identification Systems, which convert fingerprint images into digital templates by extracting minutiae points, including ridge endings (where a fingerprint line terminates) and bifurcations (where a ridge splits into two), and comparing them against stored entries. This comparison produces a similarity score, and a match is registered when the score exceeds a predefined threshold. A threshold, in this context, refers to the cut-off point used by the system to determine whether two fingerprints correspond to the same individual: the system compares two templates and assigns a similarity score indicating how closely they match, if the score exceeds the threshold, it is classified as a match, whereas if it falls below, it is not. This threshold is not inherent to the technology but is set during system design and calibration by system operators within the EU's technical and regulatory framework (notably under the supervision of bodies such as eu-LISA), reflecting institutional choices about acceptable error rates. The score itself is probabilistic, as it depends on image quality, partial prints, and algorithmic configuration, while the threshold determines the trade-off between false positives and false negatives: a lower threshold increases the likelihood of matches but also the risk of incorrectly linking different individuals (false positives), whereas a higher threshold reduces such risks but increases the likelihood of failing to detect true matches (false negatives).[108]

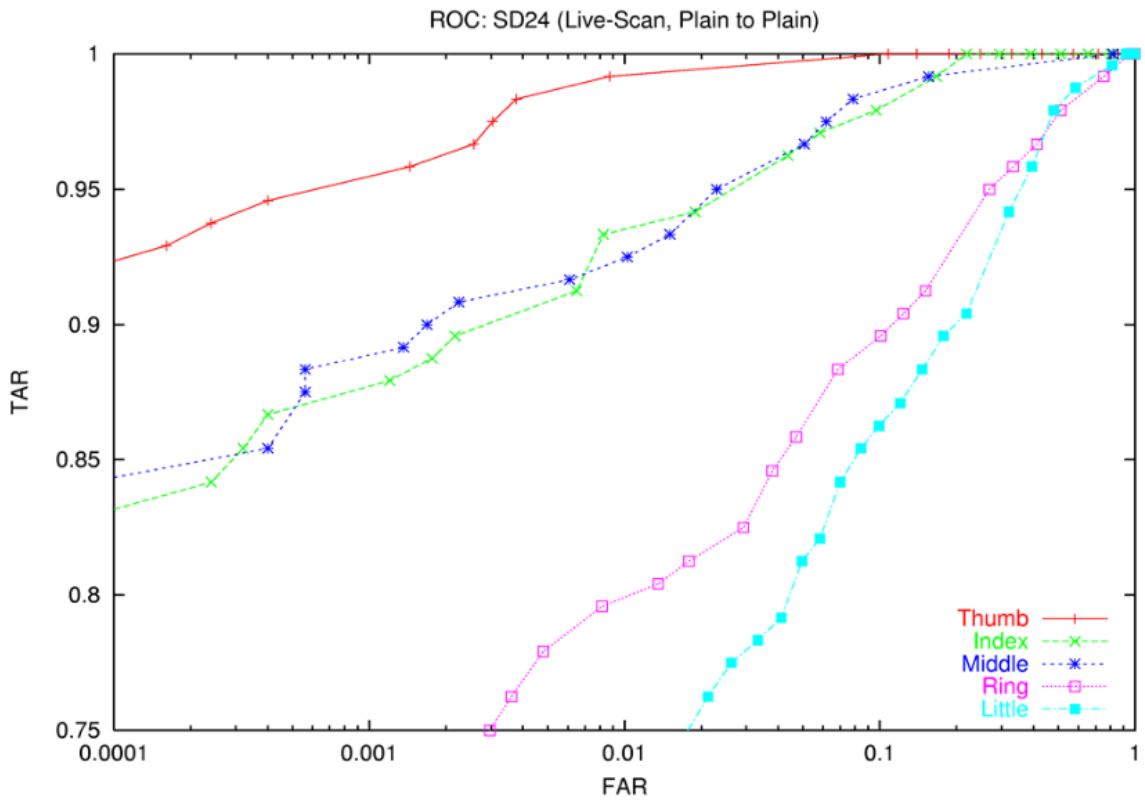


Figure 1, Relationship Between False Accept Rate (FAR) and True Accept Rate (TAR) Across Different Fingers in the NIST SD24 Verification Study
Source: NIST SD24 Verification Study, p. 25

[108] NIST Special Database 24 (n 6).

Figure 1 illustrates the relationship between false accept rate and true accept rate in fingerprint matching systems. As shown, system performance varies depending on the threshold applied, even at a fixed false accept rate of 1 percent, true accept rates range from 99 percent for thumbs to 70 percent for little fingers. This demonstrates that matching outcomes depend on calibrated trade-offs rather than certainty, and that a "match" reflects a threshold-based classification rather than definitive identification. In other words, the system does not "recognize" a person with certainty but makes a decision based on how strict or lenient the settings are. These calibrated trade-offs are achieved by adjusting the threshold: system designers and operators choose how similar two fingerprints must be before the system counts them as a match. Lowering the threshold makes the system more permissive (it finds more matches but increases the risk of mistakes), while raising it makes the system stricter (it reduces errors but may miss real matches). The figure therefore demonstrates how technical calibration choices directly shape the reliability and evidentiary value of biometric outputs later used within legal and administrative procedures[109].

Figure 2, Variability in Fingerprint Matching Accuracy Across Different Biometric Samples

SD24 FAR @ 1% & TAR @ 98%	
Thumb	
(1%, 99%)	(0.4%, 98%)
Index	
(1%, 94%)	(10%, 98%)
Middle	
(1%, 92%)	(8%, 98%)
Ring	
(1%, 80%)	(51%, 98%)
Little	
(1%, 70%)	(48%, 98%)

Source: NIST SD24 Verification Study, p. 25

The variation across fingers further confirms that matching accuracy is not uniform, but dependent on the quality and characteristics of the biometric data. These parameters, including similarity thresholds, calibration settings, and matching tolerances, are determined during system design and operational management by technical authorities and system operators, particularly eu-LISA and private contractors responsible for system development and maintenance. However, they do not normally appear within the reasoning of asylum decisions or judicial proceedings. As a result, applicants and reviewing courts are generally presented only with the final output, such as a "match" or "no match," without access to the technical assumptions and calibration choices that shaped that result. Yet this output is treated as a factual element, for example to establish prior entry or responsibility under the Dublin Regulation.[110] Appendix I.C

[109] Ibid.
[110] Dublin III Regulation (n 2).

and Appendix I.D further explain how threshold-based classification systems and calibration variability influence algorithmic outputs within migration governance systems[111].

3.1.2 The Schengen Information System (SIS)

SIS operates differently from Eurodac, as it is not primarily based on biometric comparison but on the circulation of alerts and administrative information between Member States. Established as a large-scale information-sharing system within the Schengen Area, SIS allows national authorities to upload and retrieve alerts relating to individuals and objects for purposes including border management, law enforcement, and migration control.[112] Within migration governance, SIS is particularly relevant because it enables Member States to circulate information concerning return decisions, entry bans, refusals of entry, and identity-related alerts.[113]

Unlike Eurodac, which generates outputs through fingerprint comparison, SIS functions primarily through database querying and cross-border administrative communication. National authorities may search the system using identity data, biometric information, or travel documents in order to determine whether an individual is associated with an existing alert entered by another Member State.[114] In practice, this means that asylum and migration authorities may rely on information generated elsewhere within the EU administrative system without independently reassessing the factual or legal basis upon which the original alert was created.

For example, a return decision or entry ban entered into SIS by one Member State may subsequently be retrieved and relied upon by authorities in another Member State during migration or asylum procedures.[115] This may influence decisions concerning admissibility, identity verification, procedural responsibility, or credibility assessment. In this sense, SIS functions not simply as a database storing information, but as a mechanism through which administrative determinations circulate and acquire evidentiary relevance across interconnected legal systems.

The system therefore introduces a form of distributed administrative evidence. Rather than producing entirely new evidentiary outputs through biometric calculation, SIS allows prior administrative decisions and alerts generated by one authority to influence decision-making elsewhere within the European Union. This creates a situation in which part of the evidentiary basis underlying a migration-related decision may originate outside the authority currently examining the case.[116]

This raises important questions concerning transparency, accountability, and procedural fairness. Individuals affected by SIS alerts may not always have access to the reasoning underlying the original alert, the evidence upon which it was based, or the circumstances under which it was entered into the system.[117] At the same time, national authorities relying on the alert may treat it as a reliable administrative indicator without independently reassessing the factual basis of the information. The evidentiary foundation of the decision is therefore partially externalized across interconnected administrative infrastructures.

---

[111] Appendix I.C–I.D.
[112] SIS Regulation (n 3).
[113] SIS Regulation (n 3) arts 3–6.
[114] SIS Regulation (n 3) arts 3–6.
[115] Brouwer (n 85) 74–78.
[116] Mitsilegas (n 98).
[117] Charter (n 9) arts 41 and 47; GDPR (n 21).

From a technical perspective, SIS also forms part of the EU's broader interoperability architecture linking multiple migration and border management systems. Through interoperability frameworks managed by eu-LISA, SIS may interact with systems such as Eurodac and VIS, allowing authorities to retrieve interconnected information across different databases simultaneously.[118] A more detailed explanation of interoperability infrastructures and shared biometric systems is provided in Appendix I.I.[119]

The increasing integration of SIS within EU migration governance demonstrates how digital infrastructures can influence legal decision-making even where no fully automated decision is formally taken. Although human authorities remain legally responsible for final decisions, the circulation of alerts and interconnected administrative data may shape how information is interpreted, prioritized, and relied upon within migration procedures. These dynamics become particularly significant in contexts where individuals face difficulties challenging or understanding the technical and administrative structures through which such information is produced and shared.

3.1.3 The Visa Information System (VIS)

VIS operates as a large-scale database designed to support the exchange of visa-related information between Member States. Originally developed to facilitate the management of short-stay visas within the Schengen Area, VIS stores biometric data, visa applications, travel documents, photographs, and records concerning previous visa decisions.[120] Within migration governance, VIS is particularly significant because it allows authorities to retrieve information concerning an individual's travel history, visa status, and prior interactions with migration authorities across different Member States.

Like SIS, VIS functions primarily through database retrieval and cross-border administrative coordination rather than through autonomous biometric identification. However, biometric comparison still plays an important role within the system, as fingerprint data and facial images may be used to verify whether a person corresponds to an existing visa record.[121] This enables authorities to connect individuals to prior visa applications, travel movements, or migration histories stored within the system.

Within asylum procedures, VIS records may acquire evidentiary significance in several ways. Information concerning prior visa applications, travel routes, or entries into the Schengen Area may be used to assess which Member State bears responsibility under the Dublin framework.[122] VIS data may also influence assessments concerning identity verification, travel history, or the consistency of an applicant's account. As a result, information originally collected for visa administration may later become incorporated into asylum and migration decision-making processes.

The system therefore illustrates how administrative data collected for one purpose may subsequently acquire evidentiary relevance within a different legal context. Information initially gathered to process a visa application can later influence determinations relating to asylum

[118] Regulation (EU) 2019/817 (n 7); Regulation (EU) 2019/818 (n 90).
[119] Appendix I.I.
[120] VIS Regulation (n 3).
[121] VIS Regulation (n 3) arts 5–9.
[122] Dublin III Regulation (n 2).

responsibility, identity assessment, or procedural admissibility**.** This reflects the increasingly interconnected nature of EU migration governance, where data circulates across multiple systems and administrative functions.[123]

VIS also forms part of the EU's broader interoperability framework linking migration, border management, and law enforcement databases. Through interoperability mechanisms managed by eu-LISA, authorities may retrieve interconnected records from multiple systems simultaneously, including Eurodac and SIS.[124] This infrastructure is intended to facilitate information-sharing and improve administrative coordination between Member States. At the same time, it contributes to the expansion of large-scale data-driven governance structures within migration administration.

From a procedural perspective, the increasing reliance on interconnected database systems raises important questions concerning transparency and evidentiary reliability. Individuals affected by decisions relying on VIS data may not always understand how information has been retrieved, linked, or interpreted across systems. Moreover, migration authorities may rely heavily on database records as objective indicators of identity or movement history, even though such records remain dependent upon the quality, completeness, and accuracy of the underlying data entered into the system.[125]

The legal significance of VIS therefore extends beyond its original visa-management function. As migration systems become increasingly interoperable, VIS contributes to a broader administrative environment in which digital records, biometric identifiers, and interconnected databases progressively shape how migration-related decisions are formed and justified. A more detailed explanation of interoperability systems and shared data infrastructures is provided in Appendix I.I.[126]

Across Eurodac, SIS, and VIS, a common structural feature emerges: migration decision-making increasingly relies on digital outputs generated through biometric comparison, database interoperability, and cross-system information processing. Although these systems formally operate as administrative support mechanisms, their outputs may significantly shape how identity, procedural responsibility, credibility, and movement history are interpreted within legal procedures. As the European Union Agency for Fundamental Rights has observed, the growing use of biometric and interoperable migration databases raises important concerns regarding transparency, proportionality, data protection, and effective access to remedies for affected individuals.[127] Unlike traditional documentary evidence, these systems frequently generate probabilistic or technically mediated outputs whose reliability depends on threshold settings, data quality, and technical calibration choices that remain largely invisible within legal reasoning itself.[128] The increasing integration of these systems into migration governance therefore raises broader questions concerning transparency, accountability, procedural fairness, and the ability

[123] Vavoula (n 69) 115–130; Brouwer (n 85) 74–78.

[124] Regulation (EU) 2019/817 (n 7); Regulation (EU) 2019/818 (n 90).

[125] GDPR (n 21); Charter (n 9) arts 7, 8 and 47.

[126] Appendix I.I.

[127] European Union Agency for Fundamental Rights, *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights* (2018) 11–19; Charter (n 9) arts 7, 8, 41 and 47; Vavoula (n 69) 115–130; Brouwer (n 85) 74–78.

[128] Edwards and Veale (n 15) 18–20; Appendix I.C–I.H.

of existing legal safeguards to operate effectively within increasingly data-driven administrative environments. These issues will be examined in greater detail in the following chapters.

3.2 Algorithmic Tools in Migration Management

The previous section examined the digital infrastructures through which migration-related data is collected, stored, and circulated across EU systems. Building upon this, the present section focuses on algorithmic tools that operate on such data in order to classify, verify, prioritize, or otherwise structure administrative decision-making processes. While these systems do not formally replace human decision-makers, they increasingly influence how information is interpreted and processed within migration governance. Their legal significance lies not only in the outputs they generate, but also in the fact that many of the computational processes shaping those outputs remain largely invisible within the reasoning of the final administrative decision.

3.2.1 Risk Classification Systems

A first category concerns risk classification systems, which operate by transforming input data into predefined risk categories. In the EU context, ETIAS provides a clear example. ETIAS processes personal data, including nationality, travel history, and security-related indicators, through automated cross-checking against databases such as SIS, VIS, and Europol systems.[129] It applies rule-based criteria and statistical correlations to assign individuals to risk profiles, reflecting a broader move towards predictive and classification-based governance.[130]

From a technical perspective, such systems function by mapping input variables onto predefined rules or learned patterns. For example, combinations of attributes such as nationality, travel history, or movement patterns may become associated with higher risk scores based on statistical correlations identified within datasets. Empirical research on asylum adjudication demonstrates that machine learning models can predict decision outcomes based on variables such as nationality, gender, and other attributes, highlighting how classification systems may reproduce or amplify patterns present in the data.[131]

The legal issue arises at the point where these classifications are relied upon in decision-making. EU asylum law requires that each application be assessed individually, on the basis of the applicant's specific circumstances.[132] However, the use of generalized risk categories introduces a form of reasoning based on group characteristics and statistical inference rather than individualized evidentiary assessment. Where such classifications rely on variables such as nationality , travel patterns, language, or geographic origin, they may reproduce structural patterns of differentiation capable of giving rise to indirect discrimination within the meaning of Article 21 of the Charter.[133] As scholarship on algorithmic governance has demonstrated, systems relying on statistical correlations may reproduce discriminatory effects even where protected characteristics are not explicitly used as decision variables.[134] The legal concern is therefore not the existence of classification systems as such, but the integration of their outputs into

[129] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorization System (ETIAS) [2018] OJ L236/1.

