

Freedom, Security & Justice: European Legal Studies

Rivista giuridica di classe A

2026, n. 3

EDITORIALE SCIENTIFICA

DIRETTRICE

Angela Di Stasi
Ordinario di Diritto Internazionale e di Diritto dell'Unione europea, Università di Salerno
Titolare della Cattedra Jean Monnet 2017-2020 (Commissione europea)
"Judicial Protection of Fundamental Rights in the European Area of Freedom, Security and Justice"

CONSIGLIO SCIENTIFICO

Giandonato Caggiano, Ordinario f.r. di Diritto dell'Unione europea, Università Roma Tre
Sergio Maria Carbone, Professore Emerito, Università di Genova
Roberta Clerici, Ordinario f.r. di Diritto Internazionale privato, Università di Milano †
Nigel Lowe, Professor Emeritus, University of Cardiff
Paolo Mengozzi, Professore Emerito, Università "Alma Mater Studiorum" di Bologna - già Avvocato generale presso la Corte di giustizia dell'UE
Massimo Panebianco, Professore Emerito, Università di Salerno
Nicoletta Parisi, Ordinario f.r. di Diritto Internazionale, Università di Catania - già Componente ANAC
Guido Raimondi, già Presidente della Corte EDU – già Presidente di Sezione della Corte di Cassazione
Silvana Sciarra, Professore Emerito, Università di Firenze - Presidente Emerito della Corte Costituzionale
Giuseppe Tesauro, Professore f.r. di Diritto dell'UE, Università di Napoli "Federico II" - Presidente Emerito della Corte Costituzionale †
Antonio Tizzano, Professore Emerito, Università di Roma "La Sapienza" - Vice Presidente Emerito della Corte di giustizia dell'UE
Ennio Triggiani, Professore Emerito, Università di Bari †
Ugo Villani, Professore Emerito, Università di Bari

COMITATO EDITORIALE

Maria Caterina Baruffi, Ordinario di Diritto Internazionale, Università di Bergamo
Alfonso-Luis Calvo Caravaca, Catedrático Jubilado de Derecho Internacional Privado, Universidad Carlos III de Madrid
Ida Caracciolo, Ordinario di Diritto Internazionale, Università della Campania – Giudice dell'ITLOS
Pablo Antonio Fernández-Sánchez, Profesor Emérito de Derecho Internacional, Universidad de Sevilla
Inge Govaere, Director of the European Legal Studies Department, College of Europe, Bruges
Paola Mori, Ordinario f.r. di Diritto dell'Unione europea, Università "Magna Graecia" di Catanzaro
Lina Panella, Ordinario f.r. di Diritto Internazionale, Università di Messina
Lucia Serena Rossi, Ordinario di Diritto dell'UE, Università "Alma Mater Studiorum" di Bologna – già Giudice della Corte di giustizia dell'UE

COMITATO DEI REFEREES

Bruno Barel, Associato f.r. di Diritto dell'Unione europea, Università di Padova **Marco Benvenuti**, Ordinario di Istituzioni di Diritto pubblico, Università di Roma "La Sapienza **Fiammetta Borgia**, Ordinario di Diritto Internazionale, Università di Roma "Tor Vergata" **Francesco Buonomenna**, Associato di Diritto dell'Unione europea, Università di Salerno **Raffaele Cadin**, Ordinario di Diritto Internazionale, Università di Roma "La Sapienza" **Ruggiero Cafari Panico**, Ordinario f.r. di Diritto dell'Unione europea, Università di Milano **Federico Casolari**, Ordinario di Diritto dell'Unione europea, Università "Alma Mater Studiorum" di Bologna **Luisa Cassetti**, Ordinario di Istituzioni di Diritto Pubblico, Università di Perugia **Anna Cavaliere**, Associato di Filosofia del diritto, Università di Salerno **Giovanni Cellamare**, Ordinario f.r. di Diritto Internazionale, Università di Bari **Giuseppe D'Angelo**, Ordinario di Diritto e religione, Università di Salerno **Sara De Vido**, Ordinario di Diritto Internazionale, Università Ca' Foscari Venezia **Valeria Di Comite**, Ordinario di Diritto dell'Unione europea, Università di Bari "Aldo Moro" **Marcello Di Filippo**, Ordinario di Diritto Internazionale, Università di Pisa **Carmela Elefante**, Associato di Diritto e religione, Università di Salerno **Rosario Espinosa Calabuig**, Catedrática de Derecho Internacional Privado, Universitat de València **Valentina Faggiani**, Profesora Titular de Derecho Constitucional, Universidad de Granada **Caterina Fratea**, Associato di Diritto dell'Unione europea, Università di Verona **Ana C. Gallego Hernández,** Profesora Ayudante de Derecho Internacional Público y Relaciones Internacionales, Universidad de Sevilla **Pietro Gargiulo**, Ordinario f.r. di Diritto Internazionale, Università di Teramo **Francesca Graziani**, Associato di Diritto Internazionale, Università della Campania "Luigi Vanvitelli" **Giancarlo Guarino**, Ordinario f.r. di Diritto Internazionale, Università di Napoli "Federico II" **Elspeth Guild**, Associate Senior Research Fellow, CEPS **Victor Luis Gutiérrez Castillo**, Profesor de Derecho Internacional Público, Universidad de Jaén **Ivan Ingravallo**, Ordinario di Diritto Internazionale, Università di Bari **Paola Ivaldi**, Ordinario di Diritto Internazionale, Università di Genova **Luigi Kalb**, Ordinario f.r. di Procedura Penale, Università di Salerno **Gianfranco Liace**, Associato di Diritto dell'economia, Università di Salerno **Luisa Marin**, Ricercatore di Diritto dell'UE, Università dell'Insubria **Simone Marinai**, Associato di Diritto dell'Unione europea, Università di Pisa **Fabrizio Marongiu Buonaiuti**, Ordinario di Diritto Internazionale, Università di Macerata **Rostane Medhi**, Professeur de Droit Public, Université d'Aix-Marseille **Michele Messina**, Ordinario di Diritto dell'Unione europea, Università di Messina-Esperto Giuridico presso la Rappresentanza Permanente d'Italia a Bruxelles **Stefano Montaldo**, Associato di Diritto dell'Unione europea, Università di Torino **Violeta Moreno-Lax**, Senior Lecturer in Law, Queen Mary University of London **Claudia Morviducci**, Professore Senior di Diritto dell'Unione europea, Università Roma Tre **Michele Nino**, Ordinario di Diritto Internazionale, Università di Salerno **Criseide Novi**, Ordinario di Diritto dell'Unione europea, Università di Foggia **Anna Oriolo**, Associato di Diritto Internazionale, Università di Salerno **Leonardo Pasquali**, Ordinario di Diritto internazionale, Università di Pisa **Piero Pennetta**, Ordinario f.r. di Diritto Internazionale, Università di Salerno **Francesca Perrini**, Associato di Diritto Internazionale, Università di Messina **Gisella Pignataro**, Associato di Diritto privato comparato, Università di Salerno **Emanuela Pistoia**, Ordinario di Diritto dell'Unione europea, Università di Teramo **Anna Pitrone**, Associato di Diritto dell'Unione europea, Università di Messina **Concetta Maria Pontecorvo**, Ordinario di Diritto Internazionale, Università di Napoli "Federico II" **Pietro Pustorino**, Ordinario di Diritto Internazionale, Università LUISS di Roma **Santiago Ripol Carulla**, Catedrático de Derecho internacional público, Universitat Pompeu Fabra Barcelona **Angela Maria Romito**, Associato di Diritto dell'Unione europea, Università di Bari **Gianpaolo Maria Ruotolo**, Ordinario di Diritto Internazionale, Università di Foggia **Teresa Russo**, Associato di Diritto dell'Unione europea, Università di Salerno **Alessandra A. Souza Silveira**, Diretora do Centro de Estudos em Direito da UE, Universidad do Minho **Ángel Tinoco Pastrana**, Profesor de Derecho Procesal, Universidad de Sevilla **Sara Tonolo**, Ordinario di Diritto Internazionale, Università degli Studi di Padova **Chiara Enrica Tuo**, Ordinario di Diritto dell'Unione europea, Università di Genova **Talitha Vassalli di Dachenhausen**, Ordinario f.r. di Diritto Internazionale, Università di Napoli "Federico II" **Alessandra Viviani**, Ordinario di Diritto Internazionale, Università di Siena **Valentina Zambrano**, Associato di Diritto Internazionale, Università di Roma "La Sapienza" **Alessandra Zanobetti**, Ordinario f.r. di Diritto Internazionale, Università "Alma Mater Studiorum" di Bologna

COMITATO DI REDAZIONE

Angela Festa, Docente incaricato di Diritto dell'Unione europea, Università della Campania "Luigi Vanvitelli"
Anna Iermano, Associato di Diritto Internazionale, Università di Salerno
Daniela Marrani, Associato di Diritto Internazionale, Università di Salerno
Rossana Palladino (Coordinatore), Associato di Diritto dell'Unione europea, Università di Salerno

Revisione linguistica degli abstracts a cura di
Francesco Campofreda, Dottore di ricerca in Diritto Internazionale, Università di Salerno

Rivista quadrimestrale on line "Freedom, Security & Justice: European Legal Studies" www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario
2026, n. 3

Editoriale

Quale diritto internazionale nel contesto degli attuali scenari di guerra? p. 1
Giuseppe Cataldi

Saggi e Articoli

Implementing the EU Pact at the external borders: readiness, interoperability and safeguards in Spain, Lithuania and Bulgaria p. 16
Mª Ángeles Cano Linares

Sanzioni economiche come norme di applicazione necessaria e contratti internazionali: una relazione intricata p. 46
Angelo Davì, Alessandra Zanobetti

La circolazione internazionale delle armi, la *due diligence* dello Stato esportatore e la protezione dei diritti umani nel contesto internazionale ed europeo p. 67
Alessandra Pietrobon

Cum Grano Salis: segnalazioni, controlli Schengen e immunità parlamentare europea p. 96
Angela Procaccino

Artificial Intelligence in EU migration and border control: balancing security, efficiency and fundamental rights p. 126
César A. Villegas Delgado

Dialogo a due voci: Corte di Strasburgo e giudice nazionale

L'esecuzione delle decisioni di condanna della Corte EDU tra ordinamento interno e garanzie convenzionali p. 157
Gaetano De Amicis

La "creatività" e l'interpretazione "intersistemica" della Corte di Strasburgo nel dialogo con il giudice nazionale p. 180
Guido Raimondi

Commenti e Note

Effettività della tutela degli interessi finanziari dell'Unione e *standard* nazionale di protezione dei diritti fondamentali nella sentenza *Lin II* della Corte di giustizia p. 187
Matteo Agostino

Codification of ambiguity in the European Pact on Migration and Asylum. The case of *de facto* detention in the Pantelleria hotspot p. 221
Greta Albertari

Il nuovo quadro europeo anticorruzione e le ricadute interne: la direttiva (UE) 2026/1021 tra principio di leale cooperazione e "vuoti di tutela" p. 247
Andrea Castaldo, Marco Siligato

La troisième vague dans la protection des victimes d'infractions pénales en droit de l'Union européenne: réflexions à la lumière de la révision de la directive 2012/29/UE p. 284
Alessandro Rosanò

The principle of *non-refoulement* in the face of climate-induced migration. Prospects for protection under the Inter-American human rights system p. 308
Martina Sardo

ARTIFICIAL INTELLIGENCE IN EU MIGRATION AND BORDER CONTROL: BALANCING SECURITY, EFFICIENCY AND FUNDAMENTAL RIGHTS

César A. Villegas Delgado *

SUMMARY: 1. Introduction. – 2. Artificial Intelligence and the transformation of EU migration control. – 3. A patchwork of rules: the EU legal framework governing AI in migration control. – 4. Fundamental rights at risk. – 5. Algorithmic decision-making and migrant vulnerability. – 6. The EU AI Act and migration control. – 7. Beyond compliance and towards a fundamental rights-based model of AI migration governance. – 8. Conclusions.

