InDret
2.2025

Francesca Tassinari
Universidad del País Vasco
UPV/EHU
-

La interoperabilidad en el espacio de libertad, seguridad, y justicia y el nuevo Reglamento de Inteligencia Artificial

Algunas consideraciones sobre el procedimiento de detección de identidades múltiples

Sumario

-

Los Reglamentos (UE) 817 y 818 de 2019 establecen un marco para la interoperabilidad entre los sistemas de información de la Unión Europea (UE) sobre fronteras, visados, cooperación policial y de justicia penal, asilo y migración. La interoperabilidad implementará cuatro nuevos componentes que se incorporarán a las infraestructuras de los seis sistemas informáticos subyacentes a gran escala: el portal europeo de búsqueda, el registro común de datos de identidad, el servicio de correspondencia biométrica compartido y el detector de identidades múltiples. El objetivo de este estudio es aportar algunas reflexiones sobre el detector de identidades múltiples (DIM), cuyo funcionamiento parece integrar mecanismos «inteligentes» en los procedimientos de control fronterizo. En particular, se analiza el impacto de la normativa sobre inteligencia artificial (IA) en vista de la entrada en funcionamiento del DIM, partiendo del supuesto de que este componente forma parte de la normativa sobre IA de propósito general y de las normas comunes sobre sistemas de IA de alto riesgo. Este estudio pone de relieve las consecuencias jurídicas de este encuadramiento sobre los derechos de las personas afectadas, criticando la exención del artículo 111 del nuevo Reglamento sobre IA.

Abstract

-

Regulations (EU) 817 and 818 of 2019 establish a framework for interoperability between the European Union's (EU) information systems in the field of borders, visa, police and criminal judicial cooperation, asylum, and migration. Interoperability is implementing four new components that are being incorporated into the infrastructures of the six underlying large-scale information technology systems. These components are the European Search Portal, the Common Identity Repository, the shared Biometric Matching Service, and the Multiple-Identity Detector. This paper aims to shed light on the Multiple-Identity Detector (MID), the functioning of which suggests integrating Artificial Intelligence (AI) features in border control procedures. In particular, we will study the impact of the AI act on its entry into operation, assuming that the MID might fall under the regulation of general-purpose AI and high-risk AI systems. Thus, this study highlights the legal consequences arising therefrom on individuals' rights, while criticising the exemption foreseen under Article 111 of the new AI act.

Title: *Interoperability in the area of freedom, security, and justice and the new Artificial Intelligence act: First insights into the multiple identity detection procedure.*

-

Palabras clave: Interoperabilidad, Inteligencia Artificial, Detector de Identidad Múltiple, Espacio de Libertad, Seguridad y Justicia, Unión Europea.
Keywords**:** *Interoperability, Artificial Intelligence, Multiple-Identity Detector, Area of Freedom, Security and Justice, European Union*

-

DOI: 10.31009/InDret.2025.i2.08

InDret

2.2025

Recepción
24/02/2025
-
Aceptación
12/04/2025
-

Index

-

1. Introduction
2. Interoperability in the AFSJ: isn't it an old tale?
3. The MID and the (revised) multiple identity detection procedure
3.1. The functioning of the MID according to the interoperability regulations
3.2. Unveiling the inexplicable: The MID as an automated decision-making component
4. The exemption of Article 111 of the AI act: What lies behind and why it is important
4.1. Premise: The MID as an AI system
4.2. The MID as a general-purpose AI system
a. General, multi-purpose AI models and the MID
b. Too far ahead? Highly capable foundation models and the MID
4.3. What risk does the MID pose?
a. The MID as a high-risk AI system
b. The MID as a component of a high-risk AI system
c. Temptingly governing the MID-risks
5. Final remarks and steps forward
6. Bibliography

-

1. Introduction*

In computer science, Artificial Intelligence (AI) is conceived as the transfer of human capabilities from an individual to a machine, hardware, or software[1]. AI has experienced at least three breakout waves since the 1950s[2]. The latest wave of "strong" AI[3], driven by deep learning AI (e.g., generative AI), interprets input data and creates new content such as images, text, or audio mimicking human brain functioning[4], but has found no large-scale practical implementations to date.

In July 2024, the 12th, the AI act was published in the Official Journal of the European Union (EU)[5]. The AI act's progressive application[6] is expected to leverage the EU as the leading global actor for regulating AI[7] based on the EU's foundational values and principles[8]; counteracting other AI giants[9] pursuing more efficient self-regulatory systems[10]. The AI act classifies AI systems based on their risk-management factor, which entails their regulation when

* Contact details: Francesca Tassinari (francesca.tassinari@ehu.eus). ORCiD 0000-0003-4487-7130, ResearcherID H-5751-2018. Juan de la Cierva postdoctoral researcher at the Public Law Department of the University of the Basque Country (UPV/EHU), Bizkaia, Spain. This paper is part of the aid JDC2022-048217-I, funded by MCIN/AEI/10.13039/501100011033 and the European Union «NextGenerationEU»/PRTR, the Basque University System Research Group on Social and Legal Sciences applied to New Technosciences (GI CISJANT, ref. IT1541-22) funded by the Basque Government Department of Education, the project *Gobernanza de los usos secundarios de datos de salud y genéticos en espacios compartidos (GODAS)*, funded by MCIN/AEI/10.13039/501100011033/FEDER, and the project *Gobernanza de la inteligencia artificial basada en los ciudadanos (GOIA)*, funded by MCIN/AEI/TED2021-12902B-C22. The author wishes to thank the comments of the peer reviewers.

[1] BUTTERFIELD/NGONDI/KERR, *A Dictionary of Computer Science*, ed. 7th, 2016.

[2] LAZCOZ MORATINOS, *Gobernanza y supervisión humana de la toma de decisiones automatizada basada en la elaboración de perfiles*, 2022, pp. 24 ff. The author would like to thank Dr. LAZCOZ MORATINOS for providing access to his thesis, as well as for his suggestions on this study.

[3] VALLS PRIETO, *Inteligencia artificial, derechos humanos y bienes jurídicos*, 2021, p. 20.

[4] DE MIGUEL BERIAIN/LAZCOZ MORATINOS/SANZ ECHEVARRÍA, «Machine learning in the EU health care context: exploring ethical, legal and social issues», *Information Communication & Society*, n. 8, 2020, pp. 1140 ff. E.g., automatic recognition of spoken language, natural language processing, audio recognition and bioinformatics.

[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, *OJ* L 2024/1689, 12.7.2024 (AI act hereinafter).

[6] Article 113 of the AI act: six months as a general rule and for prohibited practices; one year for provisions on notifying authorities and notified bodies, governance, general-purpose AI models, confidentiality and penalties; and three years for high-risk AI systems covered under Annex II.

[7] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM(2021) 206 final, Brussels, 21.4.2021, pp. 1-2 (AI Proposal hereinafter), and FLORIDI, «The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU», *Philosophy & Technology*, vol. XXXIII, 2020, pp. 369 ff.

[8] Article 2 of the AI act: the AI act scope was circumscribed so as to exclude national security, military and defence, as well as research and development as we criticise *infra*.

[9] EIFLING, «China's biggest AI model is challenging American dominance», *Rest of World*, 2024, https://restofworld.org/2024/alibaba-qwen-ai-model/ (access 3.12.2024).

[10] SZCZEPAŃSKI, *United States approach to artificial intelligence*, 2024.

representing a high or limited risk[11], or prohibition when the risk is unacceptable[12]. Based on the risk pyramid drawn, AI systems used in the framework of justice and home affairs domains are generally[13] high-risk[14], if not banned[15].

The AI act follows other advanced, future-proof instruments adopted at the supranational level. In the area of freedom, security, and justice (AFSJ), regulations (EU) 817[16] and 818[17] of 2019 establish a framework for the interoperability between six, centralised large-scale information technology systems in the field of borders, visa, migration, police and judicial criminal cooperation. Since its conceptualisation, interoperability has attracted huge attention and critics, questioning its legality[18], policy interest[19], appropriateness[20], transparency[21], complexity[22], and external reach[23]. Its "intelligent" nature, however, has been barely touched.[24]

---

[11] Cfr. Articles 6 and 50 of the AI act; AI systems representing minimal risks are not subject to regulation.