[130] Access Now and others, *Uses of AI in Migration and Border Control*

[131] Katsikouli and others (n 68).

[132] Asylum Procedures Directive (n 8) art 4.

[133] Charter (n 9) art 21.

[134] Barocas and Selbst (n 130);Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (OUP 2020).

administrative decision-making without disclosure of the underlying criteria or meaningful opportunities for contestation. This becomes particularly significant in migration governance, where individuals may not know why they were categorized as "high risk" or subjected to additional scrutiny, while the technical logic underlying the classification remains inaccessible within the administrative process itself.

The broader concern is therefore not automation alone, but the increasing incorporation of predictive and data-driven forms of reasoning into legal procedures traditionally based on individualized assessment and contextual evaluation.[96]

3.2.2 Automated Identity and Document Verification

A second category concerns automated identity and document verification systems, which are used during registration and early-stage processing. These systems rely on biometric matching, optical character recognition, and rule-based validation techniques. For instance, biometric systems extract features from fingerprints or facial images and compare them against stored templates using similarity metrics, producing outputs such as "match" or "no match."[135] As discussed in relation to Eurodac, these outputs are generated through probabilistic comparison processes based on threshold settings and similarity scoring rather than definitive identification.

Document verification systems operate by analyzing both visual and machine-readable features contained within identity documents. These systems examine elements such as typography, spacing, document layouts, holograms, watermarks, embedded chips, barcodes, and security patterns in order to identify signs of alteration, forgery, or inconsistency. Optical character recognition technologies may additionally extract textual information and compare it against database records or standardized document templates. Through these processes, the system generates assessments concerning the authenticity or reliability of the document presented.

These technologies are widely deployed within EU migration infrastructure, often through systems developed by private contractors working with public authorities. Their outputs function as preliminary assessments of identity or data consistency, shaping how cases are subsequently evaluated. More broadly, the increasing reliance on digital evidence reflects a shift in refugee status determination from narrative-based assessment towards data-driven verification.[136]The legal issue arises where such system-generated outputs influence the assessment of credibility or identity without being subject to scrutiny. Under EU asylum law, credibility must be assessed through a holistic and individualized evaluation of the applicant's statements and evidence.[137] However, when an applicant is flagged as "inconsistent" or "unverified" based on automated checks, this introduces an evidentiary element whose technical basis is not disclosed. The legal concern occurs when these outputs are relied upon without the applicant being able to understand or challenge how they were produced, thereby limiting the effectiveness of procedural guarantees and the right to contest the evidence used against them.[138] The European Union Agency for Fundamental Rights has similarly warned that the growing use of biometric

[135] Jain, Ross and Nandakumar (n 16).

[136] Gammeltoft-Hansen and Byrne (n 68).

[137] Qualification Directive (n 20) art 4.

[138] Charter (n 9) art 41.

and interoperable systems within migration governance may affect transparency, data protection, and effective access to remedies, particularly where individuals are unable to meaningfully challenge system-generated outputs.[139]

A more detailed technical explanation of biometric matching systems, threshold calibration, and document verification processes is provided in Appendix I.A–I.D.[140]

3.2.3 Data-Driven Decision-Support and Case Management Systems

A third category consists of data-driven decision-support systems used for case management and prioritization, which aggregate information from multiple sources, including Eurodac, SIS, VIS, and increasingly digital evidence such as mobile phone data. These systems apply rule-based or statistical models to organize administrative workflows, for example by prioritizing certain cases or flagging them for additional scrutiny. Unlike biometric verification systems, which focus on confirming identity, these tools primarily structure how information is organized, processed, and prioritized within administrative procedures.

Empirical research shows that such data sources are already integrated into asylum decision-making, with digital data, including information extracted from mobile devices, contributing directly to case evaluation and credibility assessment. Research on asylum casework in Denmark has demonstrated how mobile phone data may be used to reconstruct movement histories, verify elements of personal narratives, or identify inconsistencies within applicants' accounts[141]. Although these systems do not formally determine the outcome of asylum applications, they shape procedural trajectories in ways that are not visible in the final decision. Their legal relevance lies in this indirect influence, they affect how cases are processed, what evidence is considered relevant, and how administrative attention is distributed.

This creates a gap in legal accountability, as individuals cannot challenge influences on their case that are not explicitly articulated in the reasoning of the decision, raising concerns in relation to the right to an effective remedy under Article 47 of the Charter.[142] Where digital systems influence procedural prioritization or credibility assessment without disclosure of the underlying logic or data correlations involved, individuals may face difficulties understanding how conclusions concerning their application were reached.

Taken together, these systems introduce decision-relevant elements through processes based on classification, pattern recognition, and threshold-based evaluation. The legal problem is not automation as such, but the integration of these processes into decision-making without corresponding legal visibility. As a result, elements that shape outcomes remain outside the scope of reasoning, disclosure, and review, limiting the practical effectiveness of safeguards established under EU law.

[139] FRA, Under Watchful Eyes (n 127).

[140] Appendix I.A–I.D.

[141] Trine Rask Nielsen, Thomas Gammeltoft-Hansen and Naja Holten Møller, 'Mobile Phone Data Transforming Casework in Asylum Decision-making: Insights from the Danish Case' (2024) 1(4) *ACM Journal on Responsible Computing*.

[142] Charter (n 9) art 47.

3.3 Architecture of Algorithmic Decision Systems

The previous section identified the main categories of algorithmic tools currently used within EU migration governance. Building upon this, the present section explains, in simplified terms, how such systems technically process data and generate decision-relevant outputs. This is important because the legal concerns discussed above, particularly regarding transparency, individualized assessment, and effective review, emerge directly from these underlying computational processes[143].

Algorithmic systems used in EU migration procedures operate through layered processing structures in which raw inputs are progressively transformed into decision-relevant outputs. Rather than functioning as isolated tools, these systems are embedded within broader administrative infrastructures and rely on sequences of operations that determine how data is structured, interpreted, and ultimately translated into elements that shape legal decision-making.[144]

The process begins with data structuring and feature extraction, where heterogeneous inputs, including biometric data, application records, and cross-system identifiers, are converted into standardized and comparable formats. In biometric systems, for example, fingerprint images are transformed into digital templates through the extraction of minutiae points, enabling large-scale comparison across databases.[145] A simplified explanation of biometric template generation and minutiae extraction is provided in Appendix I.A. In computational terms, this involves reducing complex inputs to a set of features that can be processed algorithmically:

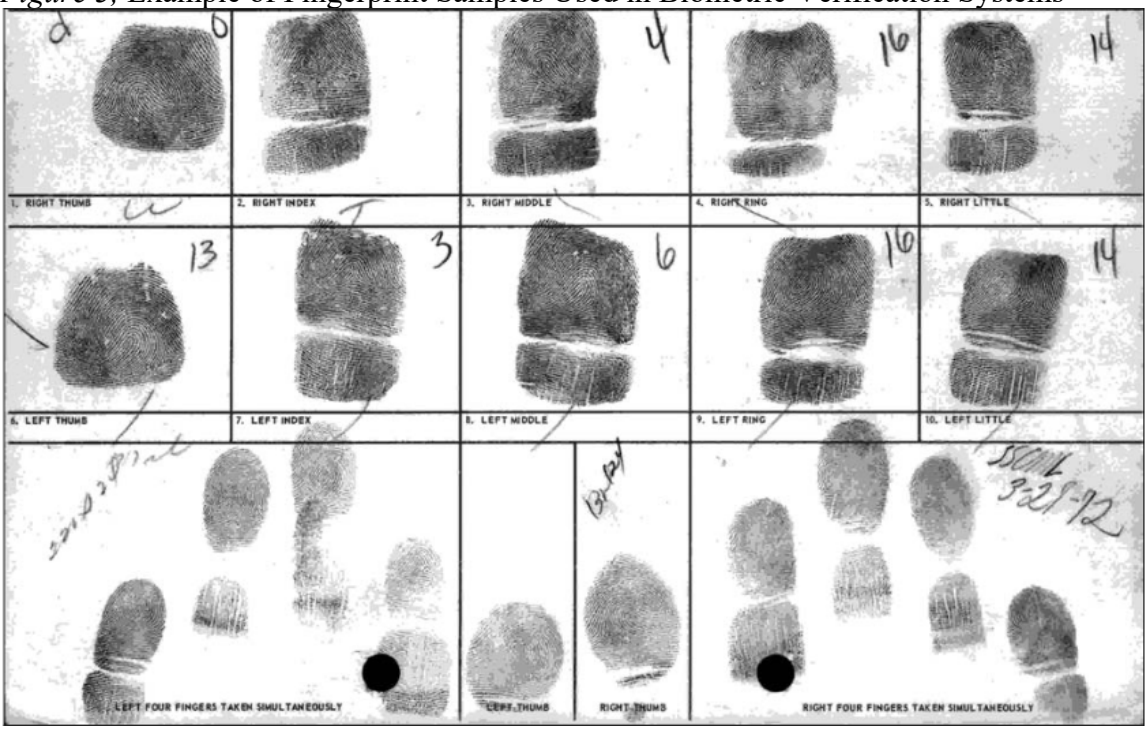
```
features = extract_minutiae(fingerprint_image)
```

[143] For more detailed technical demonstrations relating to biometric matching, feature extraction, threshold calibration, and document verification processes, see Appendix I.A–I.D.

[144] Evelien Brouwer, 'AI and Migration, Asylum and Border Control Management: Impact of the AI Act' in O Tambou and M Sweeney (eds), *Le règlement européen sur l'IA et au-delà. Quel encadrement de l'IA ?* (Bruylant 2025) https://dspace.library.uu.nl/handle/1874/483060 accessed 28 February 2026.

[145] Jain, Ross and Nandakumar (n 16).

Figure 3, Example of Fingerprint Samples Used in Biometric Verification Systems[146]



Source: NIST SD24 Verification Study, p. 25

At this stage, the system establishes the parameters within which the case becomes legible to computational processing. Only those elements that can be encoded as structured variables, such as identity markers, movement records, or prior procedural interactions, are incorporated into the system. Empirical work on digital evidence in refugee status determination shows that this process privileges data that can be formalized and cross-referenced, while contextual or narrative elements remain outside the scope of automated processing.[147] The legal issue arises where this technical structuring indirectly constrains the range of elements considered in the assessment, potentially affecting the requirement of an individual examination under Directive 2013/32/EU.[148]

The second stage involves automated comparison and classification, where structured data is evaluated against existing records or predefined patterns. In biometric matching, this involves computing similarity scores between templates; in database systems, it involves linking identifiers across datasets; and in more complex systems, it may involve classification models that associate combinations of variables with specific outcomes. At a conceptual level, this can be represented as:

```
score = similarity(features_1, features_2)
category = model.predict(applicant_data)
```

[146] This figure illustrates fingerprint samples collected for biometric verification and comparison testing. Biometric systems transform such fingerprint images into digital templates through the extraction of minutiae points, including ridge endings and bifurcations, which are then compared across databases using similarity scoring techniques. Variations in image quality, finger position, pressure, and partial prints may affect the resulting similarity score and therefore influence matching outcomes within automated identification systems.

[147] Gammeltoft-Hansen and Byrne (n 68).

[148] Asylum Procedures Directive (n 8).

The operation of similarity scoring, probabilistic classification, and biometric comparison thresholds is discussed further in Appendix I.B–I.C.

For the decision-maker, these processes are not visible as computations, but as system-generated outputs, such as identity matches, prior application records, or inconsistency flags. These outputs are the result of pattern-based processing rather than direct evidentiary verification. Research on machine learning in asylum adjudication demonstrates that such models identify correlations between variables, including nationality or procedural factors, and decision outcomes, illustrating how classification mechanisms operate through generalization across cases.[149]The legal issue arises at the point where these outputs are incorporated into the evaluation of the applicant. Although formally treated as factual elements, they are derived from processes based on correlation and similarity rather than direct evidence. This introduces a shift from evidentiary reasoning to data-driven inference. Where such outputs influence credibility assessments or procedural decisions without disclosure of the underlying logic, this limits the ability to meaningfully contest them and raises issues in relation to procedural guarantees and effective judicial protection.[150]

The final stage concerns threshold-based output generation, where intermediate results are translated into administratively actionable outcomes. Most systems do not produce definitive conclusions, but scores or probabilities, which are then converted into binary or categorical outputs through threshold settings. This can be represented in simplified form as:

```
if score >= threshold:
   result = "MATCH"
else:
   result = "NO_MATCH"
```

The critical point is that the threshold determines the outcome. In practice, threshold calibration reflects trade-offs between false positives and false negatives, meaning that system outputs are contingent rather than certain. Studies of biometric systems confirm that small variations in threshold settings can significantly alter results.[151]A simplified illustration of threshold calibration and error-rate trade-offs is included in Appendix I.B. The legal issue emerges where these threshold-based outputs are treated as conclusive within administrative procedures. The transformation from probabilistic score to categorical result is not reflected in the reasoning of the decision, yet it directly shapes the evidentiary basis on which the decision relies. This affects the ability of the applicant to understand how the result was produced and to challenge its reliability, engaging safeguards under Article 22 GDPR and the right to an effective remedy under Article 47 of the Charter.[152]

Taken together, these stages demonstrate that algorithmic systems structure not only how data is processed, but how it becomes legally relevant. Data selection determines what can be considered, classification shapes how the case is interpreted, and thresholds determine which outcomes are triggered. The legal concern arises from the cumulative effect of these processes, where technical operations influence decision-making without being fully integrated into legal reasoning, disclosure, or review.

[149]Katsikouli and others (n 68).

[150] Charter (n 9) arts 41, 47.

[151] NIST Special Database 24 (n 6).

[152] GDPR (n 21) art 22; Charter (n 9) art 47.

3.4 Human-in-the-Loop Governance

Human-in-the-loop governance in EU migration systems refers to the integration of algorithmic systems into decision-making processes while maintaining formal human responsibility for the final outcome. In technical terms, these systems are designed as decision-support architectures, where computational processes generate outputs, such as matches, classifications, or risk indicators, which are then reviewed and acted upon by a human decision-maker.[153]

In practice, this interaction follows a structured workflow. An asylum officer does not engage directly with raw data, but with system-generated outputs. For example, biometric systems produce identity matches based on similarity scores, database systems retrieve prior applications or travel records, and classification systems may flag inconsistencies or risk indicators. At the interface level, this appears as a set of predefined results, such as "match," "inconsistency detected," or "requires further verification," rather than as a transparent computational process.[154]

This model is widely implemented across EU migration infrastructures. Systems such as Eurodac, VIS, and SIS generate outputs that are routinely integrated into asylum procedures, while additional data sources, including digital evidence extracted from mobile devices, are increasingly used to support credibility assessments[155]. Empirical research shows that such data is not merely supplementary, but actively shapes how cases are constructed and evaluated within administrative processes.[156]Furthermore, from a sociotechnical perspective, this form of interaction affects how decisions are made. Human decision-makers tend to rely on system outputs, particularly where those outputs are presented as objective or technically derived. This phenomenon, often described as automation bias, refers to the tendency to favor machine-generated results over independent judgment. In contexts characterized by high caseloads and limited time, such as asylum procedures, reliance on system outputs may become routine, reducing the extent to which decision-makers critically assess or depart from them.[157]

The legal relevance of human-in-the-loop systems lies not in the presence of a human actor, but in the quality of their involvement. Under EU law, the prohibition of solely automated decision-making under Article 22 GDPR and the requirement of individualized assessment under Directive 2013/32/EU assume that the decision-maker exercises independent judgment.[158] However, where system outputs pre-structure the decision-making process, the role of the human may be limited to confirming or validating those outputs.