1. Introduction

Over the last few years Artificial Intelligence (AI) has moved from the margins to the centre of migration and border management in the European Union. In the past decade, the digitalisation of European borders has changed how Member States and EU institutions identify, monitor and assess the third-country nationals who seek to enter or remain in the Union. Technological advances and the exponential emergence of new tools such as biometric identification, automated data processing, smart surveillance, and algorithmic risk assessments are no longer experimental tools but working parts of an infrastructure built to make migration management faster, safer and better coordinated. This transformation is underpinned by several large-scale EU information systems and their increasing interoperability.[1] These systems allow national and European authorities to collect, store and cross-check personal and biometric data on a scale that would have

Double-blind peer reviewed article.

* Associate Professor of Public International and EU Law, University of Seville. E-mail: cvillegas@us.es.

The author would like to express his sincere gratitude to the journal's reviewers and, in particular, to Professor Simona Fanni for their valuable comments and insightful suggestions on an earlier draft of this article.

[1] According to IBM "interoperable systems" play an increasingly vital role in healthcare, government, commerce and public safety. Interoperability provides an efficient and effective way for diverse information technology (IT) systems in these areas to connect, communicate and share essential data. Interoperability is made possible by using common standards that define how data is formatted and exchanged between systems. Sometimes, interoperability standards are mandated by law to help ensure the compatibility of critical systems, such as those used for public health, commerce, government or public safety, https://www.ibm.com/think/topics/interoperability.

seemed unrealistic a generation ago.[2] As these systems become interoperable, the very idea of a European border starts to shift. A border check is no longer only something that happens at a checkpoint; it happens through data, often before a traveller ever reaches one, and again afterwards, through automated assessments that most people never see. None of this is arbitrary. AI-based tools can verify identity more reliably, flag likely document fraud, feed into risk assessment, strengthen cooperation between national authorities, and help handle information at a volume no single caseworker could manage alone. If used well, they promise genuine gains in efficiency and security. If used carelessly, the same tools that speed up border checks can just as easily become instruments of surveillance, profiling and automated classification of who counts as a risk.

As the European Parliamentary Research Service (EPRS) has pointed out: "There are clear benefits to be reaped from a careful adoption of AI technologies in the context of border control […]. However, these benefits need to be balanced against the significant risks posed by these technologies to fundamental rights. Despite progress regarding biometric identification technologies, the accuracy of the results still varies across technologies and depends on contextual factors. Even the relatively well-established fingerprint identification applications face challenges, at the stage of the collection of biometric data (related to, for example, subjects' age and environmental conditions). The reliability of face recognition technologies in "real world" settings is highly dependent on the quality of the images captured and on the quality of the algorithms used for biometric matching. The quality of the algorithms depends, in turn, on the quality of the

[2] As an example of these large-scale IT systems used by the EU, we can mention *Eurodac* (Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of "Eurodac" for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes), the *Schengen Information System (SIS)*, Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006. 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) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, the *Visa Information System (VIS)*, Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), the *Entry/Exit System (EES)* Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 and the *European Travel Information and Authorisation System (ETIAS)* Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.

training datasets (including the quality, completeness and relevance of training images) and the various optimisation techniques. Serious doubts exist about the scientific basis and reliability of emotion-detection algorithms. Concerns about data accuracy have been raised regarding many EU information systems and information exchange frameworks for borders and security. Face recognition technologies have come under increased scrutiny due to concerns about fundamental rights, in particular risks related to bias and discrimination, data protection and mass surveillance. Whereas great attention has been paid to the issue of bias and discrimination, it must be noted that even accurate and unbiased AI systems may pose significant other risks, including data protection and privacy. The increased use of biometric data in EU information systems amplifies the risk of unlawful profiling (for example, facial images may reveal ethnic origin). Even when profiling is not based on biometric or personal data, other types of data or combinations thereof used for algorithmic profiling may lead to discrimination based on prohibited grounds. Existing safeguards, such as the human-in-the-loop safeguard (requiring human interaction) and the right to explanation may not be sufficient to tackle these risks".[3]

In our view, this is the central paradox running through the debate on AI and migration control. The very features that make these tools attractive to policymakers, among them their speed, their capacity to process vast amounts of data, and their apparent objectivity, are precisely what make them dangerous once left unchecked. Efficiency and rights protection do not naturally align in this space; more often, they pull in opposite directions, and it is this tension that any serious account of AI in EU migration control must confront.

In light of the foregoing, this paper examines the tension between security, efficiency, and the protection of fundamental rights arising from the increasing use of AI in EU migration and border control. First, we will analyse how artificial intelligence has reshaped EU migration control, moving from biometric identification to predictive and risk-scoring tools deployed at the border. Second, the legal framework currently governing these technologies, which ranges from the EU Charter and the GDPR to more specific migration and border-management instruments, will be examined. Third, the human rights most directly placed at risk, particularly privacy, data protection and non-discrimination, are then addressed in the fourth section of our work. The fifth section examines how algorithmic decision-making exacerbates the structural vulnerability of migrants, who often lack effective means to challenge automated outcomes. Attention turns, in the sixth section, to the EU AI Act's treatment of migration-related uses and how far it addresses the concerns raised earlier. The seventh section moves beyond a compliance-based reading of the Act to outline a fundamental rights-based model of AI governance, grounded in stronger accountability, transparency and human oversight. Finally, this paper closes with some concluding remarks on balancing security, efficiency

[3] C. DUMBRAVA, European Parliamentary Research Service. *Artificial intelligence at EU borders: Overview of applications and key issues*. Briefing PE 690.706. Brussels, European Parliament, 2021, p. II, see at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)690706.

and fundamental rights in EU border control, keeping in mind that human rights and the rule of law are among the core values and principles of the EU itself.

2. Artificial Intelligence and the transformation of EU migration control

European border management[4] has not always looked the way it does today. For much of the twentieth century, controlling who crossed a border was largely a paper-based, face-to-face affair, resting on physical documents and the judgement of officials stationed at a checkpoint. That model has given way, over the past two decades, to the large-scale collection, processing and storage of migrants' personal and biometric data, carried out through an expanding network of large-scale IT systems. At the European Union level, instead, the focus of the so-called "integrated border management" is on persons rather than on goods. Integrated border management is considered a necessary corollary to the free movement of persons and central to improving migration management. Its aims include efficiently managing the crossing of the external borders and addressing migratory challenges and potential future threats at those borders, while fully respecting fundamental rights.[5] In recent decades, the way in which border management in the EU and in other Western democratic countries in general has been practised has undergone significant changes, becoming increasingly technologised and digitalised. Traditional physical borders have been supplemented by new digital borders in the form of large-scale information systems that target primarily the movements of third-country nationals,[6] weakening the role played by the physical aspect of border management, including the actual crossing of territorial borders.[7] New border control technologies, which have become increasingly reliant on systematic and large-scale processing of personal data, especially biometric data, have been deployed with the

[4] The term border security is sometimes used in everyday parlance. However, this term is not defined in EU legislation. In the EU policy context, the preferred term is *border management*. Border management, or more precisely, European integrated border management (EIBM) is defined in Regulation (EU) 2019/1896 on the European Border and Coast Guard, and comprises multiple components such as border control, search and rescue, risk analyses, information exchange and cooperation. The border control component is further defined by reference to Regulation (EU) 2016/399 on the Schengen Borders Code to comprise both border checks and border surveillance. See, D. ANDERSON, A. BELCINEANU, M. TZVETKOVA, *AI for Border Management and Customs Controls – Anthology of EU-funded projects, 2015-2024*. European Union Joint Research Centre, 2025, JCR 143223.

[5] N. MORAG, *Border Management in Europe: Is the Paradigm Evolving?*, in *Homeland Security Affairs*, 2020, no. 1. Recital 1 Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, OJ L 295, 14.11.2019, 1-131 (Frontex Regulation). See also Recital 6 Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 77, 23.3.2016, p. 1–52.

[6] G. GONZÁLEZ FUSTER, S. GUTWIRTH, *When 'Digital Borders' Meet 'Surveilled Geographical Borders': Why the Future of EU Border Management Is a Problem*, in J. PETER BURGEES, S. GUTWIRTH (eds.), *A Threat against Europe. Security, Migration and Integration*, Brussels, 2011, pp. 171-90.

[7] T. BERRY, *The Changing Border: Developments and Risks in Border Control Management of Western Countries*, in *International Review of Administrative Sciences*, vol. 76, 2010, no. 2, pp. 259-278.

objective of enhancing the efficiency of mobility control and increasing security.[8] Checks at territorial borders have become progressively automated and combined with checks before and during travel, as well as after arrival, now commonly in place.

This transformation did not occur overnight. Tracing the historical development of identification technologies in border management, from the passport and the fingerprint to photography and facial recognition, the European Parliamentary Research Service frames it as a continuous effort to render the traveller "legible" to the State.[9] In this regard, the processing of biometric data has been actively supported at EU level[10] in the context of EU-level large-scale IT systems in the Area of Freedom, Security and Justice (AFSJ). These systems, initially set up by the EU for asylum – and migration – management but increasingly also serving internal security, almost systematically rely on biometric data.[11] Today, biometric identification constitutes the technological backbone of the EU's digital border regime. Yet, what distinguishes the current phase in this technological genealogy is the progressive integration of AI into an already highly digitalised and biometric border management architecture – algorithmic systems not only store or retrieve biometric data but actively classify, score, and predict, transforming border management from a reactive, verification-based exercise into an anticipatory risk-based one.[12]

At the same time, biometric identification is embedded operationally in an expanding constellation of centralised EU information systems. Currently, the EU and its Member States have four large-scale IT systems – the Schengen Information System (SIS),[13] the

[8] G. GONZÁLEZ FUSTER ET. AL., *Privacy and Data Protection in the EU Security Continuum*, INEX Policy Brief nº 12, 2011, Brussels, Centre for European Policy Studies (CEPS), June 2011.
[9] C. DUMBRAVA, European Parliamentary Research Service, *op. cit.*
[10] For an overview of national laws of EU Member States on the processing of facial images, see Ernst & Young Baltic AS (2020), *Towards the European Level Exchange of Facial Images: Legal Analysis for TELEFI Project*, TELEFI Project (Towards the European Level Exchange of Facial Images), 7 February 2020, https://www.telefi-project.eu/telefi-project/results.
[11] The EU Agency for Fundamental Rights has highlighted that the impact of these large-scale IT systems on fundamental rights remains largely unexplored territory, see European Union Agency for Fundamental Rights (FRA), *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights*, Luxembourg, Publications Office of the European Union, 2018, doi:10.2811/136698, p. 19.
[12] C. DUMBRAVA, European Parliamentary Research Service, *op. cit.*
[13] The Schengen Information System (SIS) is the most widely used and largest information sharing system for security and border management in Europe. As there are no internal borders between Schengen countries in Europe, SIS compensates for border controls and is the most successful cooperation tool for border, immigration, police, customs and judicial authorities in the EU and the Schengen associated countries. Competent national authorities, such as the police and border guards, are able to enter and consult alerts on people and objects in one common database. These people and objects can be located anywhere within the EU and the Schengen area during border, police or other lawful checks. Each year, eu-LISA publishes a list of competent authorities, such as the one for 2025. Since 1995, the system has helped Europe preserve its security in the absence of internal border checks. In 2013, the second generation of SIS (SIS II) was rolled out, with additional functionalities, such as the possibility of adding fingerprints and photographs to alerts. In March 2023, SIS was renewed with new alerts, upgraded data and enhanced functionalities. See https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_en.