[12] Article 5 of the AI act.

[13] Article 6(3) of the AI act.

[14] Annex III, points (6) and (7) cover law enforcement and migration, asylum, and border control management.

[15] Article 5(1)(h) of the AI act refers to real-time, remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless the AI system is used for the specific objectives mentioned under points (i), (ii), and (iii). Early reflections in this regard are made by GIANNINI/TAS, «AI Act and the Prohibition of Real-Time Biometric Identification: Much ado about nothing?», *Verfassungsblog*, 2024, https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/ (access 11.12.2024).

[16] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, *OJ* L 135, 22.5.2019.

[17] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, *OJ* L 135, 22.5.2019.

[18] GONZÁLEZ FUSTER/DE HERT/GUTWIRTH, «Privacy and Data Protection in the EU Security Continuum», *CEPS Papers in Liberty and Security in Europe,* 2011, p. 3.

[19] BELLANOVA/GLOUFTSIOS, «Formatting European security integration through database interoperability», *European Security*, n. 3, 2022, pp. 454 ff.; and VAVOULA, *Immigration and Privacy in the Law of the European Union*, 2022.

[20] DE HERT, «What are the Risks and What Guarantees Need to be Put in Place in View of Interoperability of Police Databases?», *Area of Justice, Freedom & Security, Collection of Standard Bri*, 2006; and BIGO/CARRERA/HAYES et al., «Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals (December 18, 2012)», *CEPS Papers in Liberty and Security in Europe*, 2012.

[21] BOEHM, «Information Sharing in the Area of Freedom, Security and Justice—Towards a Common Standard for Data Exchange Between Agencies and EU Information Systems», in GUTWIRTH/LEENES/DE HERT et al. (eds), *European Data Protection: In Good Health?*, 2012, pp. 143-183; CATANZARITI/CURTIN, «Beyond Originator Control of Personal Data in EU Interoperable Information Systems: Towards Data Originalism», in CURTIN/CATANZARITI (eds), *Data at the boundaries of European law*, 2023, pp. 133-174.

[22] QUINTEL, «Interoperable Data Exchanges within different Data Protection Regimes - The case of Europol and the European Border and Coast Guard Agency», *European Public Law*, n. 1, 2020, pp. 205 ff.; and GALLI, «Interoperable law enforcement: cooperation challenges in the EU area of freedom, security and justice», *Working Paper EUI RSCAS*, 2019, pp. 1 ff.

[23] TASSINARI, *Data Protection and Interoperability in EU External Relations*, 2024, pp. 412 ff.

[24] LEESE, «AI and interoperability», in PAUL/CARMEL/COBBE (eds), *Handbook on Public Policy and Artificial Intelligence*, 2024, pp. 146-157.

This paper continues[25] our studies on the most complex component implemented by interoperability, namely, the Multiple-Identity Detector (MID). As we suggested, the MID might be integrated with AI features despite interoperability's ostensible neutrality[26]. Hence, we now wish to inspect the scope of the MID in light of the AI act to elucidate: 1. Whether the MID is an AI system and/or a general-purpose AI system, and 2. Whether such an AI system is prohibited under the AI act. If allowed, we will elucidate the risks presented by the MID according to the AI act systematisation, and the possible consequences it will have on the individuals affected, especially migrants and vulnerable groups. This paper is divided into three main blocks: firstly, it introduces the background of the interoperability project to grasp its rationale and evolution in the last twenty years, keeping pace with technological innovations (section 2.); secondly, it inspects the MID regulation and functioning under the sister regulations (section 3.); thirdly, it scrutinises whether and how the MID falls within the scope of the AI act, its AI system nature (of general-purpose, eventually), and the level of risk it poses to public interests and fundamental rights guaranteed under the AI act[27] (section 4.).

2. Interoperability in the AFSJ: isn't it an old tale?

Regulations (EU) 817 and 818 of 2019 establish a framework for the interoperability between the Schengen Information System[28], the Visa Information System[29], the European Dactyloscopy Database[30], the Entry/Exit System[31], the European Travel Information and Authorisation

[25] TASSINARI, «The Management of Migrants' Identities at the EU External Borders: Quo vadis Interoperability?», *ADiM Blog, Analysis & Opinions*, 2021, https://www.adimblog.com/2021/11/30/the-management-of-migrants-identities-at-the-eu-external-borders-quo-vadis-interoperability/ (access 3.12.2024).

[26] DEMOKOVÁ, «The Decisional Value of Information in (Semi-)automated Decision-making», *REALaw Blog*, 2021, https://orbilu.uni.lu/handle/10993/48650 (access 11.12.2024).

[27] Recitals (6)-(10) of the AI act, where a broad list of rights and freedoms is recalled.

[28] Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, *OJ* L 312, 7.12.2018, pp. 1-13 (SIS regulation for return); 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, *OJ* L 312, 7.12.2018, pp. 14-55 (SIS regulation for border checks); and 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, *OJ* L 312, 07/12/2018, pp. 56-106 (SIS regulation for law enforcement).

[29] Regulation (EC) 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, *OJ* L 218, 13.8.2008, pp. 60-81 (VIS regulation).

[30] 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, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council, *OJ* L 2024/1358, 22.5.2024 (Eurodac regulation).

[31] 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

System[32], and the European Criminal Records Information System for Third-Country Nationals[33]. All these systems store third-country nationals' personal data[34], while the Schengen Information System and European Criminal Records Information System for Third-Country Nationals also process that of EU citizens[35]. The "sister regulations" are part of the e-initiatives headed by the EU to innovate the public administrations of the Member States while promoting greater integration both substantially and procedurally[36]. In the AFSJ, specifically, interoperability inherits the political discussions held within the EU Council in the aftermath of the 11 September 2001 Twin Towers attacks, which gave the EU's border control strategy a strong security-focused taint[37]. Above all, the access of law enforcement authorities to "migration databases" was the focus of attention to swiftly check whether a suspected or wanted person could be located when seeking an entry visa or asylum[38].

Nevertheless, such an approach would have thinned out (or even suppressed) the silo approach adopted when establishing a new centralised "database" in the security, border, asylum, or migration field. Crumbling the silo approach raised two main concerns. Firstly, from a competence perspective, each system had been established to support a specific EU policy: blurring their lines might have caused the Union to act *ultra vires*, infringing the principle of conferral not only in the *an*[39], but also in the *quantum* and *quomodo*[40]. Second (and even if related to the previous point), a cross-cutting form of interoperability within the AFSJ raised doubts about interferences caused to individuals' rights to privacy and personal data protection[41]. Generally speaking, subjecting the governance of existing centralised databases to the political course was a warning lamp of the fallacy of the guarantees put in place to protect the individual[42]. Worries were such that the lawfulness of this complex information technology reform was questioned as new forms of data processing–some of them hitherto unexplored–had been

Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, *OJ* L 327, 9.12.2017, pp. 20-82 (EES regulation).

[32] 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, *OJ* L 236, 19.9.2018, pp. 1-71 (ETIAS regulation).

[33] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, *OJ* L 135, 22.5.2019, pp. 1-26 (ECRIS-TCN regulation).

[34] Some of which belong to vulnerable groups of data subjects according to MALGIERI, «Vulnerable data subjects», *Computer Law & Security Review*, vol. XXXVII, 2020, pp. 4 ff.

[35] Article 20 of SIS regulation for law enforcement and Article 2 of ECRIS-TCN regulation.

[36] E.g., European Data Protection Supervisor-European Data Protection Board (EDPS-EDPB), *Joint Opinion on eHDSI* (12 July 2019).

[37] CAGGIANO, «L'interoperabilità fra banche-dati dell'Unione sui cittadini degli Stati terzi», *Diritto, Immigrazione e Cittadinanza*, n. 1, 2020, pp. 173 ff.

[38] LODGE, *Are You Who You Say You Are? The EU and Biometric Borders*, W.L.P. (Wolf Legal Publishers), Oisterwijk, 2007.