The critical moment arises where reliance on algorithmic outputs replaces substantive evaluation. For example, where a biometric match is accepted without scrutiny, or where a system-generated inconsistency shapes the assessment of credibility, the decision is formally taken by a human but substantively influenced by the system. In such cases, the distinction between

[153] Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12(4) Regulation & Governance 505.

[154] European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), 'Large-Scale IT Systems' https://www.eulisa.europa.eu/activities/large-scale-it-systems accessed 28 February 2026.

[155] Gammeltoft-Hansen and Byrne (n 68).

[156] Nielsen, Gammeltoft-Hansen and Møller (n 139).

[157] Linda J Skitka, Kathleen L Mosier and Mark Burdick, 'Does Automation Bias Decision-Making?' (1999) 51(5) *International Journal of Human-Computer Studies* 991.

[158] GDPR (n 21) art 22; Asylum Procedures Directive (n 8)

automated and non-automated decision-making becomes difficult to sustain in practice.[159] This has direct implications for legal safeguards. First, the requirement to provide reasons under Article 41 of the Charter is affected where decisions rely on system outputs whose underlying logic is not disclosed. Second, the right to an effective remedy under Article 47 is limited where individuals cannot identify or challenge the elements that influenced the decision. Third, where system outputs rely on correlations linked to protected characteristics, their use may give rise to indirect discrimination under Article 21 of the Charter.[160]

Human-in-the-loop governance therefore operates as a formal safeguard that may not fully address the substantive influence of algorithmic systems. The central issue is not whether a human is involved, but whether that involvement remains independent, informed, and capable of departing from system-generated outputs. Where this is not the case, algorithmic systems effectively shape decision-making while remaining only partially visible within the legal framework.

[159] Wachter, Mittelstadt and Floridi (n 96)
[160] Charter (n 9) arts 21, 41, 47

4 Structural Tensions Between Algorithmic Systems and Legal Standards

The previous chapters examined both the legal framework governing asylum decision-making within the European Union and the digital infrastructures increasingly integrated into migration governance. Together, these developments reveal a broader transformation in the structure of administrative decision-making. While asylum procedures continue to operate formally within a legal framework centered on individualized assessment, procedural fairness, and effective judicial protection, many decision-relevant elements are now generated through computational systems relying on statistical classification, biometric matching, and data correlation.

This chapter examines the tensions arising from the interaction between these technical processes and the legal standards governing asylum procedures under EU law. It argues that algorithmic systems do not simply support administrative decision-making, but alter the conditions under which legal accountability operates. The integration of probabilistic and data-driven outputs into asylum procedures challenges core assumptions underlying administrative law, including the ability of authorities to fully reconstruct the factual basis of decisions, provide legally intelligible reasoning, and ensure meaningful contestability. The chapter therefore focuses on how their operational logic interacts with principles such as individualized assessment, transparency, procedural fairness, and effective judicial protection.

4.1 Individualized Legal Reasoning vs Statistical Classification

Chapter 3 showed that migration governance increasingly relies on computational systems that generate classifications, matches, and risk indicators before the formal legal assessment takes place. Once these outputs enter the asylum procedure, they become part of the factual basis of the case. The issue is therefore not simply the use of digital technologies, but the growing role of computational systems in shaping how asylum claims are interpreted and processed.

Under EU asylum law, authorities must assess applications individually and provide reasoned decisions based on the applicant's personal circumstances.[161] The EUAA Practical Guide on Evidence and Risk Assessment also emphasizes that asylum procedures require an individual, objective, and impartial assessment that takes into account factors such as trauma, memory distortion, cultural differences, vulnerabilities, and interview conditions.[162] However, computational systems operate differently. Rather than evaluating the applicant's narrative holistically and contextually, these systems identify statistical patterns across existing datasets and compare new cases against predefined categories, correlations, or risk indicators[163]. This creates tensions with the individualized and context-sensitive reasoning traditionally required within asylum procedures, particularly where technical classifications begin to influence how credibility, consistency, or risk are interpreted within administrative decision-making[164].

[161] Asylum Procedures Directive (n 8) arts 10(3), 11(2); Qualification Directive (n 20) art 4(3).

[162] EUAA, *Practical Guide on Evidence and Risk Assessment* (2024) 16–18 discussing individual examination, objective assessment, transparency, and factors affecting evidence assessment.

[163] Christopher M Bishop, *Pattern Recognition and Machine Learning* (Springer 2006) 179–186; Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* (MIT Press 2016) 96–110.

[164] EUAA, Practical Guide on Evidence and Risk Assessment (n 162) 16–18.

In practice, this means that systems may transform elements of an asylum claim into data points such as nationality, age, language, travel history, biometric information, previous registrations, or inconsistencies in testimony.[165] These variables are then compared with historical datasets to generate classifications, alerts, or risk indicators.

For example, an applicant who fled detention and torture may struggle to provide a fully coherent chronology during interviews because of trauma, memory gaps, or confusion regarding dates and locations. Within data-driven systems, repeated inconsistencies or corrections in testimony may still be treated as indicators statistically associated in earlier datasets with unreliable claims or identity concerns.[166] As a result, the applicant may gradually be perceived as less credible even where the inconsistencies are explainable through the circumstances of persecution or displacement.

A similar issue may arise in relation to biometric or registration systems. During displacement, applicants are often registered multiple times in different countries, detention centers, or reception facilities under slightly different spellings, translations, or dates of birth. Interoperable systems may treat these discrepancies as anomalies or identity inconsistencies because the system compares entries through similarity scores and matching thresholds rather than contextual legal interpretation.[167] Even where the inconsistencies result from translation problems, fear, exhaustion, or mistakes made during registration, the existence of multiple entries may still influence how authorities perceive the applicant's reliability during later asylum procedures.

Statistical classifications may also affect how cases are prioritized. While individual assessment requires careful consideration of contextual factors rather than rigid assumptions, prioritization systems frequently rely on standardized indicators and predefined categories.[168] Applicants whose vulnerabilities are less visible within structured categories may therefore receive reduced procedural attention despite facing serious protection risks. For example, a survivor of sexual violence who initially avoids disclosure because of shame or fear may not immediately fit predefined vulnerability indicators used during screening procedures, potentially affecting access to support or procedural safeguards at an early stage.

These systems also frequently operate through thresholds and scoring mechanisms rather than fixed factual determinations. Small changes in calibration settings may alter whether an applicant is flagged for additional review, categorized as presenting elevated risk, or treated as inconsistent despite no change in the underlying facts of the case.[169] In practice, technical design choices may therefore influence procedural outcomes in ways that remain difficult for applicants to identify or challenge.

This creates tension with individualized assessment under Article 4(3) of the Qualification Directive.[170] As Røhl and Hansen explain, automated administrative systems may create trade-

[165] For technical discussion of feature vectors, probabilistic classifications, and threshold systems, see Appendix I.B–I.D.

[166] EUAA, *Practical Guide on Evidence and Risk Assessment* (n 162) 10, 54–55.

[167] EUAA, *Practical Guide on Evidence and Risk Assessment* (n 162) 20–26.

[168] EUAA, *Practical Guide on Evidence and Risk Assessment* (n 162)16-18.

[169] For further technical discussion of threshold systems and calibration, see Appendix I.C and I.D.

[170] Qualification Directive (n 20) art 4(3).

offs between efficiency, consistency, and individualized treatment.[171] Two applicants presenting similar asylum claims may therefore experience different procedural treatment because one applicant statistically resembles patterns identified in earlier datasets.

The issue becomes more significant where systems rely on proxy variables[172] or historical administrative data. Scholarship on algorithmic discrimination shows that variables such as nationality, language, geographic origin, or mobility history may indirectly function as substitutes for protected characteristics while remaining formally neutral.[173] If earlier administrative practices disproportionately associated certain nationalities, regions, or migration patterns with fraud or security concerns, those assumptions may gradually become reinforced through later classifications.

This creates difficulties for procedural safeguards such as reasoned decision-making and effective judicial review. Fink and Finck argue that automated administrative systems complicate traditional explanation requirements because authorities may rely on outputs generated through technical processes that are difficult to explain in legal terms.[174] An applicant may therefore know that their application was classified as "high risk," inconsistent, or lower priority without understanding how that conclusion was reached or which variables influenced it most strongly.

The increasing use of automated and data-driven systems therefore affects not only administrative efficiency, but also the structure of asylum procedures themselves. The issue is not simply whether algorithmic systems assist authorities, but how statistical classifications may gradually shape credibility assessment, evidentiary evaluation, procedural prioritization, and risk interpretation within refugee status determination.

4.2 Opacity and Transparency Challenges

A separate issue from the structure of decision-making concerns the limited access to the technical systems and processes used in migration governance. Even where asylum authorities and individual case officers rely on system-generated outputs, they may lack access to the information necessary to fully assess how those outputs were generated, including the underlying datasets, algorithmic models, threshold settings, or system parameters shaping the result.[175]

This problem is often described as opacity. In this context, opacity refers to situations where the functioning of a system cannot be fully examined or understood by the people using it or affected by it. A system may produce a classification, alert, or risk score, while the logic behind

[171] Ulrik B.U. Røhl and Morten Balle Hansen, 'Automated Administrative Decision-Making and Good Governance: Synergies, Trade-offs and Limits' (2024).

[172] Proxy variables are variables that indirectly reveal or correlate with protected characteristics, even where those characteristics are not explicitly processed by the system. For example, nationality, language, geographic origin, or travel route may function as indirect indicators of ethnicity, religion, or socio-economic background.

[173] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' (2021) 41 *Computer Law & Security Review* 105567; Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671.

[174] For technical discussion of datasets, threshold systems, and probabilistic classifications, see Appendix I.B–I.D.

[175] Hanne Marie Motzfeldt and Ayo Næsborg-Andersen, 'Developing Administrative Law into Handling the Challenges of Digital Government in Denmark' (2018) 16(2) *Electronic Journal of e-Government* 136.

that result remains inaccessible because of technical complexity, proprietary software protections, security restrictions, or limited access to the underlying data and model design.[176]

This problem does not depend on how decisions are reasoned, but on the conditions under which the systems themselves can be examined. In many cases, the design of these systems, including the models used, the data on which they rely, and the parameters that shape their functioning, is not available to those who use them in practice. Access may be restricted for technical, contractual, or security reasons. As a result, key aspects of the system remain outside the reach of both the administration and the individual concerned.[177]

From an administrative law perspective, this raises a distinct difficulty. Legal control mechanisms, including the duty to give reasons and judicial review, presuppose that the relevant elements of decision-making can be accessed and assessed.[178] However, where the system itself cannot be examined, these mechanisms operate on a limited basis. The authority may rely on a system output, but lack the ability to verify how it was produced or whether it is reliable in the specific case.

This limitation is not only technical, but institutional. As Motzfeldt has shown, digitalization in public administration often involves the distribution of functions across different actors, including private providers, system designers, and public authorities.[179] In such arrangements, no single actor has full visibility over the entire system. This fragmentation of knowledge means that the administration may be legally responsible for the decision, while lacking full insight into the tools it relies on. Furthermore, this also affects individuals. The right to an effective remedy under Article 47 of the Charter requires that individuals are able to challenge decisions affecting them.[180] However, this presupposes access to the elements that influenced the decision. Where the functioning of the system is not accessible, individuals are unable to assess whether the system operated correctly or whether errors occurred in their specific case.

EU data protection law recognizes the importance of access to information in the context of automated processing. Under the GDPR, individuals have the right to obtain information about the existence of automated decision-making and certain aspects of its logic.[181] However, these rights do not guarantee full access to the system itself, and may be limited in practice where information is considered confidential or technically complex. As discussed further in Appendix I.G, explainability mechanisms often provide only partial insight into how outputs were generated, particularly in systems relying on complex statistical models or probabilistic classifications.[182]

[176] Fink and Finck (n 171); Tania Tombal, Pauline Willem and Cécile De Terwangne, 'Legal Framework for the Use of Artificial Intelligence and Automated Decision-Making in Public Governance' in *The New Digital Era Governance* (2022).; Edwards and Veale (n 15) 18–20.

[177] Tania Tombal, Pauline Willem and Cécile De Terwangne, 'Legal Framework for the Use of Artificial Intelligence and Automated Decision-Making in Public Governance' in *The New Digital Era Governance* (2022).

[178] Charter of Fundamental Rights of the European Union arts 41, 47.

[179] Hanne Marie Motzfeldt and Ayo Næsborg-Andersen, 'Digitalisation and the (Unintended) Illegal Outsourcing of Legislative and Administrative Power in Denmark' in Andres Cernadas Ramos and Ramon Bouzas-Lorenzo (eds), *Proceedings of the 18th European Conference on Digital Government ECDG 2018* (1st edn, Academic Conferences and Publishing International 2018) 135–141.

[180] Charter (n 9) art 47; *M.M.* (n 71).

[181] GDPR (n 21) arts 13–15, 22; Article 29 Working Party, *Guidelines on Automated Decision-Making* (n 23).

[182] For further discussion of explainability systems and their limitations, see Appendix I.G.

Opacity must therefore be understood as a problem of limited access rather than simply lack of explanation. It arises from the fact that the systems used in administrative decision-making are not fully open to scrutiny by those who rely on them or are affected by them. This creates a gap between legal requirements of control and the practical ability to examine the tools through which decisions are shaped.

4.3 Contestability and Procedural Rights

The limits of access and visibility described in the previous section have direct consequences for the exercise of procedural rights. Within EU administrative law, these rights are intended to ensure that individuals can actively participate in decision-making processes and challenge decisions that affect them. Their function is not merely formal, but practical: they are meant to provide individuals with the means to question how a decision was reached and to contest its underlying basis.

As already mentioned, a central guarantee in this context is the right to an effective remedy under Article 47 of the Charter, which requires that individuals have access to procedures through which administrative decisions can be reviewed.[183] This right is closely linked to broader principles of good administration under Article 41, including the right to be heard and the obligation of the administration to provide reasons.[184] Together, these guarantees presuppose that individuals have access to the elements that shaped the decision and are able to engage with them in a meaningful way. This becomes difficult to sustain in the context of algorithmic decision-making. As shown in Chapter 2, administrative authorities may rely on system-generated outputs that structure the assessment of a case. However, individuals are typically confronted only with the outcome of these processes, rather than with the information necessary to understand or evaluate them. This creates a situation in which procedural rights formally exist, but their practical effectiveness is reduced.

From a doctrinal perspective, this affects the principle of equality of arms.[185] Administrative procedures are based on the idea that both the individual and the administration can access and challenge the elements relevant to the decision. Where the administration relies on system-based outputs that are not fully accessible, this balance is disrupted. The authority is able to rely on information that the individual cannot fully assess, which limits the ability to contest the decision on equal terms. Moreover, this difficulty is further reinforced at the stage of judicial review. Courts are expected to assess the legality of administrative decisions on the basis of the reasoning provided and the evidence on which it relies. However, where part of that evidence is derived from systems that are not accessible or understandable, the scope of review becomes limited. As Fink and Finck argue, effective review depends on the ability to reconstruct the reasoning process behind a decision, a requirement that is difficult to satisfy where key elements are generated through opaque processes.[186]

Motzfeldt's work on digital administrative law highlights a related issue concerning the distribution of knowledge within administrative systems. Where decision-making relies on complex technical infrastructures, knowledge about how decisions are shaped may be dispersed across

[183] Charter (n 9) art 47.

[184] Charter (n 9) art 41.

[185] Case C-199/11 *European Community v Otis NV* EU:C:2012:684, para 71; *Dombo Beheer BV v Netherlands* (1993) 18 EHRR 213, para 33.

[186] Charter (n 9) art 41.

different actors, including system designers, developers, and public authorities.[187] This fragmentation makes it difficult for both individuals and reviewing bodies to obtain a complete understanding of how a particular outcome was produced. EU data protection law seeks to address some of these challenges by strengthening individual rights in the context of automated decision-making. Under the GDPR, individuals have the right to obtain human intervention, to express their point of view, and to contest decisions that significantly affect them.[188] These safeguards are intended to ensure that individuals are not subject to decisions that they cannot influence. However, their effectiveness depends on the availability of meaningful information about how the decision was reached.