European Dactyloscopy Database (Eurodac),[14] the Visa Information System (VIS),[15] and the Entry/Exit System (EES).[16] Soon, two other large-scale IT systems will be implemented, namely the European Travel Information and Authorisation System (ETIAS)[17] and the European Criminal Records Information System on Third-Country Nationals (ECRIS-TCN).[18]

The systems were developed over time independently for different purposes. As a result, relevant national authorities might have difficulty making connections between pieces of information, to get a clear picture. In its Communication of 6 April 2016 on *Stronger and Smarter Information Systems for Borders and Security*,[19] the European Commission underlined the need to improve the Union's data management architecture for border management and security purposes. On this basis, the EU adopted a framework for the interoperability between the Union's large-scale IT systems in the field of borders, visa, police and judicial cooperation, asylum and migration. Regulations (EU) 2019/817

[14] As of June 2026, the digitalisation of border and migration management at EU level has taken a major step forward, with the operationalisation of the new Eurodac database, the European Search Portal (ESP) and the Common Identity Repository (CIR), which enhance border security and identity management across the EU. Eurodac is the European Union's asylum and migration database. The updated Eurodac also helps authorities to tackle irregular migration, track secondary movements and improve returns of irregular migrants. EU Member States are obliged to register in Eurodac: asylum applicants; all those apprehended following irregular crossings of EU external borders; all those disembarked following search and rescue operations or found to be staying illegally in a Member State; as well as people arriving under a resettlement scheme and beneficiaries of temporary protection. The identity and biometric data of those who were apprehended following irregular crossings of EU external borders, of those disembarked following search and rescue operations and of resettled persons will remain in the system for 5 years, making it possible to retrieve information on individuals in the system for a longer period of time. For asylum applicants, the storage period remains 10 years. This will help facilitate the identification of individuals and give authorities more information allowing for speedier asylum procedures and better detection of 'secondary movements', where asylum applicants abscond to an EU Member State other than the one in which they applied for asylum. See, https://home-affairs.ec.europa.eu/policies/migration-and-asylum/migration-management/digital-border-and-migration-management-eu_en.

[15] The Visa Information System (VIS) (consolidated version) allows Schengen States to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes. See, https://home-affairs.ec.europa.eu/policies/schengen/visa-information-system_en.

[16] The Entry/Exit System (EES) is an automated IT system for registering non-EU nationals travelling for a short stay, see https://travel-europe.europa.eu/ees/what-is-the-ees.

[17] ETIAS travel authorisation is an entry requirement for visa-exempt nationals travelling to any of these 30 European countries. It is linked to a traveller's passport. It is valid for up to three years or until the passport expires, whichever comes first. If you get a new passport, you need to get a new ETIAS travel authorisation. With a valid ETIAS travel authorisation, you can enter the territory of these European countries as often as you want for short-term stays - normally for up to 90 days in any 180-day period. However, it does not guarantee entry. When you arrive, a border guard will ask to see your passport and other documents and verify that you meet the entry conditions. ETIAS is currently not in operation and no applications for travel authorisations are collected at this point. See https://travel-europe.europa.eu/en/etias.

[18] This central system aims to improve the exchange of criminal records information regarding convicted non-EU-citizens and stateless persons through the existing European Criminal Records Information System (ECRIS). See https://ec.europa.eu/commission/presscorner/detail/en/ip_19_2018.

[19] See, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A205%3AFIN.

and (EU) 2019/818 establish a framework for interoperability between EU information systems in the fields of borders and visa, and of police and judicial cooperation, asylum and migration, respectively.[20] Interoperability introduces four common components, first a shared biometric matching service, second a common identity repository, third a multiple-identity detector and finally a European search portal – that together allow a single query to search across previously separate databases simultaneously.[21] The merger of six formerly distinct EU databases into one overarching information system was designed in part to serve internal security and law enforcement objectives not necessarily foreseen when the individual databases were first established. This raises serious questions about compliance with the principle of purpose limitation, and about the additional risks faced by children, migrants, asylum seekers and other vulnerable categories of data subjects.[22]

The final layer of this technological transformation consists of predictive and risk-assessment tools that move beyond identity verification towards the anticipation of future behaviour. In 2019, the EU Agency for Fundamental Rights condemned the unrestricted use of such tools and warned against the human rights violations stemming from automated border management. AI-embedded risk evaluation and profiling algorithms determine how risky an individual is for European security.[23] The pre-defined risk indicators, such as race, sex, and nationality, can lead to discriminatory and unlawful profiling of asylum or visa applicants. The automated classification as a high or low risk incomer jeopardises human dignity and surpasses the human side of the assessment, which is biased. The automated predictive algorithms are functioning as senseless machines and that results in false decision-making. Then, due to the opacity of the automated systems, the human decision-makers cannot justify the system's decision. Hence, the applicants are deprived of their right to information.[24]

Ultimately, the border is no longer simply a line on a map. Increasingly, it has become an ongoing process, one that begins quietly collecting a traveller's data, checking their identity and weighing the risk they may pose long before they ever set foot on EU territory. This shift in what a border does, and where it happens, does not occur in a legal vacuum. Each of the tools described so far, from biometric identification to automated

[20] Regulation (EU) 2019/817 of the European Parliament and of the Council, on interoperability between EU information systems in the field of borders and visa, 20 May 2019, in OJ L 135, 22 May 2019, p. 27; Regulation (EU) 2019/818 of the European Parliament and of the Council, on interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, 20 May 2019, in OJ L 135, 22 May 2019, p. 85.

[21] E. HOFFBERGER-PIPPAN, *The Interoperability of EU Information Systems and Fundamental Rights Concerns*, in *Spanish Yearbook of International Law*, 2019, 23, pp. 426-450.

[22] C. BLASI CASAGRAN, *Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU*, in *Human Rights Law Review*, 2021, no. 2, pp. 433-457.

[23] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, see https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

[24] A. ANDREOU, *e-Securing the EU Borders: AI in European Integrated Border Management*, in *Journal of Politics and Ethics in New Technologies and AI*, 2023, no. 1, https://doi.org/10.12681/jpentai.34287.

risk-scoring and algorithmic profiling, operates within, and is meant to be constrained by, a body of EU law that was not always designed with these specific technologies in mind.

From a regulatory perspective, no single legal instrument governs the digitalisation of EU borders, as the next section explores in detail. What applies instead is a patchwork of several layers of EU law, each developed on its own timeline and for its own purposes, that now overlap and interact in practice. The EU Charter supplies the constitutional baseline; the EU's general data protection regime governs how personal information may be processed; the EU's AI Act layers a risk-based regulatory model on top of both; and a considerable body of sector-specific legislation, covering migration, asylum, border management and large-scale information systems such as Eurodac, SIS, VIS, EES and ETIAS, fills in the operational detail. Interoperability between these systems, together with the shared involvement of national authorities and EU bodies such as eu-LISA and Frontex, adds a further layer of complexity to an already crowded field.

That fragmentation matters most from a fundamental rights standpoint. Each regulatory layer has its own safeguards, covering data processing, transparency, proportionality, non-discrimination and human oversight, but none, on its own, accounts for the cumulative risk created when biometric technologies, interconnected databases and algorithmic decision-making operate together. Identifying which instrument applies to a given technology or processing operation is only half the problem; the harder question is whether these regimes, taken together, add up to protection that is effective and coherent. The EU's digital border is growing more technologically integrated year by year, however the legal safeguards meant to constrain it have not kept pace.

3. A patchwork of rules: the EU legal framework governing AI in migration control

Nowadays, border management in the EU is governed by a patchwork of legal and otherwise regulatory instruments, encompassing European primary law sources, namely the Treaties – Treaty on European Union (TEU) and Treaty on the Functioning of the European Union (TFEU) –, and the EU Charter. While Article 3(2) TEU states the essence thereof, namely that the "Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime", Title V TFEU on the AFSJ further specifies a common policy on asylum, immigration and external border control, all of which must conform to the EU Charter; under Article 51(1) of the Charter, Member States are bound by its provisions when implementing EU law.[25]

Secondary law sources, such as regulations, directives and (implementing) decisions, also play a role in framing EU border management policy. This includes, first and foremost, a legal statute for each border management tool, ranging from Schengen

[25] E. SPAVENTA, *Fundamental Rights in the European Union*, in C. BARNARD, S. PEERS (eds.), *European Union Law*, 4th ed., Oxford, 2023, pp. 242-283.

through large-scale databases and their interoperability, the Passenger Name Record (PNR) Directives, the Advanced Passenger Information (API) Directive, the European Border Surveillance System (Eurosur), the rules governing the European bodies and agencies, the rules governing border control of persons crossing the external borders of the Member States of the Union – contained in the Schengen Borders Code (SBC) –, to identity cards and passports, unmanned air vehicles, dual-use, etc.[26]

In addition to EU law, Member States are bound by public international law instruments, e.g. bilateral agreements, treaties and conventions, such as the 1950 European Convention on Human Rights, the 1951 Geneva Convention, and the 1967 Protocol Relating to the Status of Refugees. National laws play a role insofar as certain matters, directly or indirectly linked to border management, such as intelligence, military and internal security, are the exclusive competence of Member States.[27]

In addition, soft law instruments, such as internal policies and practices of border authorities and memoranda of understanding concluded between border control authorities of neighbouring countries, also come into play in the formation of policy. Finally, several technical standards fixed for biometric data contained in passports – International Civil Aviation Organisation (ICAO), National Institute of Standards and Technology (NIST) – set certain limitations on the implementation of border management policy.[28]

In this context of regulatory fragmentation, as we noted earlier, the European architecture for fundamental rights delineates the general framework for the use of biometrics and AI in the EU. It is marked by Article 2 and Article 6 of the TEU. Article 2 TEU states that the EU is "founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities". Article 6 TEU notably establishes the legally binding force of the EU Charter. In the Charter are recognised several rights very often perceived as being potentially negatively impacted by AI, such as the right to respect for private life,[29] the right to the protection of personal data,[30] and the right to non-discrimination.[31]

---

[26] J.P. BURGESS, D. KLOZA (eds.), *Border Control and New Technologies: Addressing Integrated Impact Assessment*, ASP Academic and Scientific Publishers, Brussels, 2021, p. 124.
[27] N. MORAG, *Border Management in Europe: Is the Paradigm Evolving?*, cit.
[28] J.P. BURGESS, D. KLOZA (eds.), *Border Control and New Technologies: Addressing Integrated Impact Assessment*, *op. cit.*
[29] Art. 7 EU Charter: "Everyone has the right to respect for his or her private and family life, home and communications".
[30] Art. 8 EU Charter: "1) Everyone has the right to the protection of personal data concerning him or her. 2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3) Compliance with these rules shall be subject to control by an independent authority".
[31] Art. 21 EU Charter: "1) Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. 2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited".