[39] Article 2 of the Consolidated version of the Treaty on the Functioning of the European Union, *OJ* C 326, 26.10.2012, pp. 47-390 (TFEU hereinafter).

[40] MANGAS MARTÍN, «Las competencias de la Unión Europea», in MANGAS MARTÍN/LIÑÁN NOGUERAS (eds), *Instituciones y Derecho de la Unión Europea*, 2020, pp. 77-94.

[41] EDPS, *Comments on the Communication of the Commission on interoperability of European Databases* (10 March 2006).

[42] FERRARIS, «Eurodac e i limiti della legge: quando il diritto alla protezione dei dati personali non esiste», *Diritto, Immigrazione e Cittadinanza*, n. 2, 2017, p. 13.

advanced when no enforceable framework for personal data processing in the law enforcement sector had been envisaged[43]. Hence, the earliest interoperability project was shelved, pending a more integrated and empowered Union for regulating personal data processing activities.

Following the entry into force of the Lisbon Treaty[44], and the establishment of a specific decentralised agency (eu-LISA)[45], the interoperability project was resumed under the aegis of a new strategy for innovating the EU's external border and security checks[46]. The sister regulations, establishing a framework for the interoperability between six EU's centralised databases, are the result of the high-level expert group on information systems and interoperability's meetings held since 2016[47] and, afterwards, the interinstitutional debates held behind closed doors in the 2017-2019 period[48]. The legislative texts are written under a clear functionalist logic pursuing freedom, security, and justice goals without disclosing the systems' *modus operandi*. In a nutshell, interoperability is deemed to follow four main objectives: 1. supporting the functioning of the underlying large-scale information technology systems; 2. correctly identifying individuals; 3. combating identity fraud and false identities; and 4. streamlining designated authorities' access for law enforcement purposes. Technically speaking, interoperability is implementing four new components that will absorb the six underlying large-scale information technology systems in a common interoperable platform[49]. These components are: a unique interface for accessing and retrieving the data stored in the underlying large-scale information technology systems, the EU Agency for Law Enforcement Cooperation's (Europol) data and the International Criminal Police Organisation's (Interpol) databases on Stolen and Lost Travel Document and Travel Documents Associated with Notices[50] simultaneously, known as European Search Portal; a piece of front-end infrastructure storing some of the personal data[51] held in the six underlying large-scale information technology systems, and organised in an individual file for each person, that is, the Common Identity Repository; a central container of biometric templates extracted from the corresponding biometric data called shared Biometric Matching Service; and a "complementary database" creating, establishing and storing colour-coded links between the data of the EU information systems included in the Common Identity Repository and the Schengen Information System which is labelled MID (Multiple-Identity Detector). The MID is the most inventive instrument and is suitable for achieving multiple tasks

[43] DE HERT, «What are the Risks and What Guarantees Need to be Put in Place in View of Interoperability of Police Databases?», cit. p. 3.

[44] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, *OJ* C 306, 17.12.2007, pp. 1-271.

[45] TASSINARI, «La institucionalización de la competencia operativa de la Unión Europea para la gestión y la interoperabilidad de los sistemas informáticos de gran magnitud del Espacio de Libertad, Seguridad, y Justicia: eu-LISA», *La Ley Unión Europea*, n. 111, 2023, pp. 2 ff.

[46] Communication from the Commission to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, 6.4.2016.

[47] EU Council, document 12661/ 16, Brussels, 7 October 2016.

[48] On the adoption of the interoperability package cfr. our analysis in TASSINARI, *Data Protection and Interoperability in EU External relations*, cit., pp. 308 ff.

[49] EU-LISA, «Elaboration of a Future Architecture for Interoperable it Systems at eu-LISA», *Summary of the Feasibility Study*, 2019, https://www.eulisa.europa.eu/Publications/Reports/eu-LISA%20Feasibility%20Study%20-%20Interoperability.pdf (access 8.12.2024).

[50] Already on the subject was SAVINO, «Global administrative law meets "soft" powers: The uncomfortable case of Interpol red notices», *N.Y.U. J. Int. L. & Pol.*, n. 43, 2010, p. 263.

[51] Article 18(1) of the interoperability regulations.

with the greatest effects on the migrants involved. For this reason, we are summarising its functioning below.

3. The MID and the (revised) multiple identity detection procedure

The MID was designed to accomplish two main objectives: first of all, it facilitates controls over bona fide travellers[52]; secondly, it detects identity fraudsters. According to Article 25 of the interoperability regulations, the MID comprises a central infrastructure storing links and references, and a secure communication channel that connects it with the central system of the Schengen Information System, the European Search Portal and the Common Identity Repository. The MID contains an Identity Confirmation File, regulated under Article 34 of the interoperability regulations, that gathers information on its operations and the authorities that interact with it. Specifically, the MID stores: the links referred to in Articles 30 to 33 of the interoperability regulations (red, green, and white links); an alphanumeric code of reference to the EU information systems in which the linked data is held; an alphanumeric code of a single identification number allowing the retrieval of the linked data from the corresponding EU information systems; an alphanumeric code of reference for the authority responsible for the manual verification of different identities; and the date of creation or update of the link. The Identity Confirmation File and the data stored in the MID, including the links which are personal data[53], are stored only for as long as the linked data is stored in two or more EU information systems and the Common Identity Repository. Afterwards, it must be erased from the MID using automated means in respect of predefined storage periods[54]. The MID can be accessed by the specific competent authorities in charge of carrying out the manual verification procedure[55], and also by Union agencies, depending on their access rights[56]. Such a procedure is different from the first, fully automated one, and is triggered only when the MID generates yellow links[57].

3.1. The functioning of the MID according to the interoperability regulations

As we have studied in depth[58], the multiple identity detection procedure is (eventually) composed of two phases, an automated procedure and a manual verification procedure, with different degrees of interference in the individual's rights.

---

[52] The interoperability regulations do not define who a bona fide traveller is. From a systematic reading of the two texts, this category of persons seems to refer to all those who want to cross, or pass, border controls legally, while remaining in the Schengen territory lawfully. It is, however, a presumption whereby the co-legislators assume that, given certain circumstances, the subject complies with the applicable law.

[53] Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *OJ* L 119, 4.5.2016, pp. 1-88 (or, simply, GDPR).

[54] Article 35 of the interoperability regulations.

[55] Article 26(1) of the interoperability regulations.

[56] Article 26(2) to (4) of the interoperability regulations. For an overview, cfr. the Commission Implementing Regulation (EU) 2024/2106 of 31 July 2024 amending Implementing Decision C(2021) 5052 laying down technical details for European search portal user profiles, pursuant to Article 8(2) of Regulation (EU) 2019/817 of the European Parliament and of the Council, *OJ* L 2024/2106, 1.8.2024.

[57] Article 21(1) of the interoperability regulations.

[58] E.g., TASSINARI, *Data Protection and Interoperability in EU External Relations*, cit., pp. 353 ff.

The automated procedure is triggered by the creation or updating of an individual file[59] in the Common Identity Repository[60], following the corresponding action in one of the underlying information technology systems. Said automated procedure consists of a comparison between the newly-added or erased data and those already stored in the shared Biometric Matching Service, the Common Identity Repository, and the central system of the Schengen Information System[61]. The comparison occurs within the same category of data (fingerprint data; facial images; identity data; and travel document data)[62], as long as these belong to different information technology systems[63]. Nevertheless, only one link can be established between two individual files, even when a person has more than one individual file stored within a single system, which raises doubts about its efficacy since the data, rather than the individual file, must be compared with each other (and thus linked)[64]. Hence, no MID-link is created within a sole information technology system in the event that the individual has several Schengen Information System alerts pending, for example[65]. What is expected from this automated comparison is either the establishment of colour-coded links following one or more data matches[66], or none. In concrete terms, either a white or a yellow link can be generated in an automated manner by the MID: white links are created when the identity data and/or the travel document data are found to be the same or similar, while biometric data may eventually match[67]; yellow links, instead, are established by default when the data is not even similar[68]. Besides, yellow links are provisional as the manual verification procedure should follow their creation[69]. In particular, the first scenario (i.e., white automated links), is regulated under a delegated act on the same or similar identities[70]. According to the same, if a 100% match is found between the data stored in two different EU information systems, then the match is considered to be equal; the automatically generated white link would then indicate that the data stored in the Common Identity Repository or the central system of the Schengen Information System, and the templates

[59] Each large-scale information technology system contemplates individual files with different names: alerts (Schengen Information System); links (European Dactyloscopy Database); dossier reference numbers (Visa Information System); traveler files (Entry/Exit System); linked applications (European Travel Information and Authorisation System) with the exception of identical travel documents; and data records (European Criminal Records Information System for Third-Country Nationals).