The result is a gap between the formal existence of procedural rights and their practical operation. Individuals may have the right to challenge a decision, but lack the information necessary to do so effectively. Similarly, courts may have the authority to review decisions, but face limits in assessing the elements that influenced the outcome. Contestability is therefore not only a matter of legal entitlement, but of whether the conditions required to exercise that entitlement are present. This tension reveals a broader limitation of existing administrative law frameworks. Procedural rights are designed for decision-making processes in which the relevant elements can be identified, communicated, and contested. Where decision-relevant information is generated through processes that are not fully accessible or understandable, these frameworks are placed under strain. The challenge is therefore not only to preserve procedural rights in formal terms, but to ensure that they remain effective in practice.

4.4 De Facto Automation and Legal Accountability

The issues identified in the preceding sections lead to a distinct problem of legal attribution. Even where procedural guarantees are formally preserved, the question remains whether responsibility can be meaningfully assigned where the authority does not fully control the elements on which the decision is based. EU administrative law is built on the premise that decisions are attributable to public authorities exercising legally conferred powers and that these authorities can be held responsible for both the outcome and the reasoning of the decision. This is reflected in the obligation to provide reasons under Article 296 TFEU, the right to good administration under Article 41 of the Charter, the right to an effective remedy under Article 47, and safeguards concerning automated decision-making under Article 22 GDPR.[189] These provisions presuppose that the authority is able to explain the basis of the decision and account for the elements influencing the outcome.

In contexts where decision-making relies on system-generated inputs, this presupposition becomes difficult to sustain. The authority remains the formal decision-maker, but the basis on which responsibility is attributed no longer fully corresponds to the structure of decision-making in practice. The legal framework continues to operate on the assumption that responsibility follows from authorship of the decision, while in practice the determinants of the outcome may not be fully attributable to the authority itself. Motzfeldt's analysis of digital administrative law is particularly relevant in this respect. She argues that digitalization affects not only how decisions are taken, but how administrative power is exercised and distributed.[190] Rather than

[187] Motzfeldt and Næsborg-Andersen (n 180).

[188] GDPR (n 21) art 22(3).

[189] FEU (n 35) art 296; Charter (n 9) arts 41, 47; GDPR (n 21) art 22(3).

[190] Motzfeldt and Næsborg-Andersen (n 180); Hanne Marie Motzfeldt, 'Developing Administrative Law into Handling the Challenges of Digital Government in Denmark' (2018) *Electronic Journal of e-Government*.

a formal transfer of competence, what emerges is a situation in which decision-relevant functions are performed within technical systems that are not fully integrated into the legal structure of decision-making. This creates a disconnect between the authority that issues the decision and the processes that shape its content.

Recent developments under the EU AI Act attempt to address some of these concerns by classifying AI systems used in migration, asylum, and border management as "high-risk."[191] High-risk systems are subject to requirements concerning transparency, human oversight, data governance, risk management, accuracy, and record-keeping.[192] The AI Act therefore recognizes that these systems may significantly affect fundamental rights and that purely technical regulation is insufficient without procedural safeguards. However, as Stoyanova observes, compliance with the AI Act does not automatically resolve broader human rights concerns, particularly where authorities continue to rely on opaque systems whose operation remains difficult to fully verify or contest in practice.[193]

This disconnect has implications for the doctrine of responsibility. Administrative accountability is traditionally grounded in the idea that the authority has exercised judgment and can therefore be held to account for the decision. Where the authority cannot fully reconstruct or evaluate the elements that influenced the outcome, this model becomes strained. However, where authorities rely on classifications, risk scores, or system-generated outputs that they cannot fully reconstruct or independently verify, responsibility may become largely formal rather than substantive.[194] As Olsen et al. note, computationally aided decision-making may lead to situations in which the authority retains formal responsibility while lacking substantive control over the decision-making process.[195]

From a legal perspective, this raises the question whether formal attribution is sufficient to ensure accountability. The requirement to give reasons presupposes that the authority can explain the basis of the decision in a way that is open to scrutiny. However, where relevant elements originate from processes that are not fully accessible or interpretable, the explanation may remain incomplete. As Fink and Finck argue, explanation requirements in EU law are not designed for decision-making environments in which parts of the reasoning process are external to the authority.[196]

A similar issue arises in relation to judicial review. The effectiveness of review depends on the ability to assess both the reasoning and the elements on which the decision is based. Where those elements cannot be fully examined, review may remain limited to the formal structure of the decision rather than its substantive basis. As discussed further in Appendix I.G, explainability mechanisms may provide only partial insight into probabilistic or machine-learning systems, particularly where outputs depend on complex statistical relationships or opaque model architectures.[197] This weakens the capacity of courts to perform their control function under

[191] Stoyanova (n 60) 5–7.

[192] Regulation (EU) 2024/1689 arts 8–15; Stoyanova (n 60) 6–7.

[193] Stoyanova (n 60) 6–10.

[194] Yeung (n 153) 505–507; Hildebrandt (n 134) 173–176.

[195] Henrik Palmer Olsen, Jacob Livingston Slosser, Thomas Troels Hildebrandt and Cornelius Wiesener, *What's in the Box? The Legal Requirement of Explainability in Computationally Aided Decision-Making in Public Administration* (iCourts Working Paper Series No 162, 2019).

[196] Fink and Finck (n 171).

[197] For further discussion of explainability systems and opacity, see Appendix I.G.

Article 47 of the Charter[198]. EU data protection law introduces additional safeguards through Article 22 GDPR, which requires that decisions are not based solely on automated processing and that individuals can obtain human intervention.[199] Recent CJEU case law such as SCHUFA Holding AG further demonstrates increasing concern within EU law regarding situations where automated scoring systems significantly influence decisions affecting individuals.[200] However, these safeguards do not directly address the question of responsibility in hybrid decision-making structures. The presence of a human decision-maker does not in itself ensure that responsibility corresponds to control, particularly where the role of the authority is constrained by reliance on system-generated elements.

The result is an accountability gap. Responsibility continues to be formally assigned to administrative authorities, but the legal framework does not fully capture the role of the technical processes that contribute to the decision. This gap does not arise from the existence of algorithmic systems as such, but from the persistence of a model of administrative responsibility that assumes unity between decision-making authority, control, and justification. Understanding this gap is essential for assessing the adequacy of existing legal frameworks. Where responsibility is attributed without corresponding control, the capacity of administrative law to ensure accountability is placed under pressure. The challenge is therefore not only to regulate the use of algorithmic systems, but to reconsider how responsibility is structured in contexts where decision-making is distributed across human and technical components.

[198] Charter (n 9) art 47; *M.M.* (n 71); Fink and Finck (n 171).
[199] GDPR (n 21) art 22; Article 29 Working Party, *Guidelines on Automated Decision-Making* (n 23).
[200] SCHUFA Holding AG (n 98).

5 Rethinking Legal Accountability in Algorithmic Migration Governance: outlook

The rapid use of computer algorithms and automated systems in EU migration management has created a major clash with traditional public law. While the EU has created rules for automated systems, data protection, and AI, these tools are still deeply limited when applied to migration and asylum. This chapter looks closely at these conflicts. Section 6.1 examines the gaps in GDPR and the new EU AI Act. Section 6.2 looks at the practical capacities of migration agencies, oversight bodies, and courts, showing how complex technology and human bias toward computers limit independent legal review. Finally, Section 6.3 outlines a better path forward, moving away from simply giving out basic information toward continuous technical checks, active ways for migrants to challenge decisions, and stronger courtroom remedies to protect basic rights.

5.1 The Limits of Existing EU Legal Frameworks

At the center of the current European regulatory framework stands the GDPR, particularly Article 22, which establishes restrictions on decisions based solely on automated processing. However, the practical protective scope of Article 22 remains limited within migration governance. The provision applies only where decisions are "solely" automated and produce legal or similarly significant effects, meaning that many contemporary migration systems may avoid stricter safeguards through the formal presence of human review, even where algorithmic outputs substantially influence administrative reasoning.[201] Wachter, Mittelstadt and Floridi argue that the GDPR does not establish a comprehensive or enforceable "right to explanation," but instead provides relatively limited informational obligations regarding the "logic involved" in automated decision-making.[202] Edwards and Veale similarly observe that explainability alone cannot resolve the broader structural problems generated by complex machine learning systems, particularly where the underlying issue concerns institutional accountability rather than mere informational opacity.[203] Fink and Finck further note that explainability requirements within EU law were developed primarily for traditional administrative reasoning and remain difficult to reconcile with computational systems operating through statistical optimization and opaque inferential processes.[204]

These limitations become especially significant within asylum and migration procedures, where algorithmic systems may influence identity verification, credibility assessment, procedural prioritization, and responsibility allocation. Even where final decisions remain formally attributable to human authorities, computational classifications may shape how cases are interpreted, filtered, or scrutinized throughout the administrative process. This creates tension with EU asylum law, which requires individualized examination and effective procedural safeguards, because algorithmic systems operate through generalized statistical inference rather than contextual legal reasoning.[205] Concerns regarding automation bias further complicate this issue, as decision-makers may attribute disproportionate authority to computational outputs

[201] GDPR (n 21) art 22.
[202] Wachter, Mittelstadt and Floridi (n 96).
[203] Edwards and Veale (n 15).
[204] Fink and Finck (n 171).
[205] Asylum Procedures Directive (n 8) art 10.

even where such outputs remain probabilistic and uncertain.[206] These tensions are particularly visible in biometric identification systems such as Eurodac. Automated Fingerprint Identification Systems (AFIS) compare biometric templates through similarity scoring and threshold calibration rather than exact identification. As discussed in Appendix I.C and Appendix I.D, classifications emerge through statistical probabilities and technical calibration choices. Within asylum procedures, especially Dublin transfer mechanisms, such outputs may nevertheless acquire considerable evidentiary authority despite remaining contingent statistical assessments rather than definitive factual determinations. Jain, Ross and Nandakumar note that biometric systems inherently operate through balancing false positives and false negatives rather than certainty itself.[207]

This creates a significant asymmetry between administrative authorities and affected individuals. The technical processes shaping classification outcomes often remain inaccessible within the legal reasoning visible in the final administrative decision itself. As Pasquale argues, algorithmic governance frequently functions through "black box" structures in which the operational logic influencing decisions cannot easily be scrutinized externally.[208] Within migration governance, this opacity is further reinforced by securitization practices, restricted procedural access, cross-border interoperability systems, and unequal access to technical expertise or legal assistance. Vavoula similarly observes that large-scale EU migration databases increasingly distribute decision-making across interconnected digital infrastructures that remain difficult for individuals to access or challenge effectively.[209] The resulting difficulty is therefore not limited to transparency alone, but concerns the broader capacity of individuals to meaningfully contest classifications and evidentiary outputs generated through systems that remain partially external to ordinary legal scrutiny.

The AI Act represents the European Union's most comprehensive attempt to regulate algorithmic systems through a harmonized legal framework. Importantly, Annex III explicitly classifies several AI systems used in migration, asylum, and border governance as "high-risk," including systems used for biometric identification and categorization, credibility assessment, risk analysis, document verification, and migration-related decision-support.[210] This classification constitutes an important institutional acknowledgment that algorithmic systems used in migration governance may pose serious risks to fundamental rights, including discrimination, procedural unfairness, and exclusion from protection. Unlike the GDPR, which primarily regulates data processing and automated decision-making at the level of individual rights, the AI Act attempts to regulate algorithmic systems at the infrastructural level through ex ante compliance obligations. High-risk systems are therefore subject to requirements concerning risk management, data governance, technical documentation, transparency, human oversight, accuracy, robustness, and post-market monitoring.[211] The Regulation further introduces obligations

[206] Skitka, Mosier and Burdick (n 157)

[207] Jain, Ross and Nandakumar (n 16).

[208] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 8–15.

[209] Vavoula (n 69).

[210] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L, Annex III.

[211] ibid arts 9–15.

regarding quality management systems, logging capabilities, conformity assessments, and ongoing compliance responsibilities for providers and deployers.

However, despite its breadth, the AI Act contains several structural limitations that significantly weaken its protective capacity within migration governance. One major issue concerns the Regulation's continued reliance on technical risk management rather than substantive human rights evaluation. The AI Act largely approaches harm through a product-safety logic focused on identifying, mitigating, and managing "acceptable" risks. Yet migration and asylum procedures involve decisions directly affecting liberty, family life, non-refoulement obligations, and access to international protection. The legal and ethical implications of algorithmic systems within such contexts cannot easily be reduced to technical compliance metrics alone. Brouwer argues that the AI Act ultimately prioritizes harmonization and innovation governance over robust procedural safeguards for migrants and asylum seekers.[212] A further limitation concerns the distinction between systems considered "high-risk" and systems classified as merely auxiliary or preparatory. Under Article 6(3) and Recital 53, systems performing administrative support functions may fall outside stricter obligations where they are deemed insufficiently influential over the final decision.[213] In practice, however, migration governance increasingly operates through interconnected infrastructures in which classification, filtering, prioritization, translation, and credibility support tools may substantially shape procedural outcomes long before a formal legal decision is issued. As discussed in Appendix I.A, algorithmic systems frequently influence decision-making indirectly through categorization and probabilistic inference rather than through fully automated final determinations. Røhl and Hansen similarly note that automated administrative systems frequently shape institutional behavior indirectly even where humans formally retain final authority.[214]

The AI Act also remains heavily dependent on provider-led compliance structures. Many conformity assessments are conducted internally or through procedures relying significantly on documentation produced by providers themselves. This is particularly significant in migration governance, where large-scale infrastructures are frequently developed through procurement arrangements involving private contractors specializing in biometric systems, interoperability architectures, and border surveillance technologies. As outlined in Appendix I.I, corporations such as IDEMIA, Sopra Steria, IBM, Atos, and Leonardo are deeply embedded within the technical architecture of EU migration governance. Their involvement complicates accountability because important technical design choices concerning thresholds, biometric matching, interoperability, and classification infrastructures may remain embedded within proprietary systems that are difficult to access or challenge judicially. Yeung argues that this form of "algorithmic regulation" increasingly redistributes governance authority toward technical infrastructures and private actors operating beyond ordinary democratic visibility.[215] Finally, the AI Act does not fully resolve the deeper tension between probabilistic computation and legal reasoning. Explainability obligations may improve transparency to a limited extent, yet, as discussed in Appendix I.G, explainability mechanisms often provide only statistical approximations of model behavior rather than genuine legal justification. Affected individuals may therefore receive partial information concerning influential variables without gaining meaningful insight into whether the resulting classifications were normatively legitimate, proportionate, or discriminatory. Wachter, Mittelstadt and Russell argue that fairness itself cannot be fully auto-

[212] Brouwer (n 141).
[213] AI Act (n 208) art 6(3), recital 53.
[214] Røhl and Hansen (n 169).
[215] Yeung (n 153).

mated because legal equality ultimately requires normative judgment rather than purely technical optimization.[216] The core difficulty is therefore not merely the absence of information, but the incompatibility between statistical optimization systems and legal frameworks grounded in individualized assessment, reasoned justification, and procedural fairness.

5.2 Institutional Capacity and Oversight

The existence of formal legal safeguards alone does not guarantee meaningful administrative accountability. Even where legal frameworks impose obligations concerning transparency, human oversight, and procedural fairness, the effectiveness of these safeguards depends upon the institutional capacity of authorities, oversight bodies, and courts to evaluate the technology being used. Algorithmic governance introduces forms of technical complexity that may prevent administrative institutions from independently assessing the reliability, legality, and evidentiary significance of automated outputs. Accountability therefore becomes not only a question of legal regulation, but also of institutional competence, technical literacy, and access to the inner workings of technological systems.