As the European Parliament's Research Service has pointed out, almost all fundamental rights recognised as EU fundamental rights in the EU Charter are potentially put at great risk by certain developments of AI. In this sense, for example, the tracking of individuals in public spaces can directly threaten the right to freedom of assembly and of association. Also, certain uses of biometric technologies could affect the right to a fair trial. Importantly, some uses of AI systems can be regarded as a threat to human dignity, for instance because they aim at substituting human free will with a computer decision.[32]

Furthermore, we must keep in mind that all EU Member States are parties to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and are therefore bound by its provisions. Although the EU itself has not yet acceded to the Convention, the ECHR nevertheless occupies a significant position within the EU fundamental rights architecture. In particular, pursuant to Article 52(3) of the EU Charter, where Charter rights correspond to rights guaranteed by the ECHR, their meaning and scope must be the same as those laid down by the Convention, without preventing EU law from providing more extensive protection. Moreover, Article 6(3) TEU provides that fundamental rights, as guaranteed by the ECHR and as they result from the constitutional traditions common to the Member States, constitute general principles of EU law.[33]

On the other hand, from the perspective of data protection in the EU, it should be noted that biometric data is governed by general data protection regulations such as the GDPR.[34] Within this framework, biometric data receive enhanced protection under EU data protection law. The GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person".[35] This definition therefore covers technologies such as facial recognition or fingerprint identification where the relevant data result from specific technical processing and allow or confirm the unique identification of an individual.

However, an important distinction must be drawn between biometric data as defined in Article 4(14) GDPR and their treatment as a special category of personal data under Article 9. Pursuant to Article 9(1), it is specifically the processing of biometric data "for

[32] EUROPEAN PARLIAMENTARY RESEARCH SERVICE (EPRS), SCIENTIFIC FORESIGHT UNIT (STOA), *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics in the Era of Artificial Intelligence*, European Parliament, PE 697.191, December 2021, pp. 22-23.

[33] E. SPAVENTA, *Fundamental Rights in the European Union*, *op. cit.*, pp. 242-283.

[34] It is important to note that the three major instruments of EU data protection law -the GDPR, the LED and the EU DP Regulation- have been adopted exclusively on the basis of Article 16 of the TFEU, this provision states that "1) Everyone has the right to the protection of personal data concerning them. 2) The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union".

[35] Regulation (EU) 2016/679 (GDPR), Art. 4(14); see also Art. 9(1).

the purpose of uniquely identifying a natural person" that falls within the special categories of personal data and is, as a general rule, prohibited. The distinction is significant because not every processing operation involving an image or a physical or behavioural characteristic of an individual necessarily triggers the enhanced protection provided by Article 9. As the European Data Protection Board (EDPB) has clarified, ordinary video footage does not in itself constitute the processing of biometric data for the purposes of Article 9. Rather, the nature of the data, the specific technical processing applied to them and, crucially, the purpose for which they are processed must be taken into consideration.[36] The prohibition established by Article 9(1) GDPR is not absolute. Article 9(2) sets out a few circumstances in which the processing of special categories of personal data may exceptionally be permitted. In addition, Article 9(4) allows Member States to maintain or introduce further conditions, including limitations, concerning the processing of genetic, biometric and health data. The processing of biometric data must, in any event, comply with the general principles laid down in Article 5 GDPR, including lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. These principles acquire particular importance in the context of biometric identification, given both the sensitive nature of the information involved and the potentially serious consequences resulting from inaccurate or excessive processing.[37]

The GDPR does not, however, constitute the only applicable data protection regime. Where biometric data are processed by competent national authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties or the safeguarding against and prevention of threats to public security, Directive (EU) 2016/680 (Law Enforcement Directive – LED –) applies. Article 10 LED subjects the processing of genetic and biometric data for the purpose of uniquely identifying a natural person to a particularly demanding standard since such processing is permitted only where it is strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and where it is authorised by Union or Member State law, necessary to protect vital interests, or concerns data manifestly made public by the data subject.[38] The Court of Justice of the European Union (CJEU) has reinforced the restrictive character of this provision, notably in *Ministerstvo na vatreshnite raboti*, holding that the systematic collection of biometric and genetic data cannot dispense with

[36] EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 3/2019 on processing of personal data through video devices*, Version 2.0, adopted 29 January 2020, paragraphs 74-82, https://www.edpb.europa.eu/documents/guideline/guidelines-32019-on-processing-of-personal-data-through-video-devices_en.

[37] EUROPEAN PARLIAMENTARY RESEARCH SERVICE (EPRS), SCIENTIFIC FORESIGHT UNIT (STOA), *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics in the Era of Artificial Intelligence*, *op. cit.*, p. 24.

[38] Directive (EU) 2016/680, Art. 10. For an analysis of the processing of biometric data under the LED, see S. FANNI, *The Biometric Habeas Data in the Digital and Algorithmic Era in the European Union*, in *Latin American Journal of European Studies*, 2023, no. 2, pp. 18-47.

an assessment of whether such processing is strictly necessary in the individual circumstances concerned.[39]

A third regime applies where the processing is carried out by EU institutions, bodies, offices and agencies. Regulation (EU) 2018/1725 provides the general data protection framework applicable to them and follows an approach broadly comparable to that of the GDPR. In particular, Article 10 treats biometric data processed for the purpose of uniquely identifying a natural person as a special category of personal data whose processing is, in principle, prohibited, subject to the exceptions expressly provided for by the Regulation.[40] This framework is particularly relevant in the field of EU migration and border governance because EU bodies and agencies participate, to varying degrees and within their respective legal mandates, in an increasingly data-intensive system of border management.[41]

The resulting legal framework is therefore not based on an absolute prohibition of biometric processing. Rather, EU data law establishes a system of enhanced safeguards whose precise application depends on the identity of the controller, the purpose of the processing and its legal basis. This distinction is particularly relevant in the migration and border control context, where biometric technologies are increasingly embedded in large-scale EU information systems and may be used for identification, verification, security and migration-management purposes. Consequently, determining whether a particular biometric operation is compatible with EU data protection law requires not only identifying the applicable legal instrument, but also examining the specific purpose pursued, the necessity and proportionality of the processing, the safeguards provided to the data subject and the sector-specific legal framework governing the information system concerned.

In any case, we must acknowledge that automated decision-making is where EU data protection law meets AI most directly. Article 22(1) GDPR gives individuals a right not to be subject to a decision based solely on automated processing, profiling included, whenever that decision produces legal effects for them or affects them in a similarly significant way.[42] The GDPR allows such decisions only in three narrow circumstances, namely where they are necessary for entering into or performing a contract, where Union or Member State law authorises them subject to appropriate safeguards, or where the data subject has given explicit consent.

When a decision rests on contractual necessity or explicit consent, Article 22(3) obliges the controller to put suitable measures in place to protect the individual's rights,

[39] *Ministerstvo na vatreshnite raboti* (*Recording of biometric and genetic data by the police*) (2023) CJEU C-205/21, ECLI:EU:C:2023:49, see para. 127.
[40] Regulation (EU) 2018/1725, Art. 10.
[41] See A. VALDIVIA ET AL., *Neither Opaque nor Transparent: A Transdisciplinary Methodology to Investigate Datafication at the EU Borders*, in *Big Data & Society*, 2022, no. 2, pp. 1-17.
[42] This question has been addressed by S. FANNI, *Me, my face and AI: la protección de los derechos de los migrantes y el reconocimiento facial*, in C. VILLEGAS DELGADO, E. TÉLLEZ CARVAJAL (eds.), *La protección de los Derechos Humanos en América latina y Europa en la era digital*, Tirant lo Blanch, 2024, pp. 233-268.

freedoms and legitimate interests, measures that must include, at the very least, the possibility of obtaining human intervention, expressing one's own view and contesting the decision. Biometric technologies raise this concern with particular force, since Article 22(4) goes further still and restricts automated decisions based on the special categories of personal data listed in Article 9(1); such data may be used only where the specific exceptions in Articles 9(2)(a) or 9(2)(g) apply, and only with appropriate safeguards in place.

That protection should not be overstated, though. It applies only under real conditions, most importantly that the decision must be based solely on automated processing and must produce legal effects or a similarly significant impact. The GDPR, moreover, does not govern every form of personal data processing relevant to migration, security and border control, and the parallel rules under the LED[43] are not the same. Article 22 is therefore a real safeguard against certain kinds of automated decision, but not, on its own, a comprehensive legal framework for every AI-assisted decision capable of affecting individuals within EU migration and border governance.

Finally, the adoption of the AI Act[44] layers a further set of rules on top of the protection EU data protection law already provides. Article 22 GDPR applies only where its own conditions on automated individual decision-making are met. The AI Act works differently. Its broader, risk-based approach reaches the development, deployment and use of AI systems as such, together with the risks these may pose to health, safety and fundamental rights.

Migration, asylum and border control fall squarely within its reach. Under Article 6(2) and point 7 of Annex III, certain AI systems used by or on behalf of competent public authorities in these areas count as high-risk. Subject to the conditions the Regulation sets out, the category covers systems intended to assess the risk posed by persons entering or seeking to enter the territory of a Member State, to assist competent authorities in examining applications for asylum, visas or residence permits and related complaints, and to detect, recognise or identify persons in the context of migration, asylum and border-control management.[45]

Not every AI system deployed in these fields is automatically caught, however. Article 6(3) allows systems listed in Annex III to fall outside the high-risk category where they pose no significant risk of harm to the health, safety or fundamental rights of natural persons and do not materially influence the outcome of decision-making, provided the

[43] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[44] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act), OJL, 2024/1689, 12 July 2024.
[45] Regulation (EU) 2024/1689, Art. 6(2).

Regulation's conditions are satisfied. That derogation has a firm limit. An Annex III system that performs profiling of natural persons is high-risk in every case.[46]

Where an AI system used in migration, asylum or border control falls within the high-risk categories established by Article 6(2) and Annex III, the AI Act provides for a specific set of requirements concerning, *inter alia*, risk management, data and data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity.[47] What is at stake in migration and border control gives these requirements real weight, since AI-supported assessment may feed into decisions that carry serious consequences for the individual, among them access to territory, international protection or residence. Following the amendments introduced by Regulation (EU) 2026/1744 (*Digital Omnibus on AI*), however, the application of Sections 1, 2 and 3 of Chapter III to these Annex III high-risk systems has been deferred until 2 December 2027.