[60] The MID is launched as soon as the existing large-scale information technology systems migrate to the interoperability infrastructure as well, as we have analysed in TASSINARI, *Data Protection and Interoperability in EU External Relations*, cit., pp. 352 and ff.

[61] Article 28(2) of the interoperability regulations and PRICEWATERHOUSECOOPERS (PWC), «Feasibility study on a Common Identity Repository (CIR)», *Management Study for the European Commission*, 2017, p. 3.

[62] Article 4(8), (11), and (14) of the interoperability regulations.

[63] Article 27(5) of the interoperability regulations.

[64] Further guidance is expected to be delivered in this regard.

[65] In this sense, the MID does not alter the organisation of individual files in each information technology system, but puts order to the data distributed in different EU's databases.

[66] Article 4(18) of the interoperability regulation defines match as «the existence of a correspondence as a result of an automated comparison between personal data recorded or being recorded in an information system or database».

[67] Article 33(1)(a) to (c) of the interoperability regulations. In such case, the individual is technically identified according to the "biometric identification" definition of Article 3(35) of the AI act.

[68] Articles 28(3) and (4) of the interoperability regulations.

[69] Article 30 of the interoperability regulations.

[70] Commission Delegated Regulation (EU) 2023/333 of 11 July 2022 supplementing Regulation (EU) 2019/817 of the European Parliament and of the Council as regards determining cases where identity data are considered as same or similar for the purpose of the multiple identity detection, *OJ* L 47, 15.2.2023, pp. 17-28 (delegated act on same and similar identities hereinafter).

held by the shared Biometric Matching Service belong to the same person. Same or similar identities do not require a 100% match: the former requires that only some data be equal, e.g., the surname and first name, meaning that differences between the matched data are minimal; the latter also occurs when transliteration errors or inversions of data categories are detectable to attune possible errors. Overall, an automated white link infers that the matched data belongs to the same person; an automated yellow link, on the other hand, suggests a situation of uncertainty in the face of which human intervention is indispensable.

Take as an example a Turkish citizen who wishes to fly to Spain to conduct their pre-doctoral studies[71]; they will normally have to apply for a long-stay visa at the Spanish consulate in Türkiye. Hence, a visa dossier would be inserted in the Visa Information System, which triggers the MID to check the existence of other individual files in the other information technology systems. If the Turkish citizen has already accessed the EU illegally[72], there should be a refusal for entry alert in the Schengen Information System, with the issuing Member State being, for example, Germany[73]. As travel document data is not mandatorily inserted in the Schengen Information System[74], e.g., since the migrant might not hold their passport or identity document before or after entering the Schengen area via non-authorised border crossing points, the alert might not be provided with it. The resulting link, generated between the Visa Information System dossier and the Schengen Information System alert, would be white only if the identity and biometric data were found to be the same. Thus, the individual file stored in the Common Identity Repository would be updated[75]. The Turkish national applying for a long-stay visa should be prevented from entering Spain due to having a Schengen Information System refusal of entry alert pending[76]. Even if not specified by the co-legislators, the consular authority must be made aware of the automated generation of a white link in respect of their access rights[77]. Interestingly, no interoperability between the Visa Information System and Schengen Information System has been established[78], and the MID manages to fill this gap while supporting the visa authority competent in assessing the application.

On the other hand, the manual verification procedure is conducted by a human being from an authority competent to resolve the yellow link for which purpose a notification is automatically issued by the MID. These authorities are: border guards, competent visa authorities, and immigration authorities for the Entry/Exit System; visa authorities and authorities legally

[71] Directive (EU) 2016/801 of the European Parliament and of the Council of 11 May 2016 on the conditions of entry and residence of third-country nationals for the purposes of research, studies, training, voluntary service, pupil exchange schemes or educational projects and au pairing (recast), *OJ* L 132, 21.5.2016, pp. 21-5.

[72] Article 24(2)(c) of regulation (EU) 2018/1861. Balancing the fight against illegal migrants' entry into the EU and their protection needs is FORLATI, «L'ingresso dei migranti irregolari nell'Unione Europea – Fra controllo dell'immigrazione clandestina ed esigenze di protezione» in MILITIELLO/SPENA (eds), *Il traffico di migranti – Diritti, tutele, criminalizzazione*, 2015, pp. 37-59.

[73] Article 24(2)(c) of SIS regulation for border checks.

[74] Article 20 of SIS regulation for border checks.

[75] Article 33(2) of the interoperability regulations.

[76] Article 12(2)(a)(v) of the VIS regulation.

[77] Article 33(2) *in fine* of the interoperability regulations states that «The queried EU information systems shall reply indicating, where relevant, all the linked data on the person, thereby triggering a match against the data that are linked by the white link, if the authority launching the query has access to the linked data under Union or national law».

[78] Articles 17a and 18b of the revised VIS regulation foresee automated checks against the Entry/Exit System and European Travel Information and Authorisation System only.

empowered to issue residence permits as far as the new Visa Information System is concerned; the ETIAS Central Unit and ETIAS National United for the European Travel Information and Authorisation System; the SIRENE Bureau of the Member State that creates or updates a Schengen Information System alert; and the central authorities of the convicted Member State qualified to enter data in the European Criminal Records Information System for Third-Country Nationals[79]. Paragraph (2) of Article 29 of the interoperability regulations specifies that the SIRENE Bureau of the Member State that created a so-called "sensitive" alert in the Schengen Information System is always qualified to resolve yellow links when these alerts are inserted under Articles 26, 32, 34, and 36 of SIS regulation for law enforcement. The verification must be concluded without delay, or within twelve hours when it is performed at the borders[80]. The interoperability regulations suggest that a white, green, or red link should be established by the authority responsible for the manual verification according to the following system: a white link is established when the files are deemed to belong to the same person in a justified manner; a green link indicates that the files belong to different persons whose identities have some data in common; and a red link is established where the files belong to the same or a different person in an unjustified manner. In this sense, red links flag a high risk of a person using different or false identities and the potential victim of such fraud.

Assuming, for example, that our Turkish national seeks a long-stay visa with a fake passport and a different identity (at least the first name, surname, and date of birth), the visa dossier inserted would trigger a yellow link against the Schengen Information System refusal or an entry alert, since no travel document match is possible, the identity data are different, and the biometric data are the same–which are taken live for both the Schengen Information System and Visa Information System[81]. The consular authority is the one that is competent to resolve the yellow link[82] and they may access the data stored in the Schengen Information System alert[83]. In the course of this procedure, the visa applicant is expected to be asked about their personal status or to support their application with additional documents[84]. However, the interoperability regulations do not envisage clear procedural guarantees for visa applicants, as they do in the case of border controls *stricto sensu*[85]. The interoperability regulations state that, as soon as the consular authority acknowledges that the third country national is using a false passport, the yellow link should be turned into a red one. The consequences stemming from the usage of a false document are not addressed by the interoperability regulations either, but these stress how «the presence of a red link should not in itself constitute a ground for refusal of entry and the existing grounds for refusal of entry listed in Regulation (EU) 2016/399 should therefore not be amended»[86]. From a systemic interpretation, we deduce that the long-stay visa sought should be

[79] Article 28(1) and (2) of the interoperability regulations.

[80] Article 19(3) of regulation (EU) 2019/817.

[81] Article 13(2) of the Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (consolidated version), *OJ* L 243, 15.9.2009, pp. 1-58.