One of the central challenges concerns the growing dependence of migration administrations on systems that decision-makers themselves may not fully understand. AI-supported tools are often introduced to improve efficiency, consistency, and case management. However, the increasing integration of machine learning, biometric tracking, and automated profiling may simultaneously weaken the ability of individual case workers to critically assess how outputs are generated. Hildebrandt warns that reliance on computational systems risks producing a form of institutional "deskilling" in which legal actors become unable to independently verify machine-generated findings.[217]In asylum procedures, this concern becomes particularly significant because decisions frequently involve individualized assessments concerning credibility, identity, trauma, and future risk.

The problem is therefore not necessarily the disappearance of human decision-makers, but the increasingly formalistic nature of human oversight itself. Both the GDPR and the AI Act presume the existence of meaningful human review.[218] Yet the effectiveness of such oversight depends upon whether administrative actors possess sufficient technical literacy and institutional authority to critically evaluate algorithmic outputs rather than simply defer to them. As Stoyanova observes, AI-supported decision-making gradually shifts discretion away from frontline asylum officers and toward software designers, programmers, and data selection processes.[219] This creates a structural accountability problem because discretion becomes embedded within technical infrastructures that remain partially inaccessible even to the public authorities deploying them.

Automation bias further intensifies these concerns. Skitka, Mosier and Burdick demonstrate that human decision-makers often attribute excessive authority, neutrality, or objectivity to automated outputs, particularly where systems are presented as statistically advanced or technologically reliable.[220] In migration governance, where institutions frequently operate under po-

[216] Wachter, Mittelstadt and Russell (n 170).
[217] Hildebrandt (n 134).
[218] GDPR (n 21); AI Act (n 208) art 14.
[219] Stoyanova (n 60) 6–7.
[220] Skitka, Mosier and Burdick, (n 157).

litical pressure, large caseloads, and efficiency demands, authorities may become overly dependent on automated classifications or biometric matches despite lacking the expertise necessary to evaluate possible errors or limitations critically. Consequently, the formal existence of human review does not necessarily prevent de facto automation where reviewers lack the practical capacity or confidence to challenge the system's conclusions.

Institutional accountability is further complicated by the fragmented nature of oversight mechanisms governing algorithmic systems in migration management. Oversight responsibilities are distributed across courts, data protection authorities, procurement bodies, border agencies, and private technology providers. Yet no single institution possesses comprehensive authority or technical competence to evaluate the entire lifecycle of AI-supported migration systems, including their design, training data, deployment, and long-term procedural impact. The compliance-based model of the AI Act does not fully resolve this issue because its obligations remain strongly oriented toward technical conformity and risk management prior to deployment.[221] Systems may therefore formally comply with regulatory standards while still producing opaque, discriminatory, or procedurally harmful outcomes in practice. Yeung argues that algorithmic governance increasingly creates forms of "governance by data" in which decision-making processes become embedded within technical systems that are exceptionally difficult for traditional legal institutions to scrutinize effectively.[222]

These challenges are intensified by the growing involvement of private commercial actors in migration governance. Public authorities frequently procure AI systems from external companies or rely on privately developed infrastructures. This creates additional barriers to accountability where proprietary protections, intellectual property claims, or contractual limitations restrict access to the technical information necessary for meaningful review.[223] Stoyanova notes that the development of AI systems in asylum governance involves substantial discretion regarding data selection, coding practices, and model training, yet these design choices often remain invisible both to affected individuals and to the authorities deploying the systems themselves.[224] Judicial oversight presents an additional layer of difficulty because courts traditionally review administrative reasoning through evidence, procedural guarantees, and legal justification. Algorithmic systems complicate this model where relevant reasoning processes are embedded within statistical calculations or machine learning architectures that are difficult to reconstruct or interpret. Judges may therefore face significant informational barriers when reviewing decisions influenced by AI-supported systems, particularly where probabilistic outputs or predictive classifications become influential in evidentiary assessment.[225]

The opacity of algorithmic systems also risks undermining access to effective remedies under Article 47 of the Charter and Article 13 ECHR.[226] Effective judicial protection requires that individuals possess sufficient information to understand and contest decisions affecting them. Yet where relevant reasoning processes remain embedded within statistical models, proprietary systems, or inaccessible computational architectures, judicial review risks becoming limited to procedural formalities rather than substantive evaluation of how conclusions were reached. Courts may therefore verify compliance with procedural requirements without being able to

[221] AI Act (n 208) arts 9, 16–27, 43 and 72.
[222] Yeung (n 153).
[223] Byrne and others (n 73).
[224] Stoyanova (n 60).
[225] Gammeltoft-Hansen and Byrne (n 68); Rinaldi and Teo (n 69).
[226] Charter (n 9) art 47; European Convention on Human Rights, art 13.

meaningfully assess the technical logic influencing the outcome itself. This concern is particularly significant in asylum procedures, where erroneous classifications or evidentiary assessments may expose individuals to refoulement, detention, or exclusion from international protection. Without significant institutional adaptation, formal safeguards risk becoming largely symbolic while substantive discretion increasingly shifts toward opaque technological systems operating beyond meaningful democratic and judicial scrutiny.

5.3 Toward Algorithmic Accountability in Migration Governance

The analysis developed throughout this thesis demonstrates that existing legal safeguards face increasing pressure in contexts where migration governance relies on interoperable databases, probabilistic classifications, and AI-supported administrative systems. The issue is not simply the use of digital technologies within asylum procedures, but the growing dependence of migration governance on technical infrastructures that shape how information is categorized, interpreted, and operationalized within administrative processes. As discussed throughout Chapter 4, this creates important tensions for procedural fairness, contestability, and effective judicial protection where relevant elements influencing the decision may remain partially inaccessible to affected individuals and reviewing authorities alike.[227]

The AI Act represents an important institutional acknowledgment that AI systems used in migration, asylum, and border governance may generate significant risks for fundamental rights.[228] High-risk systems are subject to obligations concerning risk management, technical documentation, transparency, human oversight, and post-market monitoring.[229] However, the findings of this thesis suggest that many accountability concerns extend beyond technical compliance alone. Formal safeguards do not necessarily resolve the broader institutional difficulties created where decision-making processes become increasingly dependent upon technical systems that public authorities themselves may not fully understand or independently evaluate in practice. As discussed further in Appendix I.G and Appendix I.H, explainability and fairness mechanisms often remain limited when applied to complex probabilistic systems operating through statistical optimization and competing calibration choices.

This creates challenges not only for individuals seeking to contest decisions, but also for administrative authorities and courts responsible for oversight. Existing procedural guarantees under Article 47 of the Charter, Article 13 ECHR, and Article 22 GDPR presuppose that relevant elements influencing the decision can be identified, communicated, and reviewed.[230] Yet algorithmic systems increasingly distribute decision-relevant processes across technical infrastructures, interoperability systems, external providers, and computational models that remain difficult to fully reconstruct within ordinary legal proceedings. As Motzfeldt argues, digital administration may therefore create situations in which responsibility formally remains with public authorities while substantive control over decision-shaping processes becomes fragmented across multiple technical and institutional actors.[231]

[227] Fink and Finck (n 171); Motzfeldt (n 172).
[228] AI Act (n 208) Annex III para 7.
[229] Ibid. arts 9, 11–15.
[230] Charter (n 9) art 47; ECHR, art 13; GDPR (n 21) art 22.
[231] Motzfeldt (n 172).

The findings of this thesis therefore suggest that accountability within algorithmic migration governance cannot be reduced to transparency obligations or the formal presence of human review alone. Meaningful accountability requires institutional structures capable of critically assessing the evidentiary role, procedural influence, and distributive effects of technological systems operating within migration administration. This may require stronger auditing mechanisms, greater technical expertise within courts and administrative bodies, improved access to system documentation, and procedural safeguards ensuring that affected individuals can effectively challenge system-generated classifications and assessments. Ultimately, the challenge posed by algorithmic migration governance is not solely technological, but structural, as it concerns the capacity of existing legal frameworks to preserve procedural fairness, responsibility, and meaningful oversight within increasingly data-driven systems of administrative decision-making.

6 Conclusion

This thesis examined how algorithmic and data-driven systems interact with existing European legal frameworks governing migration and asylum decision-making. It argued that the central challenge posed by algorithmic migration governance is not simply the use of new technologies within administrative procedures, but the growing difficulty of preserving meaningful legal accountability once decision-making becomes increasingly mediated through digital infrastructures, probabilistic systems, and interoperable databases.

The analysis demonstrated that EU migration law, human rights law, and data protection law already contain important procedural safeguards, including individualized assessment, reason-giving, non-discrimination, meaningful human oversight, and effective judicial protection. However, the thesis showed that these safeguards were largely developed for administrative systems in which factual assessment and legal reasoning remained visible, identifiable, and open to scrutiny. Algorithmic systems complicate this structure by introducing computational processes that may significantly influence evidentiary assessment, identity verification, procedural prioritization, and risk evaluation while remaining only partially accessible within legal proceedings.

A central finding of the thesis concerns the increasing role of probabilistic and data-driven forms of evaluation within migration governance. Biometric matching systems, interoperability infrastructures, and classification mechanisms do not operate through certainty, but through similarity scoring, threshold calibration, and statistical correlation. Yet once translated into administrative categories such as “match,” “risk indicator,” or “inconsistency,” these outputs may acquire substantial evidentiary authority within legal procedures. The thesis therefore demonstrated that the challenge is not simply automation itself, but the gradual shift from visible legal reasoning toward forms of infrastructural and computational authority that remain difficult to reconstruct, contest, or independently evaluate.

The research further showed that existing regulatory developments, including the GDPR and the AI Act, only partially resolve these accountability concerns. While the AI Act introduces important safeguards for high-risk migration systems, including obligations concerning transparency, human oversight, technical documentation, and risk management, the framework remains primarily focused on technical compliance and pre-deployment governance. Many of the broader accountability problems identified throughout this thesis concern the institutional and procedural consequences of algorithmic administration itself, particularly where responsibility becomes distributed across public authorities, interoperable infrastructures, and private technological contractors involved in system design and operation.

The thesis also highlighted the importance of interdisciplinary engagement when examining algorithmic migration governance. Legal analysis alone cannot fully explain how computational systems influence migration decision-making in practice, while purely technical approaches often fail to engage with procedural safeguards, human rights obligations, and administrative accountability. For this reason, the thesis combined doctrinal legal analysis with technical illustration and simplified systems modelling in order to examine how algorithmic outputs are generated and operationalized within migration governance structures. The appendices were included to support this interdisciplinary approach. Appendix I provided technical explanations relating to biometric matching, probabilistic classification, threshold calibration, explainability, and fairness metrics, while Appendix II examined the role of private technological

contractors and outsourced infrastructures involved in EU migration systems. Together, these appendices were intended to clarify the technical and institutional processes that remain partially external to ordinary legal reasoning but nevertheless shape migration governance in practice.

Several limitations should nevertheless be acknowledged. The thesis relied primarily on doctrinal legal analysis and desk-based technical illustration rather than empirical fieldwork or access to operational systems. The technical examples used throughout the analysis were simplified explanatory models intended to clarify how algorithmic systems function conceptually, rather than attempts to replicate operational EU infrastructures. In addition, the thesis focused on the European legal framework and did not examine differences in implementation between individual Member States or comparative non-European approaches.

Nevertheless, the findings of this thesis suggest that algorithmic migration governance raises broader rule-of-law questions extending beyond technological regulation alone. As migration administration becomes increasingly dependent upon data-driven infrastructures, maintaining meaningful accountability will require legal frameworks capable of addressing not only individual administrative decisions, but also the technical systems, institutional arrangements, and outsourced infrastructures through which those decisions are increasingly shaped.

7 Use of Artificial Intelligence Tools

Artificial intelligence tools were used in a limited and supportive capacity during the preparation of this thesis. Their use was restricted primarily to language support, translation assistance, formatting, and reference management.

All substantive legal analysis, interpretation, argumentation, structure, and conclusions were independently developed, reviewed, and verified by the author. Responsibility for the final content, accuracy of sources, legal reasoning, and academic integrity remains entirely with the author.

Appendix I: Technical Illustrations of Algorithmic Decision Processes

Appendix I.A Modeling Algorithmic Decision Systems

Article 3(1) of the Artificial Intelligence Act defines an AI system as:

"a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."[232]

Within migration governance, many algorithmic systems rely on machine learning techniques to process data, identify statistical patterns, and generate classifications or predictions. Machine learning is generally understood as a subfield of artificial intelligence concerned with the development of computational models capable of learning relationships from datasets rather than relying exclusively on explicitly hard-coded instructions.[233] Rather than operating through predetermined legal reasoning or fixed logical rules, machine learning systems infer relationships from statistical regularities identified within training data and subsequently apply those learned patterns to new cases.

Bellazi defines machine learning as the development of algorithms capable of making predictions or decisions based on patterns identified in data, allowing systems to improve performance through exposure to datasets rather than through direct rule-based programming. In this sense, machine learning systems differ fundamentally from traditional deterministic software systems. Conventional software operates through explicitly programmed instructions in which every possible operation is predefined by human programmers. By contrast, machine learning systems generate predictive outputs through computational training processes that adjust internal parameters according to the statistical structure of the data used during training.[234]

From a technical perspective, machine learning systems commonly operate through a computational pipeline composed of several interconnected stages:

- data collection,
- preprocessing,
- feature extraction,
- model training,
- prediction,
- evaluation.

Bellazi describes this process as a machine learning pipeline in which raw data is progressively transformed into structured representations suitable for computational analysis.[235] The initial

[232] AI Act (n 208) art 3(1).

[233] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2021) 19–28.

[234] Khalifa Bellazi, *Machine Learning-Based Solution For Automatic Border Surveillance System* (Doctoral Thesis, Universidad Politécnica de Madrid 2024) 9.

[235] ibid 11

stages of the pipeline involve collecting and organizing datasets capable of being processed computationally. During preprocessing, data may be cleaned, normalized, encoded, or transformed into machine-readable formats. Feature extraction subsequently converts raw information into structured variables capable of statistical processing, while model training involves optimizing the system's internal parameters to reduce predictive error across the training dataset.[236]

Algorithmic systems used in migration governance can therefore be understood as structured classification systems that transform input data into decision-relevant outputs through statistical and computational processes. Unlike legal reasoning, which relies on interpretation, contextual assessment, and justification, algorithmic systems operate through pattern recognition, classification, optimization, and probabilistic inference.[237] Their objective is not to interpret legal meaning in a normative sense, but to identify statistical correlations capable of generating predictive outputs.

At a technical level, many such systems function through statistical classification models that assign cases to predefined categories based on selected input variables. In simplified form, this process can be represented as:

$y=f(x1,x2,...,xn)$

where:

- $x1,x2,...,xn$ represent features of the case,
- y represents the resulting classification.

The objective of the model is to estimate the probability that a given input belongs to a particular category:

$P(y|x)$

In practice, these systems rarely generate certainty. Instead, they generate probabilistic outputs derived from statistical relationships identified within training datasets. These outputs are subsequently converted into categorical outcomes through threshold settings. For example:

$P(y)\geq 0.5 \rightarrow$ "high risk"

The resulting classification therefore depends not only on the underlying data, but also on technical design choices including:

- feature selection,
- weighting mechanisms,
- threshold calibration,
- model architecture,
- optimization procedures,
- training data composition.

[236] ibid 11–12.
[237] ibid 9–10.

These technical design choices shape how the system interprets information internally and determine which variables exert the greatest influence over predictive outputs.[238] Consequently, algorithmic systems do not produce neutral or objective determinations independent of human intervention. Rather, their outputs emerge from layered technical choices embedded within the structure of the model itself, including decisions concerning data selection, feature representation, model optimization, and classification thresholds.