In this regard, we consider that the postponement is particularly significant in the migration and border-control context, since it delays the application of some of the AI Act's most important *ex ante* fundamental-rights safeguards precisely in an area in which algorithmic assessments may have particularly serious consequences for individuals.

In any case, the AI Act therefore complements the existing data protection framework rather than replacing it. The GDPR, the LED and Regulation (EU) 2018/1725 govern the processing of personal data within their respective scopes, while the AI Act addresses the wider risk that attaches to AI systems across their development and use. A single technological operation can fall under both regimes at once. Nowhere does this matter more than in EU migration and border governance, where AI systems operate in increasingly data-intensive settings built on biometric information, large-scale information systems and automated or AI-assisted assessments.

As we have seen in this section, AI at the EU's borders does not operate in a legal vacuum. It operates, rather, inside a dense and multi-layered regulatory framework in which the EU Charter, EU data protection law, the AI Act and sector-specific migration and border legislation all bear on the same practices. Between them, these instruments lay down real safeguards, covering the processing of personal and biometric data, automated decision-making, transparency, human oversight, necessity and proportionality.

A dense framework, however, is not the same thing as effective protection. In other words, we can say that, from a technological standpoint, the EU's border is being consolidated into a single system, but from a legal standpoint, it continues to be regulated in a fragmented manner. The question worth asking is therefore no longer whether AI and biometric technologies in migration and border control are regulated at all. They plainly are. It is whether the framework that regulates them delivers effective protection when those technologies bear, directly or indirectly, on people already in particularly vulnerable situations – especially in the case of asylum seekers and refugees. That question cannot

[46] Regulation (EU) 2024/1689, Art. 6(3).
[47] Regulation (EU) 2024/1689, Arts. 9-15.

be answered from the architecture alone. It requires looking at what these technologies actually do to the rights of the people subject to them. Some of those rights, and the ways in which they may be put at risk by biometric identification, algorithmic profiling and AI-assisted decision-making, will be examined in the next section. Particular attention will be paid to the fact that these risks rarely arise in isolation, but may accumulate and reinforce one another throughout the migration and border-control process.

4. Fundamental rights at risk

It is precisely at this point that regulatory fragmentation becomes a fundamental rights concern. The adequacy of the legal framework must ultimately be tested against its capacity to protect those most exposed to AI-assisted border control. This is particularly evident in the case of asylum seekers and refugees, for whom technologically mediated assessments may have immediate and potentially irreversible consequences.

The technologies described in the preceding section 2 of this article feed directly into that assessment. Eurodac's facial-matching capability, the risk indicators embedded in the ETIAS screening algorithm, and the profiles Frontex compiles before a traveller has even boarded a flight each generates an input that an official weigh – consciously or not – in determining whether an individual is granted entry, receives a fair hearing, or is removed. Where the AI-ethics literature more generally tends to treat a wrongly flagged case as productive of delay, or as remediable on appeal,[48] the consequence in this context may be removal to the country from which the individual fled. Once executed, that outcome cannot be reversed.

In the context of border management, the use of AI and facial recognition technologies may interfere with a broad range of fundamental rights.[49] The analysis that follows is not intended to provide an exhaustive account of all the fundamental rights potentially affected by these technologies, but rather to examine several particularly relevant examples that illustrate the risks arising from their use in migration and border control. Attention will therefore be paid to respect for private life and the protection of personal data, non-discrimination, the rights of the child, the right to asylum and the principle of non-refoulement and, finally, the right to an effective remedy. These rights are treated separately below for analytical clarity, although in practice they are rarely engaged in isolation. A single erroneous risk score may simultaneously misuse the personal data on which it is based, encode a pattern that discriminates on grounds of

[48] See, e.g., D.K. CITRON, F. PASQUALE, *The Scored Society: Due Process for Automated Predictions*, in *Washington Law Review*, 2014, no. 1, pp. 1-33, available at SSRN: https://ssrn.com/abstract=2376209.

[49] Much has been written about the impact on fundamental rights of the processing of biometric data, of AI in general, and of AI enabled by biometrics more particularly –especially of facial recognition. See, for instance, I. NESTEROVA, *Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world*, SHS Web of Conferences, Vol. 74, EDP Sciences, 2020. For a study focusing on the European Union situation, see FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, *op. cit.*

nationality or route of travel, and foreclose the fair hearing that might otherwise have identified the error.

The rights to respect for private life and data protection are central to the deployment of facial recognition technology in public places. Although the two are closely related, they are distinct, self-standing rights. They have also been described as the "classic" right to the protection of privacy and a more "modern" right, the right to data protection.[50] Both strive to protect similar values, i.e. the autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely develop their personalities, think and shape their opinions. They thus form an essential prerequisite for the exercise of other fundamental rights, such as the freedom of thought, conscience and religion (Article 10 EU Charter), freedom of expression and information (Article 11 EU Charter), and freedom of assembly and of association (Article 12 EU Charter).[51]

Using live facial recognition technologies implies collecting, comparing and storing facial images in an IT system for identification purposes. It, therefore, constitutes an interference with the right to protection of personal data set out in Article 8 EU Charter (embodying pre-existing EU data protection law) and the right to private life under Article 7 EU Charter and Article 8 of the ECHR. Facial images constitute personal data, as also confirmed by the CJEU[52] and the ECtHR.[53] The latter has also addressed the broader fundamental-rights implications of facial recognition technology. In *Glukhin v. Russia*, the ECtHR found violations of Articles 8 and 10 ECHR arising from the use of facial recognition technology to identify and locate a peaceful protester, concluding that its use in the circumstances of the case was incompatible with the ideals and values of a democratic society governed by the rule of law.[54]

The concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person, and can, therefore, embrace multiple aspects of the person's physical and social identity.[55] There is also a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".[56] In other contexts, the ECtHR has used the concept of "reasonable expectation of privacy" –referring to the extent to which people can expect privacy in public spaces without being subjected to surveillance– as one of the factors, albeit not necessarily a conclusive one, to decide on a violation of the right to respect for private life. Its relevance and scope of application, however, appear to be limited.[57] Similarly, according to UN experts, the mere fact that participants in assemblies are out in public

[50] CJEU, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert GbR and Hartmut Eifert, Opinion of Advocate General Sharpston*, 17 June 2010, para. 71.
[51] FRA, Council of Europe and EDPS, *Handbook on European data protection law*, 2018 edition, Luxembourg, Publications Office, June 2018, p. 19.
[52] CJEU, C-291/12, *M. Schwarz v. Stadt Bochum*, 17 October 2013, par. 22, 48-49.
[53] ECtHR, *Szabó and Vissy v. Hungary*, No. 37138/14, 12 January 2016, par. 56.
[54] ECtHR, *Glukhin v. Russia*, No. 11519/20, 4 July 2023, par. 90.
[55] ECtHR, *López Ribalda and Others v. Spain*, Nos. 1874/13 and 8567/13, 17 October 2019, par. 87.
[56] *Ibid*., par. 88.
[57] M. VERMEULEN, *Surveille Deliverable D4.7 – The scope of the right to private life in public places*, July 2014, p. 2.

does not mean that their privacy cannot be infringed.[58] The processing of facial images in large-scale databases may, as facial recognition technology develops, raise uncharted issues about the rights to protection of private life as well as of personal data. Given that these two rights are not absolute rights, they can be subject to limitations, but any interference needs to be adequately justified[59] and cannot compromise in any event the essential, inalienable core of those rights.[60]

As we have pointed out previously, a face, once captured by Eurodac, EES or VIS, is not just an image. Processed to identify a specific individual, it becomes biometric data – a category the EU Charter and GDPR treat as sensitive precisely because, unlike a password, it cannot simply be changed. The interference does not end at the camera, either. It continues through storage, through the matching software that compares that face against a watchlist or a database of millions of others, and through whatever the result of that comparison is then used to justify. Each of those steps needs its own clear legal basis, and each must survive the same test: is this necessary, and is it proportionate to what it is trying to achieve?

That test gets harder to pass once accuracy itself turns out to be unevenly distributed. Facial recognition systems do not fail at the same rate for everyone. Performance has repeatedly been shown to vary by age, sex, and ethnic origin, largely because the datasets used to train them were not evenly representative to begin with. The most widely cited demonstration of this remains a 2018 audit of three commercial gender-classification systems, which found error rates below one per cent for lighter-skinned men and as high as thirty-four point seven per cent for dark-skinned women –the same software, the same task, just pointed at different faces.[61]

As the FRA has pointed out, discrimination in data-supported algorithmic decision making can occur due to several reasons. Discrimination can occur during the design, testing and implementation of algorithms used for facial recognition, through biases that are incorporated –consciously or not– in the algorithm itself, as well as when officers decide what action to take following a match.[62] If there are differences in the performance of an algorithm, it is usually very difficult and sometimes impossible to remove the bias through mathematical or programmatic solutions.[63] An important cause of discrimination

[58] UN, Human Rights Committee, *draft General Comment No. 37 Article 21: right of peaceful assembly*, draft prepared by the Rapporteur, Christof Heyns, July 2019, para. 69.
[59] See also FRA, Council of Europe and EDPS, *Handbook on European data protection law*, 2018 edition, Luxembourg, Publications Office, June 2018, pp. 35-52.
[60] See European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence*, Strasbourg, Council of Europe, 2019, pars. 133 and 136.
[61] J. BUOLAMWINI, T. GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning Research*, 2018, 81, pp. 77-91.
[62] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, *op. cit.*
[63] FRA, *Preventing unlawful profiling today and in the future: a guide*, Luxembourg, Publications Office, December 2018, p. 26.

is the quality of data used to develop algorithms and software.[64] To operate effectively and accurately, facial recognition software needs to be trained on large datasets of facial images. More facial images lead, in principle, to more accurate predictions. However, accuracy is not only determined by the number of facial images processed but also by the quality of such facial images. Data quality requires also a representative set of faces reflecting different groups of people.[65] Yet to date, facial images used to develop algorithms in the Western world often over-represent white men, with lower numbers of women or individuals of other ethnic backgrounds. As a result, facial recognition systems worked well for white men, but not for black women.[66]

At a border, where a false match triggers further questioning or a secondary check, that statistical unevenness stops being a technical footnote and starts looking like discrimination by another name. Evaluating one of these systems on its overall accuracy alone, then, misses the point; what matters is whether that accuracy holds up across the groups it is used on.[67]

On the other hand, children raise a version of this problem that the recast Eurodac Regulation illustrates directly because it lowers the age at which a child's biometric data may be captured from fourteen to six. Article 24 EU Charter requires that the child's best interests come first in any such decision, and a six-year-old's face is, in a fairly literal sense, still changing – a technical fact that makes biometric matching less reliable over time,[68] quite apart from the separate legal question of whether registering a six-year-old's face was proportionate in the first place. None of this makes the technology indefensible in every case because facial recognition has a real role to play in finding a missing child or identifying a child victim of trafficking. But it cuts both ways, and the younger the subject, the less that cuts in favour of routine use. Children should not be put in a situation in which they would, because of their age, be disproportionately affected by the negative consequences of facial recognition technologies. The processing needs to fully respect Article 24 (rights of the child) of the EU Charter.