[82] Article 29(1)(b) of the interoperability regulations.

[83] Article 34(1)(f) of the SIS regulation for border checks. The competent authority may also access already existing links, if existing, for the purpose of verifying the yellow link.

[84] Article 23(3) of the Visa Code.

[85] Article 29(4) of regulation (EU) 2019/817 refers to the Entry/Exit System and foresees: «Such manual verification of different identities shall be initiated in the presence of the person concerned, who shall be offered the opportunity to explain the circumstances to the authority responsible, which shall take those explanations into account».

[86] Recital (63) of the interoperability regulations.

refused according to the Visa Code[87]; forging passports, instead, should eventually be punished according to Turkish national law.

Overall, the MID (via the European Search Portal and shared Biometric Matching Service) supports the Common Identity Repository[88] in determining the type of links to be generated or resolved in the different systems' identity files and stores the links in the Identity Confirmation File for future use. These abilities turn the MID into a powerful police tool. However, its complex functioning deserves further inspection in light of the inferences it has on migrants' rights in the border control procedures.

3.2. Unveiling the inexplicable: The MID as an automated decision-making component

The MID is driven by pre-established categories of personal data[89]–namely, identity, travel document, and biometric data–on which basis it creates new information embedded in colour-coded links. Previously, we criticised the compatibility of this component with the EU data protection framework–and, as a last resort, the Charter of Fundamental Rights of the EU[90] (CFREU)–in view of the interferences the multiple identity detection procedure causes to the individual's right when processing[91] their personal data[92]. Specifically, our studies focused on Article 22 of the GDPR[93], which anticipated the EU's regulation of algorithm technology from a human-centric perspective[94]. Its provision, even though vague and restrictive considering the entire algorithm lifecycle[95], has been interpreted as providing the highest degree of protection for establishing the right not to be subject to a decision based solely on automated processing[96]. In the famous *SCHUFA* judgment[97], the Court of Justice of the EU (CJEU) has (arguably) clarified the scope of Article 22 of the GDPR by pointing out three essential elements: a decision (1.) that is taken based on solely automated processing (2.) and produces legal effects (3.). According to the CJEU, these features must be cumulatively met to protect the individual from automated decision-making procedure, including profiling[98]. Above all, the CJEU has embraced a wide

[87] Article 32(1)(a) of the Visa Code.

[88] To our knowledge, it is the Common Identity Repository that detects new identities and decides whether a white/yellow link should be created. The Common Identity Repository itself instructs the MID of the links created in the Identity Confirmation File. However, the competent authority in charge of the manual verification procedure interacts with the MID to verify the yellow links according to Article 29 of the interoperability regulations.

[89] Article 4(1) of the GDPR.

[90] Charter of Fundamental Rights of the European Union, *OJ* C 326, 26.10.2012, pp. 391-407.

[91] Article 4(2) of the GDPR.

[92] TASSINARI, «ADM in the European Union: An Interoperable Solution», in LEGIND LARSEN/MARTIN-BAUTISTA/RUIZ et al. (eds), *Flexible Query Answering Systems. FQAS 2023. Lecture Notes in Computer Science*, 2023, pp. 290-303.

[93] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *OJ* L 119, 4.5.2016, pp. 1-88.

[94] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 2020.

[95] LAZCOZ MORATINOS, *Gobernanza y supervisión humana de la toma de decisiones automatizada basada en la elaboración de perfiles*, loc. cit.

[96] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (3 October 2017).

[97] Judgment of 7 December 2023, *OQ v Land Hessen*, C-634/21, ECLI:EU:C:2023:957.

[98] Article 4(4) of the GDPR.

definition of "decision"–as suggested by Advocate General Pikamäe–to include decisions that produce not only legal, but also economic or social effects on the individual[99], such as a scoring rate calculated on the granting of a loan. As known, the CJEU went one step further Pikamäe–who had leveraged the circumstances of the automated decision-making procedure at stake to assess the relevance of the decision on the individual–by questioning the effects produced by two different decisions, namely those of granting the loan and performing the profiling procedure. As the Advocate General noted: «If the scoring were carried out without any human intervention that could, where necessary, verify its result and the fairness of the decision to be taken in respect of the loan applicant, it would seem logical for the scoring itself to be considered to constitute the "decision" under Article 22(1) of the GDPR»[100]. Otherwise, Pikamäe alleged that the decision of the financial institution as to whether to grant or deny the loan was the only one relevant in the light of GDPR Article 22. In sum, Pikamäe was (reasonably) weighing human participation in the entire decision-making procedure, as only if the financial institution attached gave «paramount importance» to the machine scoring rate[101] would the outcome be considered a "decision". Based on this analysis we estimated[102] that the MID-coloured links could be seen as decisions in GDPR jargon if the authority inserting or erasing an identity file in the system and the Common Identity Repository, or the one competent to verify the yellow link, decided without intermediation or «merely applying the result of that evaluation to the specific case»[103]. In concrete terms, we noted that white links generated in an automated manner could be considered decisions, but verified white, green, or red links (and *a fortiori* automated yellow links) could not[104].

Today, our analysis should veer (albeit controversially) towards the different position taken by the CJEU in its later judgment. According to the CJEU, the scoring rate calculated by the private company SCHUFA must be considered the relevant "decision" in the light of Article 22 of the GDPR, provided that its guarantees might be circumvented when externalising the decision-making process[105]. Such a (partial)[106] decision–notwithstanding the human *ex post* involvement–is accordingly forbidden unless one of the exceptions of Article 22(2) of the GDPR applies. Following the CJEU's reasoning, we appreciate that both the MID white and yellow links generated in an automated manner are fully-fledged decisions under Article 22 of the GDPR despite the provisional character of the latter. In a nutshell, the CJEU has downgraded the *a sensu contrario* prohibition of Article 22(1) of the GDPR at an earlier stage, that of the machine's (in our case the MID's) outcome[107]. Subsequent "decisions", of human or computerised nature, are no longer relevant. This interpretation allows the data subject whose personal data are processed

[99] Opinion of AG Pikamäe of 16 March 2023, *OQ v Land Hessen,* C-634/21, ECLI:EU:C:2023:220 referring to recital (71) of the GDPR.

[100] Opinion of AG Pikamäe, point 42.

[101] Opinion of AG Pikamäe, point 43.

[102] TASSINARI, «ADM in the European Union: An Interoperable Solution», cit., p. 11

[103] Opinion of AG Pikamäe, point 43.

[104] TASSINARI, «ADM in the European Union: An Interoperable Solution», cit., p. 11.

[105] *OQ v Land Hessen*, para 50.

[106] LEGGIO, «L'impatto della digitalizzazione sull'attività conoscitiva pubblica nel settore migratorio e la riscoperta della centralità del dato», *ADiM Blog*, *Analyses & Opinions*, 2024 https://www.adimblog.com/wp-content/uploads/2024/12/M.-Leggio_def.pdf (access 30.12.2024), pp. 5 ff.

[107] *OQ v Land Hessen*, para 50: «[…] the establishment of that value must be qualified in itself as a decision producing vis-à-vis a data subject 'legal effects concerning him or her or similarly significantly [affecting] him or her' within the meaning of Article 22(1) of the GDPR».

within the multiple-identity detection procedure to oppose it at the earlier stage unless one of the exceptions of Article 22(2) of the GDPR applies. Specifically, Article 22(2)(b) of the GDPR allows automated decision-making procedures if authorised by the laws of the Union or the Member State to which the controller[108] is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests[109]. The provision of suitable safeguards is mandatory in the case of implementing automated decision-making procedures for another important reason: Article 22(4) of the GDPR prohibits the processing of special categories of personal data, such as biometric data for the purposes of uniquely identifying a natural person[110], unless leveraging on point (a) or (g) of Article 9(2)[111]. In sum, and within the MID context, a (possible) processing of biometric data needs to be justified as being necessary «for reasons of substantial public interest»[112]. Such a provision[113] is laid down in Article 48 of the interoperability regulations establishing the right to access, rectify, and erase personal data stored in the MID, as well as the right to restrict its processing. However, not only is the exercise of the rights enshrined therein particularly complex[114], but also there is no provision in the interoperability regulations that contemplates the right to obtain human intervention on the part of the controller[115].