From a legal perspective, this creates a significant tension between computational reasoning and individualized legal assessment. EU migration and asylum law requires decisions to be based on individualized examination, reasoned justification, and procedural safeguards.[239] Machine learning systems, however, operate by generalizing across datasets and applying probabilistic inference derived from prior statistical patterns. The resulting outputs therefore reflect computational inference rather than individualized legal reasoning, raising important questions concerning transparency, contestability, accountability, and compatibility with procedural fairness guarantees.[240]

Appendix I.B Feature Selection and Feature Vectors

Algorithmic systems cannot process human narratives, legal testimony, or contextual experiences directly. Before information can be analyzed computationally, it must first be transformed into structured numerical representations capable of machine processing. This process is commonly described as feature engineering.[241]

In machine learning systems, information is represented through feature vectors:

$x=(x1,x2,...,xn)$

where each variable corresponds to a selected attribute of the case. These variables function as measurable representations of characteristics considered relevant to the predictive task performed by the system.

Within migration governance, features may include:

- nationality,
- travel route,
- prior asylum applications,
- biometric matches,
- visa history,
- geolocation metadata,
- language indicators,
- device identifiers,
- social media activity,
- document verification results.

[238] Ibid.
[239] Asylum Procedures Directive (n 8) art 10.
[240] Edwards and Veale (n 15) 24–29.
[241] Bellazi, (n 234)11–13.

These features are subsequently transformed into machine-readable formats through preprocessing procedures such as:

- normalization,
- categorical encoding,
- vectorization,
- scaling,
- dimensionality reduction.

For example, categorical variables such as nationality may be converted into numerical representations capable of computational processing, while biometric information may be transformed into mathematical templates or similarity scores.[242] This transformation process enables the model to compare, classify, and rank individuals according to statistically learned patterns.

Feature engineering is not a neutral or purely technical exercise. The selection, construction, and weighting of variables fundamentally shape how the system internally represents the individual case. Complex personal experiences, including displacement histories, trauma narratives, or contextual vulnerability factors, are reduced into simplified computational categories capable of statistical manipulation.[243]

From a technical perspective, the quality and structure of features directly influence model performance. Machine learning systems rely heavily on feature selection because the predictive accuracy of the model depends on identifying variables that correlate with the target outcome.[244] Variables considered statistically informative are therefore prioritized during training, regardless of whether those variables are normatively or legally appropriate.

This creates a significant risk within migration governance systems. Variables such as nationality, travel route, language, or geographic origin may function as indirect proxy variables for protected characteristics including ethnicity, religion, or political affiliation. Even where explicitly protected categories are formally excluded from the system, correlated variables may reproduce substantially similar outcomes through statistical association.

Technically, this occurs because machine learning systems optimize predictive performance rather than legal legitimacy. During training, the model identifies variables that reduce prediction error across the dataset. If certain variables consistently correlate with previous administrative outcomes, the system may assign them significant predictive weight even where those variables reflect structural bias or discriminatory historical practices.[245]

The construction of feature vectors therefore shapes not only computational performance, but also the distribution of legal risk within the system itself. Different feature configurations may produce substantially different outputs, meaning that the design of the data representation layer can directly influence classification outcomes.[246]

[242] Ibid.
[243] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019) 220–245.
[244] Bellazi (n 234) 11–15.
[245] Barocas and Selbst (n 170) 691–705.
[246] Pasquale (n 206) 8–15.

From a legal perspective, this raises important concerns regarding equality, individualized assessment, and non-discrimination. EU migration and asylum procedures require decisions to be based on individual circumstances rather than generalized assumptions associated with group membership.[247] However, machine learning systems necessarily operate through abstraction and statistical generalization, creating a structural tension between computational efficiency and individualized legal reasoning.

Appendix I.C Threshold-Based Risk Classification

Many machine learning systems used in administrative and migration governance operate through weighted classification models designed to estimate the probability that a case belongs to a predefined category. Rather than producing conclusions through legal interpretation or contextual reasoning, these systems generate outputs through statistical calculations based on relationships identified within training data.[248]

At a simplified level, risk scoring systems can be represented as weighted classification functions:

$$score = w_1x_1 + w_2x_2 + w_3x_3$$

where:

- x_n represents input variables or features,
- w_n represents the weights assigned to each feature by the model.

The assigned weights reflect the relative statistical importance attributed to each variable during the training process. Variables that appear strongly correlated with a target outcome within the training dataset may receive greater predictive weight than variables considered less statistically informative.[249]

The resulting score is subsequently converted into a categorical classification through threshold settings:

$$\text{if } score \geq t \rightarrow \text{“high risk”} \quad \text{else} \rightarrow \text{“low risk”}$$

This threshold-based structure is characteristic of many statistical classification systems. Rather than producing certainty, the model estimates probabilities or confidence values, which are then translated into binary or categorical outputs through predefined decision boundaries.[250]

In practice, this process involves two distinct stages:

- training,
- inference.

[247] Asylum Procedures Directive (n 8) art 10.
[248] Bellazi (n234), 9-15.
[249] Ibid.
[250] Bishop (n 163) 179–186.

During training, the system analyzes historical datasets in order to identify statistical patterns associated with previous outcomes. The model adjusts its internal parameters through optimization procedures intended to minimize predictive error across the training data.[251] This process can be expressed through the minimization of a loss function:

$$L(f(x),y)$$

where:

- f(x) represents the model prediction,
- y represents the known label or outcome.

Optimization techniques such as gradient descent or probabilistic optimization methods iteratively adjust model parameters in order to reduce the difference between predicted and actual outcomes.[252]

Once trained, the system enters the inference stage, during which new data is processed through the learned model to generate predictions for previously unseen cases. In migration governance contexts, this may involve the classification of individuals into categories associated with:

- security risk,
- credibility,
- identity verification,
- procedural prioritization,
- anomaly detection.

A simplified computational illustration may be expressed as follows:

```
def risk_score(nationality, travel_route, previous_application):
    score = (
        0.5 * nationality +
        0.3 * travel_route +
        0.2 * previous_application
    )
    return score

def classify(score, threshold=0.5):
    if score >= threshold:
        return "high risk"
    return "low risk"
```

This simplified example demonstrates how multiple variables may be combined into a weighted numerical score and subsequently transformed into a categorical classification through threshold settings. The example is illustrative only and does not reflect any operational system.

Importantly, the resulting classification depends not only on the input data itself, but also on technical design decisions embedded within the model architecture. Adjustments to feature

[251] Bellazi (n 234) 11-15.
[252] Goodfellow, Bengio and Courville (n 163) 96–110.

weights, threshold settings, optimization strategies, or training data composition may substantially alter the resulting classification despite identical underlying facts.[253]

A relatively minor threshold adjustment may therefore transform the same individual case from "low risk" to "high risk" without any change in the underlying data. This reflects the broader statistical trade-off between false positives and false negatives commonly identified within machine learning and biometric matching systems.[254] Lower thresholds generally increase system sensitivity while also increasing the likelihood of false positives, whereas higher thresholds may reduce false positives while increasing false negatives.

This probabilistic structure creates significant implications for migration governance. Machine learning systems optimize predictive performance according to statistical criteria rather than normative legal standards.[255] As a result, classifications emerge through mathematical optimization processes rather than individualized legal reasoning. The apparent objectivity of numerical outputs may therefore obscure the discretionary technical choices embedded within the system itself, including the selection of variables, calibration of thresholds, and weighting of predictive factors.

From a legal perspective, this creates a structural tension between computational classification and procedural fairness guarantees. EU asylum and migration law requires decisions to be individually assessed, reasoned, and contestable.[256] However, threshold-based machine learning systems operate by reducing complex personal circumstances into probabilistic calculations and statistical categories. The resulting decision-making logic may therefore be difficult for individuals to understand, challenge, or meaningfully contest, particularly where the underlying computational reasoning remains opaque.[257]

Appendix I.D Threshold Variability and Output Sensitivity

One of the defining characteristics of machine learning classification systems is their sensitivity to threshold calibration. Because many algorithmic systems generate probabilistic rather than deterministic outputs, the final classification depends on the threshold selected to convert probability scores into categorical decisions.[258] Small modifications to these threshold settings may therefore produce substantially different outcomes despite identical underlying data.

This can be illustrated through a simplified example:

```
decision_1 = classify(score, threshold=0.5)
decision_2 = classify(score, threshold=0.6)
```

[253] Pasquale (n 206) 8–15.
[254] NIST Special Database 24 (n 6).
[255] Barocas and Selbst (n 170) 691–705.
[256] Asylum Procedures Directive (n 8) art 10.
[257] Edwards and Veale (n 15) 24–29.
[258] Bishop (n 163) 179–186.

In this example, the same input data is processed through the same model, yet the final classification changes solely because the threshold value has been modified. The underlying information concerning the individual case remains identical, but the technical calibration of the system alters the resulting output.

From a technical perspective, thresholds function as decision boundaries separating categories within the classification model.[259] The model itself produces a probability estimate or confidence score indicating the likelihood that a case belongs to a particular category. The threshold determines the point at which this probability becomes sufficient to trigger a specific classification outcome.

For example: $P(y|x)=0.55$

If the threshold is set at: $t=0.50$

the case may be classified as: “high risk”

However, if the threshold is increased to: $t=0.60$

the identical probability score would instead produce: “low risk”

The resulting classification therefore depends not only on the statistical output generated by the model, but also on the policy and technical decisions embedded within threshold calibration itself.[260]

Threshold selection is closely connected to the broader statistical trade-off between false positives and false negatives commonly identified in machine learning and biometric matching systems. A false positive occurs when the system incorrectly classifies a case as belonging to a target category, while a false negative occurs when the system fails to identify a case that should have been classified within that category.

This relationship can be represented through a confusion matrix structure:

	Predicted Positive	**Predicted Negative**
Actual Positive	True Positive	False Negative
Actual Negative	False Positive	True Negative

Lower threshold settings generally increase system sensitivity by identifying a greater number of potential matches or risks. However, this often increases the likelihood of false positives. Conversely, higher threshold settings may reduce false positives while increasing the number of false negatives.[261] Threshold calibration therefore reflects a balancing exercise between different forms of statistical error rather than a process capable of producing certainty.

This dynamic is particularly visible within biometric identification systems. Fingerprint and facial recognition systems operate by generating similarity scores rather than exact matches.

[259] Ibid.
[260] Pasquale (n 206) 8–15.
[261] Bellazi (n 234) 15-16.

The system compares biometric templates and calculates the statistical likelihood that two samples correspond to the same individual.[262] Whether the result is treated as a "match" depends on the similarity threshold configured within the system.

Empirical studies demonstrate that different threshold settings may substantially alter system performance. The National Institute of Standards and Technology (NIST), for example, has shown that fingerprint matching systems produce varying true accept and false accept rates depending on the threshold selected and the quality of the biometric sample.[263] A "match" therefore reflects a probabilistic classification based on calibrated trade-offs rather than definitive identification.

From a technical standpoint, threshold variability demonstrates that machine learning outputs are not fixed objective truths, but contingent statistical determinations shaped by calibration choices. The apparent precision of numerical outputs may obscure the discretionary decisions involved in determining where decision boundaries are placed.

This has significant implications within migration governance systems. Threshold settings may directly influence:

- risk classifications,
- biometric matching outcomes,
- fraud detection,
- credibility scoring,
- anomaly detection,
- procedural prioritization.

Even relatively minor technical adjustments may therefore alter whether an individual is flagged for additional scrutiny, subjected to enhanced security procedures, or categorized as presenting elevated risk.[264]

From a legal perspective, threshold variability creates tension with principles of legal certainty, transparency, and individualized assessment. EU migration and asylum law requires decisions affecting individuals to be reasoned, contestable, and based on individualized examination.[265] However, threshold-based systems produce outcomes through probabilistic calibration mechanisms that may remain invisible to the affected individual. The resulting classification may therefore appear authoritative despite depending on technical parameters that are adjustable, contestable, and ultimately contingent rather than legally determinate.[266]

Appendix I.E Proxy Variables and Indirect Discrimination

One of the central concerns surrounding algorithmic decision-making systems is the manner in which discriminatory outcomes may emerge through the use of proxy variables. Machine learning systems frequently rely on variables that are not themselves protected characteristics, but which correlate strongly with them statistically. These variables are commonly described as

[262] Bellazi (n 234) 9-15.
[263] NIST Special Database 24 (n 6).
[264] Barocas and Selbst (n 170) 691–705.
[265] Asylum Procedures Directive (n 8) art 10.
[266] Edwards and Veale (n 15) 24–29.

proxy variables because they indirectly reproduce information associated with protected categories such as ethnicity, religion, nationality, gender, or political affiliation.

From a technical perspective, proxy discrimination emerges because machine learning systems optimize predictive accuracy rather than legal or normative legitimacy. During training, the model identifies variables that reduce prediction error across the dataset. Where certain variables correlate strongly with historical outcomes, the model may assign them substantial predictive weight regardless of whether those correlations reflect structural discrimination or legally problematic assumptions.[267]

This relationship may be expressed in simplified probabilistic form as:

$P(y|xi) \approx P(y|z)$

where:

- xi = proxy variable,
- z = protected characteristic.

The formula illustrates that the predictive relationship generated by the proxy variable approximates the predictive relationship associated with the protected characteristic itself. In practical terms, the system may therefore reproduce discriminatory effects even where explicitly protected categories have been formally excluded from the model.[268]

Within migration governance, variables such as:

- nationality,
- travel route,
- language,
- geographic origin,
- document type,
- device metadata,
- biometric similarity patterns,

may function as indirect proxies for broader categories associated with ethnicity, religion, socio-economic status, or geopolitical identity.[269]

For example, a model may not explicitly process "ethnicity" as an input variable while simultaneously relying heavily on nationality or region of origin, both of which may correlate strongly with ethnic or religious identity. Similarly, travel routes may correlate with geopolitical instability, refugee-producing regions, or racialized migration patterns, thereby functioning as indirect indicators of protected characteristics.

A simplified computational illustration may be expressed as follows:

[267] Barocas and Selbst (n 170) 691–705.
[268] Wachter, Mittelstadt and Russell (n 170) 5–8.
[269] Bellazi (n 234) 11-15

```
def risk_score(nationality, travel_route):
    return 0.7 * nationality + 0.3 * travel_route
```

In this simplified example, the variable "nationality" receives greater predictive weight within the classification model. The resulting output is therefore disproportionately shaped by nationality-based correlations identified during training. The example is illustrative only and does not reflect any operational system.

Importantly, the discriminatory risk does not arise solely because a variable exists within the model, but because of the statistical relationships generated between variables and outcomes during training. Machine learning systems do not distinguish between legally legitimate and illegitimate correlations.[270] Any variable capable of improving predictive accuracy may become statistically significant regardless of whether its use produces discriminatory effects.

This dynamic is reinforced by the structure of historical datasets. Administrative and migration datasets are often shaped by pre-existing institutional practices, discretionary enforcement patterns, and unequal social conditions.[271] If historical decisions disproportionately targeted or scrutinized particular nationalities, ethnic groups, or migration routes, the resulting dataset may encode those patterns into the training process itself.

As a result, algorithmic systems risk reproducing forms of indirect discrimination embedded within prior administrative behavior. This phenomenon is often described through the principle of "bias in, bias out," meaning that biased historical data may generate biased predictive outputs even where the computational process itself appears formally neutral.[272]

From a technical standpoint, proxy discrimination is particularly difficult to identify because it frequently emerges through combinations of variables rather than through a single explicit feature. In high-dimensional machine learning systems, multiple variables may interact simultaneously to reproduce protected characteristics indirectly.[273] This complexity makes discriminatory effects difficult to detect through ordinary human review alone.

The issue becomes even more significant within migration governance because asylum and border systems frequently operate under conditions of evidentiary uncertainty and asymmetric power relations between individuals and administrative authorities.[274] Variables associated with nationality, mobility patterns, language use, or document history may therefore become disproportionately influential within predictive systems despite their limited legal relevance to individualized protection claims.