[64] FRA, *Data quality and artificial intelligence –mitigating bias and error to protect fundamental rights*, Luxembourg, Publications Office, June 2019.
[65] *Ibid*.
[66] J. BUOLAMWINI, T. GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, *op. cit*., pp. 1-15.
[67] See FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, *op. cit*., pp. 27-28.
[68] See B.I. MARCU, *Eurodac: Biometrics, Facial Recognition, and the Fundamental Rights of Minors*, in *European Law Blog*, 2021, 29 April. Eurodac Supervision Coordination Group (coordinated by the European Data Protection Supervisor), in a Letter to the co-legislators on the proposed recast Eurodac Regulation (March 2023), noting "unresolved concerns regarding the necessity and proportionality of this measure... in view of the evidence suggesting decreasing reliability of a fingerprint match and lower efficiency in facial recognition systems deployed on children". In other words, the EU's own data protection authority put the same technical concern in writing. Available at https://edps.europa.eu/system/files/2023-03/eurodac_scg_letter_on_eurodac_fin.pdf.

Regarding the right to asylum, Article 18 of the EU Charter states that this right "shall be guaranteed with due respect for the rules of the Geneva Convention".[69] The right to asylum is also affirmed and supported by the principle of non-refoulement under Article 19(2) of the Charter, which prohibits returning an asylum seeker to a country where they would face the death penalty, torture or other inhuman or degrading treatment.[70]

The CJEU has been notably unwilling to let this guarantee become a formality. In its 2019 judgement on the revocation of refugee status – joining proceedings from Belgium and the Czech Republic, one of them concerning an Ivorian national convicted of a serious crime – the Court confirmed that Member States may revoke or refuse refugee status on security grounds, but only where the individual poses a "genuine, present and sufficiently serious threat", a proportionality test the Court refused to let collapse into "convicted, therefore removable".[71] Even where revocation is justified, the Court held, the person does not simply stop being a refugee for Geneva Convention purposes; core protections survive the revocation itself. If an individualised threat assessment is required before EU law will let a state act on a criminal conviction –about as concrete a fact as a legal system can rely on– it sits uneasily with a system that sorts asylum seekers by an algorithmic risk score built on proxies far less concrete than a conviction.

That is where the AI Act's own architecture becomes relevant, and where its gaps start to matter. Article 5 of the AI Act does prohibit real-time remote biometric identification in public spaces, but only for law enforcement purposes and only in real time; retrospective matching against a database – precisely what Eurodac's facial-image search or a VIS lookup does – falls outside that prohibition entirely and lands instead in the high-risk category, where, as the previous section noted, the safeguard is a provider's own internal conformity assessment rather than independent scrutiny.[72] Whether a migration authority even counts as "law enforcement" for these purposes is itself unsettled, leaving considerable room for exactly the kind of profiling and risk-based surveillance the preceding sections describe to continue largely unconstrained by the prohibitions of Article 5 of the AI Act. None of this means the AI Act is being used to arrest anyone directly, but the legislation's loopholes will aid in discriminatory practices against refugees like profiling and surveillance.[73] A flawed risk indicator that funnels someone toward secondary screening, and secondary screening that leads to detention pending an asylum decision, do not need the AI Act's blessing to produce that outcome

[69] Art. 18 EU Charter: "The right to asylum shall be guaranteed with due respect for the rules of the Geneva Convention of 28 July 1951 and the Protocol of 31 January 1967 relating to the status of refugees and in accordance with the Treaty on European Union and the Treaty on the Functioning of the European Union".
[70] Art. 19(2) EU Charter: "No one may be removed, expelled or extradited to a State where there is a serious risk that he or she would be subjected to the death penalty, torture or other inhuman or degrading treatment or punishment".
[71] CJEU, Joined Cases C-391/16, C-77/17 and C-78/17, *M and Others (Revocation of Refugee Status)*, 14 May 2019.
[72] Regulation (EU) 2024/1689, Art. 5(1)(h); See also L. MATHESON, *Red Lines under the EU AI Act: Restricting Real-time Remote Biometric Identification Systems for Law Enforcement Purposes*, in *Future of Privacy Forum*, 7 April 2026.
[73] A. IBSAIS, *AI at the Borders: How the EU AI Act Can Prove to Be Incompatible with Fundamental Rights for Refugees*, in *Georgetown Journal of International Law*, 2025, 56(3), p. 747.

between them; they only need the gaps described above to go unaddressed. Detention reached by that route is not a neutral administrative consequence. It is a serious deprivation of liberty triggered, at least in part, by an automated judgement the person detained had no opportunity to contest before it was acted on[74] – an affront, in fairly direct terms, to the human dignity that Article 1 EU Charter and Article 1 of the Universal Declaration of Human Rights both treat as the foundation the rest of each instrument rests on.

Finally, we must point out that Article 47 EU Charter guarantees the right to an effective remedy before a tribunal, including a fair trial. This fundamental right of horizontal character empowers individuals to challenge a measure affecting any right conferred to them by EU law and not only in respect of the fundamental rights guaranteed in the Charter.[75] The right to an effective remedy also covers decisions taken with the support of facial recognition technologies, for example, a measure (such as a police officer stop) that has solely or significantly been informed by facial recognition.[76]

None of the rights just described in this section mean much without Article 47 behind them and that is where this entire chain tends to break down in practice. Challenging a decision requires knowing what it was based on, and a facial-recognition match, an ETIAS risk score, or an automated threat assessment sitting quietly behind an administrative outcome is exactly the kind of input a person detained or refused entry has no obvious way of finding out about, let alone contesting in the time an appeal allows.[77] Everything raised in this section – the accuracy disparities, the treatment of children, the risk to asylum seekers – converges on the same practical requirement because none of these problems can be caught, argued, or fixed unless someone outside the system can see what it did and how.

Separated for analytical clarity, the rights examined in this section are engaged at the border as a single sequence. A face is captured and matched, a score is produced, an officer acts on it; at each step a different right is in play, and the person concerned is usually the last to find out. Whatever these systems achieve in aggregate, each error has to be contested one person at a time, and only by someone who knows it was made. The test set at the outset was whether the legal framework can protect those most exposed to AI-assisted border control, and on the evidence reviewed here it does not yet do so consistently. The shortfall is clearest in the right to an effective remedy, which comes last on the list but carries more weight than its position suggests. Scrutiny has to reach the

[74] See UN Working Group on Arbitrary Detention, *Report of the Working Group on Arbitrary Detention*, UN Doc. A/HRC/45/16, 24 July 2020, paras. 57-60. No case of detention traceable directly to an algorithmic decision has yet reached the Working Group, but its approach to modern technologies in other contexts offers useful guidance.

[75] See EU Network of Independent Experts on Fundamental Rights, *Commentary on the Charter on Fundamental Rights of the European Union*, June 2006, p. 360.

[76] Council of Europe Commissioner for Human Rights, *Unboxing Artificial Intelligence: 10 steps to protect Human Rights – Recommendation*, Council of Europe, Strasbourg, May 2019, p. 13.

[77] A. THOMMANDRU ET AL., *Algorithmic Profiling and Facial Recognition in EU Border Control: Examining ETIAS Decision-Making, Privacy and Law*, in *WIREs Data Mining and Knowledge Discovery*, 2025, 15, https://doi.org/10.1002/widm.70013.

match, the score and the risk indicator before they harden into a decision, because for someone removed to the country they fled, a remedy that comes afterwards comes too late.

5. Algorithmic decision-making and migrant vulnerability

Article 22 GDPR and Article 11 LED prohibit, as a general rule, automated decision-making, meaning any "decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". The prohibition lifts only where Union or Member State law authorises it and builds in safeguards for the data subject's rights and freedoms, starting with the right to obtain human intervention from the controller.[78] Where special category data is involved – facial images among them – the controller must additionally put in place suitable measures safeguarding the data subject's rights, freedoms and legitimate interests. Every trial and deployment planned across EU Member States builds in this kind of human intervention. In practice, a facial-recognition match is flagged to a human operator – typically a police officer – who reviews it and decides how to act. Many false positives are already ruled out at this stage.

But what counts as "automated" is harder to pin down than it sounds, and the question deserves more scrutiny than it has had so far. If human intervention amounts to little more than signing off on whatever the system outputs, the decision stays automated in substance, whatever name is attached to it.[79] The opposite case – an officer who genuinely reviews the match and can override it – looks different on paper, but raises a problem of its own, one well worth examining.

The available research suggests that officers tend to overrule an algorithm precisely when doing so lines up with their own stereotypes, which again tends to disadvantage minority groups. That pattern erodes the one thing automated processing was supposed to offer: a check that could, at least in principle, be more accurate – and sometimes fairer – than human judgement on its own.[80]

On the other hand, technological advances have enabled the development of profiling algorithms that rely on correlations and patterns in data. Profiling refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, personal

[78] See FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, *op. cit.*, p. 26.
[79] M. VEALE, L. EDWARDS, *Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling*, in *Computer Law & Security Review*, 2018, no. 2, pp. 398-404.
[80] B. GREEN, Y. CHEN, *Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments*, in *Proceedings of the Conference on Fairness, Accountability, and Transparency* (FAT '19), 2019, pp. 90-99.

preferences, interests, reliability, behaviour, location or movements – Article 4(4) GDPR. Profiling is a legitimate tool used by law enforcement officers and border guards to prevent, investigate and prosecute criminal activity, as well as to prevent and detect irregular immigration.[81]

However, we must remember that profiling based on special categories of data, including biometric data for the purpose of uniquely identifying a natural person, is exceptionally allowed if adequate fundamental rights safeguards are put in place and if it does not lead to discrimination. One safeguard provided by the LED in the context of profiling is the right to obtain human intervention on the part of the controller (Article 11). Such a "human-in-the-loop" safeguard, however, may be weakened in practice by automation bias – the fact that human operators tend to defer to automated systems (especially when in doubt) when taking decisions.[82] Another safeguard concerns the right of data subjects to receive an explanation of the decision. Such a right to explanation, which is mentioned only in the recitals of the GDPR and the LED,[83] has been intensely debated in association with opaque AI applications (black boxes). Given that there are no explicit legal provisions on this right to an explanation or any relevant jurisprudence, the scope of this right remains unclear.[84]

For asylum seekers and refugees, though, the picture gets more complicated still. Where automated decision-making and data collection lead to heightened scrutiny, harassment, higher rejection rates or transfers, the fallout can bear directly on whether someone secures international protection at all. That is precisely what makes it worth asking what additional safeguards are supposed to exist for this group –and whether they actually hold up in practice. In *Aranyosi and Căldăraru v. Generalstaatsanwaltschaft Bremen*, the CJEU emphasised that human dignity must be considered even in cases of surrender under the European Arrest Warrant, where one cannot be surrendered if they would be subject to "inhuman or degrading treatment".[85] The safeguard of "human dignity" is reduced by the AI Act's exemptions, which enable automation in a system where discrimination is already rampant – at EU airports, for instance, many respondents in a study believed that secondary screening occurred because of their race, appearance, or religious beliefs.[86] This higher rate of discrimination occurs in the public context of travelling, where other travellers can observe discrimination taking place. Without any