The right to obtain human intervention has its conceptual origin in the necessity to preserve human interaction in a machine-learning decision-making process, *ex post* in this case[116]. It is explained under Article 22(3) of the GDPR for automated decision-making based on contractual obligations or the individual's consent together with the right to express their point of view and

[108] Cfr. Article 40(3) of the interoperability regulations referring to the European Border and Coast Guard Agency and the Member States' authorities adding or modifying the data in the Identity Confirmation File of the MID.

[109] On the subject, cfr. MALGIERI, «Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations», *Computer Law & Security Review*, n. 35, 2019, pp. 4 ff.; and PALMIOTTO, «Preserving Procedural Fairness in The AI Era», *Verfassungsblog: On Matters Constitutional*, 2023, https://intr2dok.vifa-recht.de/receive/mir_mods_00014868 (access 30.12.2024).

[110] Article 9(1) of the GDPR.

[111] Notably, Article 10(5) of the AI act foresees that special categories of personal data may be used for bias detection and correction in relation to high-risk AI systems, when the conditions [lets. a) to f)] listed therein are respected.

[112] Article 9(2)(g) of the GDPR.

[113] ibidem.

[114] Cfr. Article 48 of the interoperability regulations.

[115] Recital (71) of the GDPR refers to the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment, and to challenge the decision. It also adds that such measures should not concern a child. Cfr. FERNÁNDEZ-LLORCA/GÓMEZ/SÁNCHEZ et al., «Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making», *IEEE Xplore*, n. 1, 2022, doi: 10.1109/MCI.2021.3129960, pp. 72 ff.

[116] MARTÍN JIMÉNEZ, «Inteligencia artificial y ética: hacia una aplicación de los principios éticos en el ámbito de la UE», *Cuadernos Europeos de Deusto*, n. 68, 2023, https://doi.org/10.18543/ced.2699, p. 102. More difficult is knowing how humans are engaging with the MID *ex ante* as the interoperability regulations do not regulate the design, testing, and validating stages (human-out-the-loop), cfr. GÓMEZ-CARMONA/CASADO-MANSILLA/LÓPEZ-DE-IPIÑA et al., «Human-in-the-loop machine learning: Reconceptualizing the role of the user in interactive approaches», *Internet of Things*, n. 25, 2024, and our analysis *infra*.

to challenge the decision[117], and, broadly, by Article 11(1) of the Law Enforcement Directive[118] (LED), which is one of the requisites that must be explained under the laws of the Union or the Member States when authorising automated decision-making, including profiling, «which produces an adverse legal effect [...] or significantly affects him or her». Indeed, Article 11(1) of the LED allows automated decision-making procedures when supported by a legal basis in the laws of the Union or the Member States which is provided with appropriate safeguards. Also, the implementation of profiling techniques on the individual seems more permissible than the GDPR, whose prohibition under Article 22(1) applies to an automated decision-making that merely «produces legal effects». Even so, suitable measures to safeguard the data subject's rights and freedoms and legitimate interests must be in place[119]. The cross-cutting nature of interoperability confers on the MID a hybrid nature so that one part of its functionality might fall under the scope of the GDPR, while other falls under the LED and national laws of the Member States.[120] Indeed, the scope of the LED is restricted to the processing of personal data performed by a competent authority[121] for the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Both the objective and subjective scope are necessary for the applicability of the LED to be invoked. The application of the GDPR or, alternatively, the LED, will therefore, depend on domestic law, i.e., whether the authority adding or modifying data in the Identity Confirmation File under national law is competent or not in the light of the LED, while pursuing the latter's objectives. In the past, we have already noted how difficult the assignation of the data protection controller and processor roles is under the interoperability regulation[122] and, even more so, in the framework of the multiple identity detection procedure[123]. In practice, it will be very hard for the individual effected (especially third-country nationals) to determine the legal framework of reference–eventually including the EUDPR–and, consequently, with whom the responsibility for personal

[117] Article 22(2)(a) and (c) of the GDPR, and PALMA ORTIGOSA, *Decisiones automatizadas y protección de datos: Especial atención a los sistemas de inteligencia artificial*, 2022, pp. 286 ff. referring to the (argued) right of explanation as well.

[118] 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, *OJ* L 119, 4.5.2016, pp. 89-131.

[119] Article 11(2) of the LED.

[120] From our viewpoint, Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, *OJ* L 295, 21.11.2018, pp. 39–98 (EUDPR hereinafter) is not relevant here being its scope limited to Union institutions, bodies, offices and agencies only.

[121] Article 3(7) of the LED.

[122] TASSINARI, «The role of eu-LISA in the implementation of the interoperability framework», *ADiM Blog, Analyses & Opinions*, 2023, https://www.adimblog.com/wp-content/uploads/2023/02/4.-Tassinari-eu-LISA.February2023_DEF.pdf (access 8.12.2024), p. 5.

[123] ibid p. 6.

data processing lies[124]. The AI act thins out such dichotomy, maintaining some exceptions concerning the activities of law enforcement authorities, as we are inspecting below[125].

4. The exemption of Article 111 of the AI act: What lies behind and why it is important

AI was one of the political commitments undertaken by President von der Leyen in her first mandate between 2019-2024[126]. The European Commission officially started working on it by launching a White Paper on AI in February 2020[127] which was followed by a Proposal for a regulation published on 21 April 2021. Back then, the interoperability package had already been adopted, and during the negotiations of the AI act, concerns about the Union's large-scale information technology systems and interoperability components were raised by the Portuguese Presidency[128]. It was observed that the AI applications currently used by law enforcement authorities listed as high-risk would not be «included within the scope of the proposal». In addition, the AI act would be applicable one year after the general date of application–that is, two years after the date of its entry into force–unless there were significant changes to those components based upon a legal amendment: «Though the implications for current or mid-term use and development of those systems or their components would be limited, it is highly likely that any new developments in the overall JHA information architecture would need to be evaluated from a different perspective»[129]. According to the European Commission's Proposal, the AI act should not have applied to the justice and home affairs information technology systems and interoperability components[130] provided they were not placed on the market or put into service one year from the date of application of the AI act[131]. Moreover, the requirements laid down in the AI act should have been considered in the evaluation of each large-scale information technology system, according to their legal bases[132]. Other high-risk AI systems placed on the market or put into service before the date of application of the AI act would, instead, have been subject to the AI act provisions «only if, from that date, those systems are subject to significant changes in their design or intended purpose»[133]. The exemption proposed found no support from the European Parliament that suggested submitting the Union centralised systems and components to the AI act if these had been placed on the market or put into service

[124] FORTI, «Flussi migratori e protezione dei dati personali: alla ricerca di un punto di equilibrio tra sicurezza pubblica e tutela della privacy dei migranti e dei rifugiati all'interno del territorio europeo», *Rivista di Diritto dei Media*, n. 2, 2020, p. 229, recalls that the EU's security strategy should not overlook migrants' rights to privacy and personal data protection, including in times of crisis.

[125] Cfr. Article 2(7) of the AI act on the non-affectation relationship between the AI act and the EU's data protection *acquis*.

[126] VON DER LEYEN, *A Union that strives for more. My agenda for Europe*, 2019, https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf (access 7.12.2024).

[127] European Commission, White Paper on Artificial Intelligence, cit.

[128] EU Council, document 9096/21, Brussels, 31 May 2021, p. 6.

[129] ibidem.

[130] Cfr. Annex IX attached to the AI Proposal.

[131] Article 85(2) of the AI Proposal foresaw twenty-four months after the entry into force of the AI act.

[132] Article 83(1), second paragraph, of the AI Proposal.

[133] Article 83(2) of the AI act.

before the entry into force of the AI act. In concrete terms, the "operators"[134] of those AI systems should have taken the necessary steps to comply with the requirements laid down in the AI act[135]. Nevertheless, the deadlines proposed by the European Commission, firstly, and the European Parliament, afterwards, turned out to be too short considering the substantial delays in implementing the new information technology systems and interoperability components, which might have hampered the whole smart borders project[136]. Indeed, in the event of not complying with the AI act provisions, the interoperability components could not have been activated at all.