From a legal perspective, proxy discrimination creates significant tension with principles of equality and non-discrimination under European human rights and asylum law. EU legal frame-

[270] Barocas and Selbst (n 170) 691–705.
[271] Virginia Eubanks, *Automating Inequality* (St Martin's Press 2018) 126–154.
[272] Cathy O'Neil, *Weapons of Math Destruction* (Penguin Books 2016) 17–31.
[273] Pasquale (n 206) 8–15.
[274] Didier Fassin, *Policing Borders, Producing Boundaries* (Duke University Press 2011) 213–230.

works require individualized assessment and prohibit discriminatory treatment based on protected characteristics.[275] However, machine learning systems may generate discriminatory effects indirectly through statistically correlated variables while appearing formally neutral at the surface level.

This creates a structural challenge for accountability and contestability. Because discriminatory outcomes emerge through statistical correlations embedded within model architecture and training data, affected individuals may face significant difficulties identifying, understanding, or challenging the discriminatory logic influencing the decision-making process.[276] The resulting opacity complicates both procedural fairness and effective judicial review.

Appendix I.F Bias in Training Data

Machine learning systems are typically trained using historical datasets composed of paired inputs and outputs:

$D=\{(x1,y1),(x2,y2),...,(xn,yn)\}$

where:

- x_n represents the input features associated with a case,
- y_n represents the recorded outcome or classification linked to those features.

Within supervised learning systems, the dataset functions as the primary source through which the model learns predictive relationships. The model analyzes repeated associations between variables and outcomes in order to identify statistical regularities capable of being generalized to future cases.[277]

Importantly, machine learning systems do not independently evaluate whether historical outcomes were legally justified, proportionate, or procedurally fair. The system processes historical decisions as training signals rather than normative judgments.[278] Consequently, patterns embedded within previous administrative practices may become statistically reinforced during model training.

A simplified illustration may be represented as follows:

```
data = [
   {"nationality": 1, "decision": 1},
   {"nationality": 1, "decision": 1},
   {"nationality": 0, "decision": 0}
]
```

In this simplified example, the system repeatedly observes a correlation between a particular variable and a specific administrative outcome. During training, the model may therefore learn

[275] Charter (n 9) art 21.
[276] Edwards and Veale (n 15) 24–29.
[277] Bishop (n 163) 179–186.
[278] O'Neil (n 272) 17–31.

to associate that variable with a greater probability of producing the same classification in future cases. The example is illustrative only and does not reflect any operational system.

From a technical perspective, this occurs because supervised learning models optimize prediction by identifying recurring statistical relationships within the dataset.[279] Variables consistently associated with prior outcomes acquire predictive significance regardless of whether those relationships emerged from lawful decision-making, discretionary administrative behavior, institutional practices, or broader structural inequalities.

Bias may therefore emerge through several mechanisms within the dataset itself, including:

- imbalanced class distributions,
- incomplete data representation,
- inconsistent labeling,
- historical overrepresentation of particular groups,
- sampling bias,
- measurement bias,
- administrative feedback loops.

Imbalanced datasets are particularly significant within migration governance systems. If particular nationalities, migration routes, or demographic groups appear disproportionately within specific administrative categories, the model may internalize these distributions as predictive indicators rather than contingent historical outcomes.[280]

A further difficulty arises from the fact that historical migration and asylum datasets are frequently generated within institutional environments characterized by evidentiary uncertainty, discretionary credibility assessments, and unequal power relations between applicants and authorities.[281] The resulting datasets may therefore reflect broader administrative assumptions, enforcement priorities, or geopolitical patterns rather than objective indicators of risk or credibility.

From a computational standpoint, the model cannot distinguish between:

- statistically recurring patterns,
- legally legitimate reasoning,
- historically contingent administrative behavior.

Any recurring correlation capable of improving predictive accuracy may become embedded within the learned model architecture.[282] This creates the possibility that machine learning systems reproduce forms of structural inequality without explicit discriminatory intent being programmed into the system itself.

The problem may also intensify over time through feedback loops. Where algorithmic systems influence future administrative decisions, the outputs generated by the model may themselves

[279] Goodfellow, Bengio and Courville (n 163) 96–110.
[280] Barocas and Selbst (n 170) 691–705.
[281] Fassin (n 274) 213–230.
[282] Pasquale (n 206) 8–15.

become incorporated into subsequent training datasets.[283] This can reinforce existing statistical patterns and progressively stabilize particular classifications or assumptions within the system.

In migration governance contexts, these dynamics may affect:

- risk scoring systems,
- biometric matching systems,
- fraud detection tools,
- credibility assessments,
- predictive border surveillance systems,
- automated prioritization mechanisms.

Because these systems derive predictive logic from prior data, their outputs remain heavily dependent on the quality, representativeness, and historical structure of the training dataset itself.[284]

From a legal perspective, the reliance on historically generated datasets raises important concerns regarding equality, procedural fairness, and individualized assessment. EU asylum and migration law requires decisions to be based on the individual circumstances of the applicant rather than generalized statistical assumptions.[285] However, supervised machine learning systems necessarily operate by identifying and generalizing patterns across populations. The resulting tension reflects a broader structural conflict between probabilistic governance and individualized legal reasoning.

Appendix I.G Explainability and Technical Transparency

The increasing use of machine learning systems within migration governance has generated significant attention toward explainability and technical transparency as potential mechanisms for accountability. Explainability mechanisms aim to approximate how variables influence algorithmic outputs through feature attribution methods, local explanation techniques, and model interpretation tools. These techniques are intended to make complex statistical systems more understandable by providing information concerning how particular variables contributed to a predictive outcome.

From a technical perspective, explainability methods operate by estimating the relative influence of different features within a model. Common approaches include:

- feature importance scoring,
- local interpretable model approximations,
- saliency mapping,
- decision tree approximations,
- sensitivity analysis.

[283] Eubanks (n 271) 126–154.
[284] Bellazi (n 234) 11-15.
[285] Asylum Procedures Directive (n 8) art 10.

These methods attempt to identify which variables exerted the greatest influence over a particular classification or prediction.[286] For example, an explainability tool may indicate that nationality, travel route, or biometric similarity contributed significantly to a risk score generated by the system.

However, explainability tools do not reconstruct the internal reasoning process of the model in a fully transparent manner. Instead, they generate statistical approximations of model behavior derived from observable correlations between inputs and outputs.[287] In many cases, explainability mechanisms function as secondary interpretive layers applied externally to complex machine learning architectures rather than direct representations of the model's internal computational logic.

This creates an important distinction between:

- computational explanation,
- legal justification.

Computational explanation concerns the statistical contribution of variables to a predictive outcome. Legal justification, by contrast, concerns whether the resulting decision complies with normative legal standards including proportionality, equality, procedural fairness, and individualized assessment.[288]

A system may therefore identify which variable influenced a classification without determining whether reliance on that variable is legally legitimate. For example, an explainability mechanism may reveal that nationality exerted substantial influence over a predictive outcome, yet the system itself cannot evaluate whether such reliance constitutes indirect discrimination or violates principles of equal treatment.[289]

This limitation reflects a broader structural difference between computational reasoning and legal reasoning. Machine learning systems operate through probabilistic inference and optimization, while legal systems require normative justification grounded in rules, rights, evidence, and procedural safeguards.[290] Statistical explanation therefore does not necessarily satisfy legal requirements concerning reason-giving or accountability.

The problem becomes particularly significant in relation to complex machine learning architectures, including deep learning systems. In such systems, predictions may emerge from interactions between thousands or millions of internal parameters distributed across multiple computational layers. Even where individual variables can be identified as influential, the overall interaction between variables may remain opaque due to the scale and complexity of the model architecture.

---

[286] Finale Doshi-Velez and Been Kim, 'Towards A Rigorous Science of Interpretable Machine Learning' (2017) arXiv preprint arXiv:1702.08608, 2–6.

[287] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31 Harvard Journal of Law & Technology 841, 861–870.

[288] Edwards and Veale (n 15) 24–29.

[289] Wachter, Mittelstadt and Russell (n 170) 5–8.

[290] Pasquale (n 206) 8–15.

From a technical standpoint, opacity may arise through several mechanisms:

- model complexity,
- high-dimensional feature interactions,
- proprietary restrictions,
- inaccessible training data,
- distributed system architecture,
- adaptive model behavior.

As a result, transparency cannot be reduced simply to access to source code or disclosure of individual variables. Understanding why a model generated a specific output may require access to:

- training datasets,
- model parameters,
- optimization procedures,
- calibration settings,
- feature engineering methods,
- deployment context.

Even where such information is available, the resulting computational processes may remain difficult to interpret meaningfully outside specialized technical expertise.[291]

This difficulty has led to the development of technical auditing and algorithmic accountability mechanisms intended to evaluate system behavior at a broader structural level. Auditing may involve testing systems for:

- discriminatory patterns,
- error rates,
- robustness,
- calibration consistency,
- fairness metrics,
- model drift over time.

However, audits themselves remain constrained by data availability, technical access, and methodological limitations.[292] In many operational environments, external actors may lack access to the training data or model architecture necessary to conduct meaningful independent evaluation.

Within migration governance, these issues are particularly significant because algorithmic systems frequently operate in contexts involving:

- evidentiary uncertainty,
- unequal power relations,
- restricted procedural access,
- cross-border information systems,

[291] Goodfellow, Bengio and Courville (n 163) 1–18.
[292] Barocas and Selbst (n 170) 691–705.

- large-scale biometric infrastructures.

Individuals affected by algorithmic classifications may therefore face considerable difficulties understanding how decisions were generated or identifying the technical basis upon which classifications were produced.[293]

From a legal perspective, explainability limitations create important tensions with procedural fairness guarantees under EU law. European legal frameworks require individuals to receive meaningful reasons for decisions affecting their rights and to possess the ability to challenge those decisions effectively.[294] However, statistical approximations of variable influence do not necessarily provide legally sufficient justification capable of supporting meaningful contestation or judicial review.

Consequently, explainability mechanisms should not be understood as complete solutions to algorithmic opacity. While they may improve technical visibility into model behavior, they cannot independently resolve the deeper structural tensions between probabilistic computation and normative legal accountability.[295]

Appendix I.H Fairness Metrics and Mathematical Incompatibility

Algorithmic auditing and bias assessment mechanisms frequently rely on quantitative fairness metrics intended to evaluate whether machine learning systems produce unequal outcomes across different groups. These metrics attempt to measure whether predictive systems distribute errors, classifications, or outcomes in a statistically balanced manner. However, fairness within machine learning is not a singular or universally agreed concept. Different technical definitions of fairness prioritize different forms of equality and may produce conflicting results within the same system.

Common fairness metrics include:

- equal accuracy,
- equal false positive rates,
- demographic parity,
- equalized odds,
- predictive parity,
- calibration consistency.

Each metric evaluates fairness according to a different statistical objective.

Demographic parity, for example, requires that different groups receive positive classifications at approximately equal rates regardless of underlying outcome distributions.[296] Equalized odds instead requires that error rates remain similar across groups, meaning that false positives and

[293] Fassin (n 274) 213–230.
[294] Charter (n 9) arts 41 and 47.
[295] Edwards and Veale (n 15) 24–29.
[296] Solon Barocas, Moritz Hardt and Arvind Narayanan, *Fairness and Machine Learning* (fairmlbook.org 2023) chs 1–3.

false negatives are distributed proportionately. Predictive parity focuses on maintaining equivalent predictive reliability across demographic categories, while calibration consistency requires probability scores to correspond equally to actual outcomes across groups.[297]

These approaches frequently conflict because they optimize different statistical relationships simultaneously. In practice, satisfying one fairness criterion may require violating another. This problem is commonly described as the mathematical incompatibility of fairness metrics.

For example, where two groups display different base rates within a dataset, it may be mathematically impossible to achieve:

- equal false positive rates,
- equal predictive value,
- equal calibration,

simultaneously within the same model.[298] Adjusting the system to satisfy one fairness metric may therefore worsen performance under another metric.

From a technical perspective, this incompatibility emerges because fairness constraints alter the statistical distribution of predictions and errors across groups. Machine learning systems operate through probabilistic optimization processes designed to maximize predictive performance according to selected objectives.[299] Once fairness constraints are introduced, the model must balance competing statistical priorities, often requiring trade-offs between:

- accuracy,
- sensitivity,
- specificity,
- calibration,
- group equality.

As a result, fairness cannot be reduced to a purely technical calculation capable of producing universally neutral outcomes. Different fairness metrics reflect different normative assumptions regarding which forms of inequality or error should be minimized.[300]

This becomes particularly significant within migration governance systems because classification errors may generate serious consequences for affected individuals. False positives may incorrectly categorize individuals as presenting elevated security or credibility risks, while false negatives may fail to identify individuals requiring protection or procedural attention. The selection of fairness metrics therefore indirectly determines how risks and errors are distributed across populations.[301]

[297] Wachter, Mittelstadt and Russell (n 170) 5–8.

[298] Jon Kleinberg, Sendhil Mullainathan and Manish Raghavan, 'Inherent Trade-Offs in the Fair Determination of Risk Scores' (2017) 8 Innovations in Theoretical Computer Science 1, 1–23.

[299] Bishop (n 163) 179–186.

[300] Wachter, Mittelstadt and Russell (n 170) 5–8.

[301] Eubanks (n 271) 126–154.

The problem is further complicated by the fact that migration datasets often involve highly heterogeneous populations, unequal sample sizes, and incomplete or uncertain information. Statistical disparities between groups may therefore arise from:

- data imbalance,
- inconsistent labeling,
- historical administrative patterns,
- demographic variation,
- unequal representation within training datasets.

Under these conditions, fairness metrics may produce unstable or contradictory results depending on the composition of the dataset and the technical configuration of the model.[302]

Algorithmic auditing systems attempt to evaluate these risks by testing models against selected fairness criteria. Audits may involve measuring:

- disparate impact,
- error distribution,
- calibration differences,
- group-level outcome disparities,
- threshold sensitivity.

However, because fairness metrics themselves remain contested, auditing cannot provide a singular objective determination of whether a system is "fair."[303] Instead, auditing reflects institutional decisions concerning which statistical inequalities are considered acceptable and which forms of error are prioritized within the governance framework.

From a legal perspective, this creates important tensions with principles of equality and non-discrimination under European law. EU legal standards evaluate discrimination through normative and contextual analysis rather than purely statistical optimization.[304] Machine learning fairness metrics, by contrast, translate equality concerns into mathematical constraints operating at the level of population distributions and error rates.

Consequently, technical fairness metrics cannot independently determine whether a system complies with legal standards of equal treatment. A model may satisfy selected statistical fairness criteria while still producing outcomes that raise concerns regarding indirect discrimination, procedural fairness, or individualized assessment.[305] Fairness within algorithmic governance therefore remains not only a technical problem, but also a legal, institutional, and political question concerning how risk, error, and inequality are distributed across affected populations.

[302] Barocas, Hardt and Narayanan (n 296) chs 3–5.
[303] Pasquale (n 206) 8–15.
[304] Pasquale (n 206) 8–15.
[305] Edwards and Veale (n 15) 24–29.

Appendix II : Private Contractors and EU Migration Infrastructure

Large-scale EU migration and border management systems are formally managed by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). However, substantial parts of the technical infrastructure underlying these systems are developed and maintained through procurement contracts awarded to private technology companies specializing in biometrics, interoperability systems, digital identity infrastructures, and border management technologies.[306]

1. IDEMIA and Sopra Steria and the Shared Biometric Matching System (sBMS)

In 2020, eu-LISA awarded a framework contract to a consortium composed of IDEMIA and Sopra Steria for the development of the Shared Biometric Matching System (sBMS), following competitive tender LISA/2019/RP/05 EES BMS and sBMS.[307] According to the procurement announcement, the contract was awarded for four years with the possibility of extension up to six years.[308]

The sBMS forms the core biometric interoperability infrastructure connecting multiple EU migration and border systems, including:

- Eurodac,
- the Visa Information System (VIS),
- the Entry/Exit System (EES),
- ETIAS,
- interoperability architectures managed by eu-LISA.[309]

According to IDEMIA's own project description, the sBMS stores and compares fingerprints and facial images of more than 400 million third-country nationals and was specifically designed to support Schengen border and migration management.[310]

---

[306] eu-LISA, 'About eu-LISA', https://www.eulisa.europa.eu/activities/large-scale-it-systems, accessed 17 May 2026.