[81] C. DUMBRAVA, *European Parliamentary Research Service. Artificial intelligence at EU borders: Overview of applications and key issues*., *op. cit*., p. 29.
[82] L.L. SKITKA, K.L. MOSIER, M. BURDICK, *Does Automation Bias Decision-Making?*, in *International Journal of Human-Computer Studies*, 2000, no. 5, pp. 991-1006.
[83] See GDPR, recital 71: "the right ... to obtain an explanation of the decision reached"; see also LED, recital 38: "right to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision".
[84] FRA, *Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security*, 2017, p. 44. For a more detailed discussion, see G. SARTOR, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, European Parliamentary Research Service (EPRS), European Parliament, 2020.
[85] CJEU, Joined Cases C-404/15 and C-659/15 PPU, *Aranyosi and Căldăraru*, 5 April 2016, par. 91.
[86] FRA, *Dignity: Fundamental Rights at Airports: Border Checks at Five International Airports in the European Union*, Publications Office of the European Union, Luxembourg, 2014, pp. 49, 122.

oversight, in a private setting, concerning an already vulnerable population, we must assume that AI will only exacerbate the already existing discrimination. The impact of this discrimination may cause increased denial of asylum applications, forcing vulnerable communities to either face irregular status in a safer country or return to an environment where inhuman treatment is more likely to occur.[87]

The Asylum Procedures Directive also places nominal protections as it requires "individual, objective" examination.[88] As stated, the AI Act permits automation and data capture in a system that relies on skewed data without doing individual examination.[89] Studies find that error rates for dark-skinned individuals are significantly higher than those for light-skinned individuals in biometric identification systems.[90] Like other data-driven AI tools, biometric identification systems use a database of known identities.[91] As Ahmad Ibsais has pointed out, the AI Act will create dangerous conditions, seeing that most asylum seekers in the EU have been those from Africa and the Middle East, who typically will have a different complexion not common in biometric galleries.[92]

Every safeguard traced in this section shares the same fault line. What looks like meaningful human judgement dissolves under scrutiny – automation bias, a rubber-stamped "human in the loop", or an AI Act exemption drafted with someone else's face in mind. For refugees and asylum seekers, that fault line runs beneath human dignity itself, the one value the CJEU has refused to treat as negotiable even in surrender proceedings. When the system reviewing their claim was never built to see them clearly, the "individual, objective" examination the law promises is not being denied to them – it was never on offer.

It is precisely against this background that the AI Act must be assessed. If the risks identified above arise not merely from the use of AI itself, but from the conditions under which automated outputs enter decisions affecting migrants and asylum seekers, the crucial question is whether the new regulatory framework can translate fundamental rights protection into effective safeguards. The next section therefore examines the extent to which the AI Act responds to these concerns, and where its risk-based approach may still leave significant gaps in protection.

---

[87] A. IBSAIS, *AI at the Borders: How the EU AI Act Can Prove to Be Incompatible with Fundamental Rights for Refugees*, *op. cit.*, p. 751.

[88] 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 (Asylum Procedures Directive), OJ L 180, 29 June 2013, Art. 10.

[89] K. MOSENE, *One Step Forward, Two Steps Back: Why Artificial Intelligence Is Currently Mainly Predicting the Past*, in *Humboldt Institute for Internet and Society*, 15 October 2024.

[90] J.J. BUOLAMWINI, T. GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, *op. cit.*, pp. 77-91.

[91] AMNESTY INTERNATIONAL, *Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing*, 26 January 2021. Available at https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.

[92] A. IBSAIS, *AI at the Borders: How the EU AI Act Can Prove to Be Incompatible with Fundamental Rights for Refugees*, *op. cit.*, p. 751.

6. The EU AI Act and migration control

The adoption of the AI Act marks a genuine turning point in how AI is regulated in migration and border management. Member States were already bound by EU fundamental rights and data protection law when developing or deploying AI-based technologies in this field, but the Act is the first attempt to build a framework addressing specifically the risks that AI itself introduces. The regulation is unusually candid about why this matters, acknowledging that AI systems used in migration, asylum and border control reach people who are often particularly vulnerable, and whose rights may depend directly on the decisions of the authorities administering these systems.[93] The Act is best read, then, not as a replacement for the existing legal framework but as a new layer laid on top of it, addressing risks that framework was never designed to catch.

At the centre of that new layer sits a risk-based model, where an AI system's obligations track its classification. Correct classification is close to a *condicio sine qua non* for the Regulation's fundamental-rights strategy, since most substantive obligations bind only high-risk systems, and nowhere does that matter more than in migration and border management, where AI ranges from routine administrative processing to decisions on asylum, visas or residence permits. Whatever protection the Regulation offers a migrant depends, first, on whether their case falls within its scope at all, and only then on what level of risk gets attached to it.[94]

Being named in Annex III does not settle that question on its own. Article 6(3) carves out a *de minimis* exception, under which an Annex III system can avoid the high-risk label where it poses no significant risk to health, safety or fundamental rights, including by not materially influencing a decision's outcome, provided it does not perform profiling. That flexibility comes at a price. The initial call on whether a system qualifies is left largely to providers themselves, opening a real possibility that systems capable of affecting fundamental rights slip past the high-risk safeguards altogether – so how well the Regulation protects anyone depends not only on what those safeguards require, but on how carefully, and how honestly, that classification is made.[95]

As we have pointed out in section 3 of this article, even a system correctly classified as high-risk, though, is not yet bound by any of this in practice. On 24 July 2026, Regulation (EU) 2026/1744, the Digital Omnibus on AI, was published and entered into force three days later, amending Article 113 of the AI Act to defer the application of Chapter III's high-risk obligations for standalone Annex III systems, migration included, from 2 August 2026 to 2 December 2027. Until that date, an immigration authority implementing a high-risk system is not subject to any of the safeguards set out in the AI Act – that is to say, neither the fundamental rights impact assessment, nor the conformity

[93] M.P. AMOROSO, *Intelligent Borders: Exploring the Suitability of Artificial Intelligence Systems in Refugee Status Determination Under International Law*, in *Refugee Survey Quarterly*, 2024, 43(4), p. 411.
[94] L.S. STEWART, *The Regulation of AI-Based Migration Technologies under the EU AI Act: (Still) Operating in the Shadows?*, in *European Law Journal*, 2024, nn. 1-2, p. 126.
[95] L.S. STEWART, *The Regulation of AI-Based Migration Technologies under the EU AI Act: (Still) Operating in the Shadows?*, *op. cit.*, pp. 127-128.

assessment regime, nor even registration in the database. The Commission justified the delay by pointing, *inter alia*, to the delayed availability of harmonised standards, common specifications and alternative guidance, as well as delays in establishing the competent national authorities – genuine implementation problems, but ones whose cost, in the meantime, once again falls on the individuals against whom these systems are used.[96]

Where a system is classified as high-risk, the regime tightens considerably. Under Articles 9 to 15, providers face obligations on risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity – particularly the Article 9 requirement to run a risk-management system across the AI system's whole lifecycle, identifying known and reasonably foreseeable risks to health, safety and fundamental rights. In migration and border management these obligations are not abstract. Deficiencies in training data, biometric misidentification, algorithmic bias or thin human oversight translate directly into decisions with real consequences, and the high-risk regime is meant to catch these problems before they materialise, working as prevention rather than cure.

Whether it manages to do so is another matter, since the effectiveness of these safeguards leans heavily on discretion left to providers. Several key obligations turn on open-ended language – what counts as "appropriate", "adequate" or "proportionate" data, accuracy or oversight is left largely undefined, and providers, in practice, decide for themselves. Some of that flexibility is defensible, since technology moves faster than legislators can specify, but it costs legal certainty and enforceability, especially where private companies build systems that public authorities use to make decisions bearing directly on fundamental rights, and the judgement calls about whether a safeguard is adequate end up resting with the very actor that built and sells the technology.[97] Nor does responsibility sit with one actor alone. Article 3(3) and (4) distinguish providers from deployers, and the AI Act spreads obligations accordingly, addressing providers under Article 16 and deployers under Article 26. In a typical migration scenario, a private company supplying the system is the provider, and the public authority using it is the deployer – a division that can let responsibility slip through the cracks between designer and user, especially where public authorities lack the technical capacity to build these systems themselves and depend on private providers instead. Meaningful accountability requires that responsibility survive that handover, holding together across the designer, the deploying authority, and the official who ultimately relies on the system's output.

Article 27 addresses part of this gap. Deployers of certain high-risk systems must now carry out a fundamental rights impact assessment before deployment, since technical conformity alone cannot predict what a system will do once embedded in a real institutional setting. Stewart notes the final text is weaker than what the European

[96] EUROPEAN COMMISSION, *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)*, COM (2025) 836 final, Brussels, 19 November 2025.

[97] L.S. STEWART, *The Regulation of AI-Based Migration Technologies under the EU AI Act: (Still) Operating in the Shadows?*, *op. cit.*, pp. 129-130.

Parliament had pushed for, particularly on transparency and stakeholder participation.[98] Transparency is where the Regulation's limits show most starkly. The AI Act creates a public database for high-risk systems, but carves out law enforcement, migration, asylum and border management entirely. Under Article 49(4), these systems sit in a non-public section visible only to the Commission and national authorities – the systems most capable of harming vulnerable people face the least scrutiny. Migrants, lawyers and researchers lose the basic ability to know which systems are even in use. The conformity-assessment regime shares this weakness. Article 43 requires a provider to show its system meets the Regulation before reaching the market, but this comes down, in most cases, to internal self-assessment under Annex VI; independent review by a notified body is mandatory only in limited cases, chiefly real-time biometric identification. A provider certifying its own compliance blunts the mechanism's preventive value – and here, an error that slips through can later shape someone's access to territory or claim to protection.

Ex post supervision matters correspondingly more given how much rests on self-assessment upfront. How well this works depends on market-surveillance authorities' capacity to scrutinise complex systems against fundamental rights implications. Stewart flags two obstacles: on the one hand, enforcement left to national authorities risks uneven protection, and, on the other, effective supervision demands resources and expertise spanning both AI and fundamental rights.[99]

The AI Act also provides affected individuals with new tools – deployers of certain Annex III systems must disclose their use, and people can request an explanation under Article 86 or lodge a complaint under Article 85, a real step up from the Commission's original proposal. Whether this amounts to much here is another matter: migrants already face serious obstacles accessing information and representation, obstacles that harden against a system that is technically complex and, by design, opaque. What matters is not whether the AI Act formally provides redress, but whether someone can understand, contest, and have the decision that affected them reviewed.

Taken together, everything this section has traced is a regulation that keeps finding new ways to ask less of itself exactly where migration is concerned: a *de minimis* exception providers apply to themselves, a compliance deadline pushed back by sixteen months, a database closed to the public, a conformity check the provider signs off on alone. None of that is unlawful. All of it is, on its own terms, working as designed. That is the problem the section that follows takes up. Compliance with the AI Act, even full compliance, was never built to guarantee that a migrant's rights are respected – only that a box has been checked. The following section considers what would have to change for those two things to start meaning the same thing.