Trialogues led to the reformulation of the proposed exemption and current Article 111 of the AI act regulates AI systems already placed on the market or put into service, together with general-purpose AI models already placed on the market. According to the first paragraph of Article 111: «Without prejudice to the application of Article 5 as referred to in Article 113(3), point (a), AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex X that have been placed on the market or put into service before 2 August 2027 shall be brought into compliance with this Regulation by 31 December 2030».

Hence, the six large-scale information technology systems and four interoperability components are not exempt from the prohibition of certain AI practices according to Article 5 of the AI act, which is applicable as of 2 February 2025. In this sense, none of the interoperability components could be used, for instance, to exploit the vulnerabilities of the individuals or groups of persons affected (e.g. minors)[137], evaluate or clarify them based on their predicted personal or personality traits (e.g. ethnic minority)[138], or biometrically identify individuals in publicly accessible spaces for the purposes of law enforcement, remotely and in real-time[139]. In addition, the prohibition of assessing or predicting the risk of a natural person committing a criminal offence based on their profiling or characteristics (e.g. nationality and place of birth) applies[140]. The latter prohibition is particularly worrying in the MID case if we consider that, in the example given earlier, the generation of a yellow link between the Visa Information System and the Schengen Information System hints at an individual (a Turkish national) who has possibly counterfeited a national identity document; this inference, albeit provisional, results from biometric and identity data

[134] Article 3(8) of the AI act states that operator means a provider, product manufacturer, deployer, authorised representative, importer, or distributor.

[135] Cfr. the amendments n. 686 and ff. in Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), Strasbourg, 14 June 2023.

[136] EU-LISA, «Updated roadmap to interoperability endorsed by EU Council», *EU Council*, 2024, https://www.eulisa.europa.eu/Newsroom/News/Pages/Updated-roadmap-to-Interoperability-endorsed-by-EU-Council.aspx (access 10.12.2024).

[137] Article 5(1)(b) of the AI act and KURIAN, «'No, Alexa, no!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models», *Learning, Media and Technology*, 2024, https://doi.org/10.1080/17439884.2024.2367052, pp. 1-14.

[138] Article 5(1)(c) of the AI act and, e.g., MOZUR, «One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority», *The New York Times*, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (access 5.02.2025).

[139] Article 5(1)(h) of the AI act, and the Communication to the Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final, Brussels, 4.2.2025, pp. 95 ff. Envisaging the use of the Schengen Information System in this regard is VASILKOV, «Artificial intelligence in the service of border control in the EU», *ADiM Blog, Analysis & Opinions*, 2024, https://www.adimblog.com/wp-content/uploads/2024/12/New-Vasilikov_DEF.pdf (access 1.02.2025), p. 2.

[140] Article 5(d) of the AI act.

matches without further evidence of the underlying criminal activity[141]. Anyhow, the MID is not going to be placed on the market or put into service for this specific purpose, namely, to assess or predict the risk of the person committing a criminal offence, but aims to reach the "correct" identification of people through real case studies. Perhaps it would have been prudent to include a provision prohibiting different uses, including profiling, explicitly[142].

Notwithstanding such a concern, framing the six information technology large-scale IT systems and interoperability components within the AI rules is (fictitiously)[143] exempted until 31 December 2030 if these are placed on the market or put into service before 2 August 2027; at that date, interoperability is expected to be fully operational with no turning back. Article 111(1) adds that the requirements laid down in the AI act shall be taken into account in the evaluation of each large-scale information technology system as provided for in those legal acts and where those legal acts are replaced or amended. In sum, the AI act does not engage in assessing the type of risks (eventually) posed by the Union large-scale information technology systems and interoperability components (including the MID) according to the AI act but delegates such exercise to the periodic evaluation activity provided for by each legal basis, even when replaced or amended. In other words, if even one of these systems or components is placed on the market or put into service after 2 August 2027, then, no *gratiae* period would apply and the AI act general requirements must be met in their entirety. We can, therefore, imagine the European Commission racing to place on the market or put into service these systems and components by 2 August 2027 to benefit from the exemption of Article 111(1) of the AI act. Still, costs might be high for third-country nationals if interoperability is found not to comply with the AI act.

In the following sections, we shed light on the AI act requirements and the consequences stemming from their application to the MID so as to anticipate some of the issues raised by the insertion of AI features into the multiple identity detection procedure on migrants' rights.

4.1. Premise: The MID as an AI system

As Finocchiaro finds, «[b]efore embarking on a discussion of the regulation of artificial intelligence (AI), it is first necessary to define the subject matter regulated»[144]. Indeed, before assessing whether the MID is compliant with the AI act, we must clarify which AI systems are regulated under the AI act and if the MID fits into its scope.

---

[141] This example highlights how in-depth reflections on the interoperability package are needed as this framework may end up revealing much more information (whether personal or not) than originally intended by the co-legislators.

[142] The prohibition of Article 5(d) of the AI act does not apply in case the AI system is used «[…] to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity». In our example, could the pre-existing SIS alert fulfil this requirement? The answer is controversial since the SIS alert was inserted for another infringement than document forgery, that is, the illegal entry into the EU. There would then be a risk of stigmatising the Turkish national as an all-out criminal.

[143] ESCAJEDO SAN-EPIFANIO, «El reconocimiento biométrico en el Reglamento de inteligencia artificial: exenciones, prohibiciones y especialidades de alto riesgo», in COTINO HUESO/SIMÓN CASTELLANO (eds), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, 2024, pp. 183-235, p. 174.

[144] FINOCCHIARO, «The regulation of artificial intelligence», *AI & Society*, n. 39, 2024, pp. 1961 ff.

The AI act defines[145] an AI system as «a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments»[146]. According to recital (12) of the AI act, the AI system definition finally adopted is made up of the following elements: "machine-based", instead of software as initially proposed by the European Commission[147]; "autonomy", referring (albeit vaguely) to the capacity of AI to run without human intervention; "adaptiveness", which points to the AI self-learning experience that improves its functioning; "explicit or implicit objectives" achievable by AI, depending on whether these are originally programmed or self-learned; "infers" in reference to the output (prediction, content recommendation, decision, AI models, and algorithms)[148]; and "environments", i.e., the context in which the AI operates.

Such a definition abandons the descriptive one proposed by the European Commission[149]. In its Proposal, the European Commission opted for establishing a list of techniques and approaches in Annex I, such as machine learning approaches, including deep learning; logic- and knowledge-based approaches; and statistical approaches, Bayesian estimation, search and optimisation methods. The broad, flexible definition proposed was criticised by many stakeholders for raising legal uncertainty and confusion[150]. SMUHA/AHMED-RENGERS/HARKENS et al. highlighted that simple systems that use logic-based or statistical approaches that are not usually meant to be "intelligent" would be included in the AI act[151]. The authors then suggested either broadening the scope of the AI Proposal to algorithm or software technology in general, or limiting it to machine learning only. The co-legislators have broadened the AI system scope by suppressing the reference to "software" while excluding «simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations»[152]. Other critics related to the exclusion of academic research, military, security, and intelligence domains[153]. Consequently, AI systems placed on the market or put into service for scientific research and development have been excluded from the AI act scope[154], as is the case of AI systems made available–i.e., placed on the

---

[145] OECD, *Recommendation of the Council on Artificial Intelligence*, 2024, https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449 (access 10.12.2024) and EU Council, document 11124/22, Brussels, 15 July 2022, p. 3.

[146] Article 3(1) of the AI act.

[147] Such an AI system definition leaves aside systems that may function with a certain degree of autonomy, but cannot be considered as autonomous.

[148] DE MIGUEL BERIAIN, «¿Explicar o predecir?», *Investigación y ciencia*, n. 538, 2021, pp. 52-53.

[149] For a critic see FINOCCHIARO, «The regulation of artificial intelligence», cit. p. 39.