[307] Press release IDEMIA and Sopra Steria chosen by eu-LISA to build the new Shared Biometric Matching System (sBMS) for border protection of the Schengen Area https://www.soprasteria.com/docs/librariesprovider2/sopra-steria-corporate/cp/080620_cp-fr_eu-lisa_vdef14289c11-114d-4481-89a8-8ec3cbad599a.pdf?sfvrsn=c71639dc_7 , accessed 17 May 2026.

[308] Sopra Steria, 'Sopra Steria and IDEMIA: Strengthening Border Security in the Schengen Area',
, accessed 17 May 2026.

[309] eu-LISA, 'First Interoperability Milestone Achieved: sBMS and VIS4EES Go Live',
, accessed 17 May 2026; Regulation (EU) 2019/817 (n 7); Regulation (EU) 2019/818 (n 31).

[310] IDEMIA, 'IDEMIA and Sopra Steria Chosen by eu-LISA to Build the New Shared Biometric Matching System (sBMS) for Border Protection in the Schengen Area',
, accessed 17 May 2026.

IDEMIA publicly markets itself as a provider of:

- biometric identification systems,
- facial recognition technologies,
- automated border control systems,
- AI-supported border management,
- traveler risk analysis systems.[311]

Its BORDERGUARD platform specifically advertises:

- AI-driven border processing,
- interoperability between migration databases,
- risk-based passenger analysis,
- biometric verification infrastructures,
- identity fraud detection.[312]

The company further states that its systems are developed for migration authorities and border agencies while emphasizing "privacy regulations," "ethical AI," and "compliance with EU requirements." IDEMIA, 'EU Entry/Exit System', https://www.idemia.com/eu-entry-exit-system, accessed 17 May 2026.[313]

Sopra Steria similarly presents itself as a provider of:

- homeland security infrastructures,
- governmental interoperability systems,
- migration and border databases,
- public sector digital governance systems.[314]

Company materials describe Sopra Steria and IDEMIA as "long-standing partners" involved in EU systems including VIS, SIS, and Eurodac for more than fifteen years.[315]

2. Atos, IBM, and Leonardo and the Entry/Exit System (EES)

In 2019, eu-LISA formalized a framework contract for the implementation of the Entry/Exit System (EES) with a consortium composed of Atos Belgium, IBM Belgium, and Leonardo

[311] IDEMIA, 'BORDERGUARD Solutions', , accessed 17 May 2026.

[312] IDEMIA, 'BORDERGUARD Intelligence', , accessed 17 May 2026.

[313] IDEMIA, 'EU Entry/Exit System', , accessed 17 May 2026.

[314] Sopra Steria, 'Sopra Steria and IDEMIA: Strengthening Border Security in the Schengen Area', , accessed 17 May 2026.

[315] IDEMIA, 'IDEMIA Public Security and Sopra Steria Launch Successful Go-Live of Shared Biometric Matching System with eu-LISA', , accessed 17 May 2026.

S.p.A. According to eu-LISA, the overall ceiling of the EES framework contract exceeded €142 million for a maximum period of six years.[316]

The EES constitutes one of the central components of the EU's "smart borders" architecture and is intended to record:

- entries and exits of third-country nationals,
- biometric identifiers,
- visa status,
- overstay calculations,
- travel movement histories.[317]

Research and reporting on EU migration infrastructures identify Atos as one of the principal contractors involved in interoperability and border database systems.[318] Leonardo participated as part of the consortium responsible for EES implementation, while IBM provided technical infrastructure and software support.[319]

Investigative reporting and eu-LISA internal communications later linked the consortium to substantial delays and technical implementation problems affecting deployment of the EES infrastructure.[320]

3. Technical Expertise and Migration Governance

The contractual structure of EU migration infrastructures demonstrates that private corporations are not merely generic software providers, but companies explicitly specializing in:

- biometric identification,
- migration databases,
- border surveillance,
- interoperability architectures,
- AI-supported risk analysis,
- digital identity systems.

These companies publicly market expertise in:

- border governance,
- migration control,

[316] eu-LISA, 'Today We Placed the Cornerstone of the New Information Architecture for Justice and Home Affairs',
, accessed 17 May 2026.

[317] ETIAS Regulation (n 129); Regulation (EU) 2019/817 (n 7); European Parliamentary Research Service, 'Artificial Intelligence at EU Borders',
, accessed 17 May 2026.

[318] Biometric Update, 'Atos and Partners Blamed for EES Delays',
, accessed 17 May 2026.

[319] eu-LISA, 'Today We Placed the Cornerstone of the New Information Architecture for Justice and Home Affairs', (n 316).

[320] ID Tech Wire, 'Investigation Blames Consortium as Key Obstacle to EU's Biometric Border Rollout',
, accessed 17 May 2026.

- Schengen interoperability,
- risk-based traveler assessment,
- biometric identity verification,
- compliance with EU regulatory frameworks.[321]

This is significant because technical design choices concerning:

- biometric thresholds,
- similarity scoring,
- interoperability structures,
- database architecture,
- risk classification systems,
- feature weighting,

are partially shaped through outsourced technological infrastructures developed by private actors operating outside ordinary public administrative structures.[322]

From a legal perspective, this complicates accountability and transparency because the technical logic influencing migration decision-making may be embedded within procurement contracts, proprietary infrastructures, and computational architectures that remain inaccessible to affected individuals and difficult to scrutinize judicially.[323]

[321] IDEMIA, 'BORDERGUARD Solutions', , accessed 17 May 2026; eu-LISA, 'Large-Scale IT Systems', , accessed 17 May 2026.

[322] Motzfeldt and Næsborg-Andersen (n 180); Yeung (n 153); Hildebrandt (n 134).

[323] Fink and Finck (n 171); Brouwer (n 141); Access Now and others (n 130); Stoyanova (n 60).

BIBLIOGRAPHY

I. Academic Literature

Books

Anil K Jain, Arun Ross and Karthik Nandakumar, *Introduction to Biometrics* (Springer 2011).

Cathy O'Neil, *Weapons of Math Destruction* (Penguin Books 2016).

Christopher M Bishop, *Pattern Recognition and Machine Learning* (Springer 2006).

Didier Fassin, *Policing Borders, Producing Boundaries* (Duke University Press 2011).

Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

Gregor Noll, *Proof, Evidentiary Assessment and Credibility in Asylum Procedures* (Martinus Nijhoff 2005).

Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* (MIT Press 2016).

Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford University Press 2020).

Niovi Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill 2022).

Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019).

Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2021).

Virginia Eubanks, *Automating Inequality* (St Martin's Press 2018).

Journal Articles and Chapters

Didier Bigo, Sergio Carrera and Elspeth Guild, 'What Future for the Area of Freedom, Security and Justice? Recommendations on EU Migration and Borders Policies in a Globalising World' (CEPS Policy Brief No 156, 2008).

Eleni Katsikouli and others, 'Machine Learning and Asylum Adjudications: From Analysis of Variations to Outcome Predictions' (2022) 10 *IEEE Access* 130955.

Evelien Brouwer, 'AI and Migration, Asylum and Border Control Management: Impact of the AI Act' in O Tambou and M Sweeney (eds), *Le règlement européen sur l'IA et au-delà. Quel encadrement de l'IA ?* (Bruylant 2025).

Evelien Brouwer, ‘Large-Scale Databases and Interoperability in Migration and Border Policies’ (2020) 26 *European Public Law* 71.

Finale Doshi-Velez and Been Kim, ‘Towards A Rigorous Science of Interpretable Machine Learning’ (2017) arXiv preprint arXiv:1702.08608.

Hanne Marie Motzfeldt and Ayo Næsborg-Andersen, ‘Developing Administrative Law into Handling the Challenges of Digital Government in Denmark’ (2018) 16(2) *Electronic Journal of e-Government* 136.

Karen Yeung, ‘Algorithmic Regulation: A Critical Interrogation’ (2018) 12(4) *Regulation & Governance* 505.

Linda J Skitka, Kathleen L Mosier and Mark Burdick, ‘Does Automation Bias Decision-Making?’ (1999) 51(5) *International Journal of Human-Computer Studies* 991.

Maya Ellen Hertz, Thomas Gammeltoft-Hansen and William Hamilton Byrne, ‘What “Real Risk” Means For AI-Assisted Refugee Status Determination’ (2025) *Verfassungsblog*.

Melanie Fink and Michèle Finck, ‘Reasoned A(I)dministration: Explanation Requirements in EU Law and the Automation of Public Administration’ (2022) *European Law Review*.

Robert Thomas, ‘Assessing the Credibility of Asylum Claims: EU and UK Approaches Examined’ (2006) 8(1) *European Journal of Migration and Law* 79.

Sandra Wachter, Brent Mittelstadt and Chris Russell, ‘Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR’ (2018) 31 *Harvard Journal of Law & Technology* 841.

Sandra Wachter, Brent Mittelstadt and Chris Russell, ‘Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI’ (2021) 41 *Computer Law & Security Review* 105567.

Sandra Wachter, Brent Mittelstadt and Luciano Floridi, ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’ (2017) 7 *International Data Privacy Law* 76.

Sebastiano Antonio Piccolo and others, ‘On Predicting and Explaining Asylum Adjudication’ (2023) *Proceedings of the International Conference on Artificial Intelligence and Law* 217–226.

Solon Barocas and Andrew D Selbst, ‘Big Data’s Disparate Impact’ (2016) 104 *California Law Review* 671.

Thomas Gammeltoft-Hansen and Rosemary Byrne, ‘Digital Evidence in Refugee Status Determination’ (2021) *Nordic Journal of International Law* 1.

Trine Rask Nielsen, Thomas Gammeltoft-Hansen and Naja Holten Møller, ‘Mobile Phone Data Transforming Casework in Asylum Decision-Making: Insights from the Danish Case’ (2024) 1(4) *ACM Journal on Responsible Computing* art 27.

Ulrik B.U. Røhl and Morten Balle Hansen, 'Automated Administrative Decision-Making and Good Governance: Synergies, Trade-offs and Limits' (2024).

Valsamis Mitsilegas, 'The Transformation of European Border Controls: The New Architecture of EU Migration Management' (2022) 44 *Journal of Ethnic and Migration Studies* 1.

William Hamilton Byrne and others, 'Data-Driven Futures of International Refugee Law' (2024) 37(4) *Journal of Refugee Studies* 915–937.

II. Legal Instruments

European Union Law

Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47.

Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection [2011] OJ L337/9.

Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection [2013] OJ L180/60.

Directive 2013/33/EU of the European Parliament and of the Council of 26 June 2013 laying down standards for the reception of applicants for international protection (recast) [2013] OJ L180/96.

European Commission, *Communication on a New Pact on Migration and Asylum* COM (2020) 609 final.

Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) [2008] OJ L218/60.

Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 [2013] OJ L180/1.

Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast) [2013] OJ L180/31.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorization System (ETIAS) [2018] OJ L236/1.

Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) [2018] OJ L295/99.

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) [2018] OJ L312/56.

Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa [2019] OJ L135/27.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police cooperation, judicial cooperation, asylum and migration [2019] OJ L135/85.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L.

Treaty of Amsterdam [1997] OJ C340/1.

Treaty of Lisbon [2007] OJ C306/1.

III. Case Law

Court of Justice of the European Union

Case C-277/11 *M.M. v Minister for Justice, Equality and Law Reform* EU:C:2012:744.

Case C-634/21 *SCHUFA Holding AG v OQ* EU:C:2023:957.

Joined Cases C-411/10 and C-493/10 *N.S. v Secretary of State for the Home Department* EU:C:2011:865.

Joined Cases C-148/13 to C-150/13 *A, B and C v Staatssecretaris van Veiligheid en Justitie* EU:C:2014:2406.

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* EU:C:2014:238.

Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others*EU:C:2020:791.

Case C-199/11 *European Community v Otis NV* EU:C:2012:684.

European Court of Human Rights

Dombo Beheer BV v Netherlands (1993) 18 EHRR 213.

M.S.S. v Belgium and Greece App no 30696/09 (ECtHR, 21 January 2011).

IV. Reports and Documents from International Organizations

EUAA, *Practical Guide on Evidence and Risk Assessment* (2024).

European Union Agency for Fundamental Rights, *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights* (2018).

UNHCR, *Handbook on Procedures and Criteria for Determining Refugee Status* (2019).

V. Reports and Documents from NGOs

Access Now and others, *Uses of AI in Migration and Border Control*.

PICUM, *Data Protection, Immigration Enforcement and Fundamental Rights* (2019).

VI. Institutional and Technical Online Sources

European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), 'About eu-LISA' https://www.eulisa.europa.eu/activities/large-scale-it-systems accessed 17 May 2026.

Press Release, 'IDEMIA and Sopra Steria Chosen by eu-LISA to Build the New Shared Biometric Matching System (sBMS) for Border Protection of the Schengen Area' https://www.soprasteria.com/docs/librariesprovider2/sopra-steria-corporate/cp/080620_cp-fr_eu-lisa_vdef14289c11-114d-4481-89a8-8ec3cbad599a.pdf?sfvrsn=c71639dc_7 accessed 17 May 2026.

Sopra Steria, 'Sopra Steria and IDEMIA: Strengthening Border Security in the Schengen Area' https://www.soprasteria.co.uk/insights/client-success-stories/details/sopra-steria-and-idemia-strengthening-border-security-in-the-schengen-area accessed 17 May 2026.

European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), 'First Interoperability Milestone Achieved: sBMS and VIS4EES Go Live' https://www.eulisa.europa.eu/news-and-events/news/first-interoperability-milestone-achieved-sbms-and-vis4ees-go-live accessed 17 May 2026.

IDEMIA, 'IDEMIA and Sopra Steria Chosen by eu-LISA to Build the New Shared Biometric Matching System (sBMS) for Border Protection in the Schengen Area' https://www.idemia.com/press-release/idemia-and-sopra-steria-chosen-eu-lisa-build-

new-shared-biometric-matching-system-sbms-border-protection-schengen-area-2020-06-04 accessed 17 May 2026.

IDEMIA, 'BORDERGUARD Solutions' https://www.idemia.com/border-control-solutions-borderguard accessed 17 May 2026.

IDEMIA, 'BORDERGUARD Intelligence' https://www.idemia.com/borderguard-intelligence accessed 17 May 2026.

IDEMIA, 'EU Entry/Exit System' https://www.idemia.com/eu-entry-exit-system accessed 17 May 2026.

IDEMIA, 'IDEMIA Public Security and Sopra Steria Launch Successful Go-Live of Shared Biometric Matching System with eu-LISA' https://www.idemia.com/press-release/idemia-public-security-and-sopra-steria-launch-successful-go-live-shared-biometric-matching-system-eu-lisa-2025-08-25 accessed 17 May 2026.

European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), 'Today We Placed the Cornerstone of the New Information Architecture for Justice and Home Affairs' https://www.eulisa.europa.eu/news-and-events/news/today-we-placed-cornerstone-new-information-architecture-justice-and-home accessed 17 May 2026.

European Parliamentary Research Service, *Artificial Intelligence at EU Borders*https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA%282021%29690706_EN.pdf accessed 17 May 2026.

Biometric Update, 'Atos and Partners Blamed for EES Delays' https://www.biometricupdate.com/202412/atos-and-partners-blamed-for-ees-delays accessed 17 May 2026.

ID Tech Wire, 'Investigation Blames Consortium as Key Obstacle to EU's Biometric Border Rollout' https://idtechwire.com/investigation-blames-consortium-as-key-obstacle-to-eus-biometric-border-rollout/ accessed 17 May 2026.

National Institute of Standards and Technology, 'NIST Special Database 24: SD24 Fingerprint Database' (NIST, 2000).