[98] *Idem*, p. 131.
[99] *Idem*, pp. 133-134.

7. Beyond compliance and towards a fundamental rights-based model of AI migration governance

A fundamental rights-based model of AI governance in border management does not require scrapping the AI Act's architecture, only closing the discretion it leaves at the exact points where caution matters least to the actors exercising it. Concretely, that means a classification decision that cannot be left to the party with an interest in getting it wrong. It requires a conformity check with an eye outside the company that built the system. It demands transparency that reaches the people capable of using it, not only the regulator. It takes a right of redress that survives a detention centre and a language barrier. It calls for responsibility that travels with the system all the way through. And it presupposes that a compliance deadline sixteen months away is no licence, in the meantime, to operate as though none of this applied. This section takes up each of these junctures.

Regarding self-classification, the most direct fix targets the *de minimis* exception under Article 6(3), since a provision that lets providers decide for themselves whether their own system "materially influences" a decision is, in practice, an invitation to classify downward.[100] A narrower reading might still make sense for genuinely low-stakes tools, but for anything touching migration, asylum or border decisions, that initial call should not rest with the party that stands to gain from getting it wrong. Requiring an independent body – the national market-surveillance authority, or a dedicated unit within it – to confirm or reject a provider's self-classification before deployment would cost little in administrative terms and close what is otherwise the widest door out of the high-risk regime altogether.

In relation to self-assessment, the same logic applies further along the pipeline, where Annex VI leaves conformity assessment almost entirely to the provider and reserves independent, notified-body review under Annex III (1) alone.[101] The regulation already treats vulnerability as a reason to escalate scrutiny elsewhere in its text; there is no obvious reason migration and asylum systems, which meet that description as squarely as any use case in Annex III, should be left outside that logic. Extending mandatory third-party conformity assessment to high-risk systems used in this field specifically would not require rewriting the Regulation's architecture, only widening a category it already recognises.

On the other hand, the blanket carve-out for law enforcement, migration, asylum and border systems under Article 49(4) does not have to mean choosing between full public disclosure and none at all.[102] A structured middle tier – access for the European

[100] Regulation (EU) 2024/1689, Art. 6(3).
[101] N. VAVOULA, *Regulating AI at Europe's Borders: Where the AI Act Falls Short*, in *Verfassungsblog*, 13 December 2024, DOI: 10.59704/10a27137a898fa42. Available at https://verfassungsblog.de/regulating-ai-at-europes-borders/.
[102] E. BROUWER, *EU's AI Act and Migration Control: Shortcomings in Safeguarding Fundamental Rights*, in *Verfassungsblog*, 12 December 2024, DOI: 10.59704/a4de76df20e0de5a. Available at https://verfassungsblog.de/eus-ai-act-and-migration-control-shortcomings-in-safeguarding-fundamental-rights/.

Ombudsman, the Fundamental Rights Agency, and accredited researchers or civil-society organisations under confidentiality terms, rather than the general public – would preserve whatever operational-security justification the exclusion originally had, while giving the people whose job it is to scrutinise these systems something to scrutinise. As matters stand, the actors best placed to catch a problem cannot see far enough into the system to look for one.

With respect to redress, the gap is not that Articles 85 and 86 fail to give an affected person the right to a complaint and an explanation, but that a right depending on knowing one has been profiled, finding a lawyer, and doing all of this from immigration detention or before a removal deadline is a right largely on paper.[103] GDPR Article 80 already lets a data subject authorise a not-for-profit body to exercise their rights on their behalf, and several Member States go further, letting such bodies act without an individual mandate at all. Importing that model into Articles 85 and 86 – letting an NGO already working with a specific migrant, or one with recognised standing in this field, lodge a complaint or request an explanation on someone's behalf – would do more to make these rights real than any amount of redrafting their wording.

Turning to the provider-deployer gap, the obvious legislative vehicle for closing it, an EU-level liability regime spanning both, no longer exists. The Commission withdrew its proposed AI Liability Directive in February 2025, a withdrawal formalised in the Official Journal that October, leaving AI-related harm to fall back on national tort law and on the revised Product Liability Directive, which extends strict liability to software but was built for defective products reaching consumers, not for a public authority's use of a system it did not build. That gap will not close itself. Short of a new EU liability instrument, the AI Act could still address it directly, through a joint-responsibility clause requiring the deployer's fundamental rights impact assessment and the provider's technical documentation to be read together, with liability following whichever party's failure the record actually points to, rather than defaulting to whoever is easier to sue.

As for the *Digital Omnibus* gap, until December 2027 none of the above binds anyone, since no high-risk obligation under the AI Act applies to standalone Annex III systems in the meantime. That gap is not, however, a legal vacuum. The EU Charter and the GDPR were never suspended by the *Digital Omnibus*, and nothing stops a migration authority from applying the impact assessment of Article 27 or the conformity checks of Article 43 voluntarily while the formal deadline still runs. Whether any authority will do so without being required to is another question, but the case for asking them to is strongest precisely now, while technology keeps shipping and the obligations meant to accompany it do not.

Finally, and underneath all the proposals above, sits one shift more basic than any of them: treating fundamental rights as a design constraint on migration AI systems rather

[103] S. DEMKOVA, *The AI Act's Right to Explanation: A Plea for an Integrated Remedy*, in *SSRN*, 31 October 2024, DOI: 10.2139/ssrn.5010892. Available at http://dx.doi.org/10.2139/ssrn.5010892.

than a box checked once development is finished.[104] The GDPR took roughly this approach with data protection by design under Article 25, building the requirement into a system's architecture rather than bolting it on at the point of certification. Nothing in the AI Act prevents a similar principle from taking hold in migration and border management specifically; what is missing is the will to make it a starting condition rather than an afterthought, and that, more than any single article discussed above, is the gap this article has been describing all along.

8. Conclusions

Having analysed how biometric records, predictive algorithms and an increasingly interoperable database architecture have transformed EU border management, and having weighed this infrastructure against the safeguards designed to limit it, this article returns to the tension between security, efficiency and fundamental rights that motivated it. Taking up each of the objectives set out in the Introduction, it reaches the following conclusions.

The analysis showed that AI has changed the very logic of EU migration control. Large-scale IT systems such as Eurodac, SIS, VIS, EES and ETIAS, originally designed to identify individuals, have become increasingly interconnected tools of risk assessment, so that the border now operates before the traveller arrives and on the basis of probabilities attached to categories of people. The study of the legal framework revealed a body of rules that is dense but not always coherent. The EU Charter, the GDPR and the LED offer robust general guarantees, and the sectoral regulations governing each large-scale IT system add specific safeguards on purpose limitation, data retention and access. These instruments, however, were largely designed with databases in mind, rather than systems that learn, infer and rank. The outcome is a fragmented landscape in which the level of protection depends heavily on which system is used, by which authority and for what declared purpose. Interoperability adds a further difficulty, since it tends to blur precisely the boundaries between systems and purposes on which data protection law has traditionally relied.

The rights to privacy and data protection enshrined in Articles 7 and 8 of the EU Charter are affected by the mass collection and long-term storage of biometric data, often from people who have no real choice about providing it. The right to non-discrimination under Article 21 is exposed in a less visible but equally serious way, as risk indicators and training data may reproduce assumptions linked to nationality, ethnicity or religion even when these characteristics are never explicitly used. The analysis suggests that these harms are rarely the product of a single decision. They accumulate across systems and over time, which makes them harder to detect and harder still to challenge.

[104] See K. YEUNG, A. HOWES, G. POGREBNA, *AI Governance by Human Rights-Centred Design, Deliberation, and Oversight*, in M.D. DUBBER, F. PASQUALE, S. DAS (eds.), *The Oxford Handbook of Ethics of AI*, Oxford, 2020.

As far as algorithmic decision-making is concerned, we have seen that migrants and asylum seekers face automated systems from a position of marked asymmetry, frequently without legal assistance, without command of the language used by the administration and with an uncertain legal status that discourages them from contesting decisions. The opacity of the systems compounds this situation, as it becomes very difficult to exercise the right to an effective remedy under Article 47 of the EU Charter when the reasons behind an outcome remain hidden. Moreover, the tendency of officials to defer to machine outputs weakens the protection that Article 22 of the GDPR was meant to provide. Algorithms, in this sense, do not create the vulnerability of migrants, but they deepen it and make it more durable.

Regarding migration control, the AI Act deserves credit for classifying several uses in migration, asylum and border control management as high-risk and for subjecting them to obligations on risk management, data governance, human oversight and, in the case of public deployers, fundamental rights impact assessments. Yet the protection it offers in this field is noticeably weaker than its general architecture might suggest. High-risk systems used in migration are registered in a non-public section of the EU database; the AI components of the large-scale IT systems listed in Annex X benefit from a transitional period that extends to the end of 2030; and the prohibitions in Article 5 leave considerable room for practices that raise serious concerns when applied at the border. The AI Act therefore addresses some of the problems identified earlier, but it does so through the logic of product safety and conformity, which is not always well suited to situations in which the core issue is the exercise of public power over people in a position of weakness.

A fundamental rights-based model of AI migration governance should treat rights as the starting point rather than a compliance exercise. In other words, such a model must be based on the premise that rights are not a box to be ticked once a system has been designed but the framework within which its use must be justified from the outset. It calls for human oversight that is genuine, meaning that officers must have the authority, the time and the competence to depart from what the system recommends. It requires transparency not only towards supervisory bodies but also towards the persons concerned, who should be able to know when an automated tool has shaped a decision about them and on what grounds. It also depends on accountability mechanisms that clearly allocate responsibility among providers, deployers and public authorities, supported by accessible remedies and by independent scrutiny from data protection authorities, the Fundamental Rights Agency and civil society.

Finally, we must point out that a border which is efficient but non-transparent cannot be regarded as secure in a Union founded, as Article 2 TEU recalls, on human dignity, the rule of law and human rights. How the EU treats those at its borders remains a crucial test of its own values.

ABSTRACT: This paper analyses the growing use of artificial intelligence in migration control across the European Union. It focuses on technologies such as biometric identification, smart surveillance systems and predictive algorithms deployed at the external borders and within the Union's large-scale information systems. These tools are presented by EU institutions as instruments to improve efficiency, security and coordination among Member States. Their deployment, however, raises serious concerns regarding the protection of fundamental rights. The analysis explores the tensions between these technologies and key legal principles, notably privacy, data protection and non-discrimination, and it considers the risks of algorithmic bias and opaque decision-making. Particular attention is given to the legal framework governing Artificial Intelligence in the field of migration within the European Union (EU), including the EU Charter of Fundamental Rights (EU Charter), the General Data Protection Regulation (GDPR) and Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act). The article assesses whether the safeguards currently in place are sufficient to prevent rights violations and argues that technological innovation is advancing faster than regulatory oversight, with the result that individuals in vulnerable migration situations face heightened risks of harm. It concludes by calling for stronger accountability, transparency and human oversight mechanisms, and for a shift from formal, procedural compliance towards a substantive, fundamental rights-based model of AI governance in migration control.

KEYWORDS: EU migration control – biometrics – fundamental rights – AI Act – interoperability – data protection.