[150] VEALE/ZUIDERVEEN BORGESIUS, «Demystifying the Draft EU Artificial Intelligence Act», *Computer Law Review International*, n. 22, 2021, https://ssrn.com/abstract=3896852.

[151] SMUHA/AHMED-RENGERS/HARKENS et al., «How the EU can achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act», *LEADS Lab @University of Birmingham. For a Legal, Ethical & Accountable Digital Society*, 2021, pp. 13 ff.

[152] Recital (12) of the AI act.

[153] SMUHA/AHMED-RENGERS/HARKENS et al., cit.

[154] Recital (25) of the AI act, but the EU's data protection regime remains applicable as DE MIGUEL BERIAIN, «La utilización de datos con fines de investigación científica (XXI)», in COTINO HUESO (ed), *La Carta de Derechos Digitales,* 2022, pp. 299-326 finds. For a critic on the AI Proposal cfr. EBERS/R.S. HOCH/ROSENKRANZ et al., «The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)», *Multidisciplinary Scientific Journal*, n. 4, 2021, https://doi.org/10.3390/j4040043, p. 591.

market or put into service in the Union or whose output is used in the Union–for military, defence, or national security purposes[155].

Recently, the European Commission has adopted new guidelines on the AI system definition[156] and, despite their non binding character, such a soft analysis helps us understand whether the MID falls within the AI act scope. The European Commission states that an AI system is made of seven elements by splitting the "inference" requirement from the output exemplifications (namely, prediction, content recommendation, decision, AI models, and algorithms), but warns that some of these may not be present throughout the algorithm lifecycle. First, the MID must be "machine-based", that is, developed and run on machines of a hardware or software nature. The fact that the MID (whose fate is followed by the others the other interoperability components) is not allocated a specific site in Strasbourg[157], suggests we see it as a software rather than a hardware component[158]. Second, the MID should benefit from certain "autonomy". Human involvement and intervention can be either direct or indirect, according to the European Commission. Third, the MID may show "adaptiveness" in terms of self-learning capabilities, for example, by learning from its mistakes or discovering new patterns or relationships among the datasets[159]. Fourth, the MID pursues specific objectives as automated link generation can be seen as an explicit objective, for example. Yet, and as we have already emphasised above, the MID could incidentally reveal hidden information, or metadata, from the underlying systems or during its training. Fifth, the MID must carry an "inference" capacity, which consists of outputs. As we assumed elsewhere[160], the MID can be classified as supervised[161] machine learning, replacing or supporting decision-making in external (including, de-territorialised)[162] border controls. Machine learning is «the technique that improves system performance by learning from

[155] Article 2(3) of the AI act.

[156] Annex to the Communication to the Commission, Approval of the content of the draft Communication from the Commission - Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), C(2025) 924 final, Brussels, 6.2.2025.

[157] Article 17(3) of Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, *OJ* L 295, 21.11.2018, p. 99–137 (eu-LISA regulation hereinafter).

[158] Cfr. the definition in ScienceDirect https://www.sciencedirect.com/topics/computer-science/software-component (access 31.03.2025).

[159] AI might consist of handcrafted rules, instead of data, like Stockfish, a free and open-source chess engine available at https://stockfishchess.org/ (access 31.03.2025).

[160] TASSINARI, «ADM in the European Union: An Interoperable Solution», cit.

[161] JANIESCH/ZSCHECH/KAI et al., «Machine learning and deep learning», *Electron Markets*, 2021, pp. 685-695. Three types of machine learning are identified by scholars: supervised, unsupervised, and reinforced. In cases where supervised machine learning is required, it is the human being who chooses the categories of data to be matched, as well as the outcome pursued as a result of the analysis of that data. On the other hand, unsupervised machine learning requires the machine to detect hidden correlations among the data used in order to detect similarities (clustering) and anomalies. Finally, reinforced machine learning works on the basis of the carrot and stick rationale, that is, by classifying the machine output as right or wrong so as to reward or punish it.

[162] DEL VALLE GÁLVEZ, «La Fragilidad de los Derechos Humanos en las fronteras exteriores europeas, y la Externalización / Extraterritorialidad de los controles migratorios», in SOROETA LICERAS/ALONSO MOREDA (eds), *Anuario de los cursos de derechos humanos de Donostia-San Sebastián Vol. XVIII*, 2019, pp. 25-49, p. 44.

experience via computational methods»[163] to create new knowledge[164]. As such, machine learning is seen as a requirement of AI as long as the learning capacity is a data-driven smart task[165]. However, a more primitive form of AI cannot be excluded, namely that of logic- or knowledge-based approaches. If so, the MID would work based on human knowledge via deductive or inductive operations to draw conclusions. Sixth, the MID generates "outputs" and, specifically, content or new material in the form of colours. Seventh, the MID can be deemed to "influence" the virtual environment in which it operates, that is, the other systems and components that are part of the interoperability architecture. Overall, and although the MID analytical capacity would be limited compared to much more invasive AI systems, its "commercialisation" imposes respecting ethical and legal guidance, which restrains the impact of the multiple identity detection procedure on individuals' (especially migrants') rights.

4.2. The MID as a general-purpose AI system

a. General, multi-purpose AI models and the MID

Considering the MID not merely as an AI system, but as a general-purpose AI system[166] means attributing it the accomplishment of the generality and distinct task criteria[167], some of which have already emerged from this study (i.e., link searching and generation, or error detections), and the possibility of integrating it with a variety of downstream systems or applications (e.g., the central system of the Schengen Information System, European Search Portal, and Common Identity Repository). General-purpose AI refers to the possibility of pursuing different goals through specific AI models[168] or systems[169].

General-purpose AI was not included in the AI Proposal[170], but found regulation following the spread of OpenAI[171], which raised great inter-institutional controversies[172]. Specifically, Chat GPT emerged in the midst of negotiations in 2023–GPT is a chatbot program developed by the American Research Institute OpenAI that implemented it in a Chat Generative Pre-Trained Transformer[173]. Within the EU Council, general-purpose AI was initially presented as falling

[163] ZHOU, *Machine Learning*, 2021, p. 2. Cfr. also EL NAQA/MURPHY, *What is Machine Learning?*, 2015, p. 3.

[164] LAZCOZ MORATINOS, *Gobernanza y supervisión humana de la toma de decisiones automatizada basada en la elaboración de perfiles*, cit., p. 30.

[165] ALPAYDIN, *Machine Learning*, Revised and updated ed., 2021, p. 18.

[166] On the difference between AI model and system see *infra*.

[167] Article 113 of the AI act sets forth that Chapter V of the AI acts applies as of 2 August 2025.

[168] Cfr. EDPB, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models* (17 December 2024) p. 12.

[169] A general-purpose AI system is a complex application joined by one or more models, plus a data collection and processing tool, a user interface, and an infrastructure. Article 3(66) of the AI act finds that a general-purpose AI system «means an AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems».

[170] Cfr. Article 1 of the AI Proposal, and current Article 1.2 let. e) of the AI act.

[171] EU Council, document 8534/23, Brussels, 8 May 2023, p. 2.

[172] GSTREIN/HALEEM/ZWITTER, «General-purpose AI regulation and the European Union AI Act», *Internet Policy Review: Journal on internet regulation*, n. 3, 2024, https://doi.org/10.14763/2024.3.1790.

[173] YANG, «Research on the legal regulation of Generative Artificial intelligence Take ChatGPT as an example», *SHS Web of Conferences*, n. 02017, 2023, https://doi.org/10.1051/shsconf/202317802017.

outside the risk-based approach pursued by the AI act due to its lack of intended purposes[174, 175]. Yet, one of the main concerns raised was that a general-purpose AI model could be integrated into an AI system (and, eventually, a high-risk AI system) without the provider—to whom the obligations of Article 16-25 of the AI act apply—of the general-purpose AI system «having any or only limited influence over compliance with obligations of the regulation»[176]. Under the French Presidency, the general-purpose AI definition was revisited to «balance the requirements and obligations between the providers of such systems and the providers of high-risk AI systems likely to use them»[177]. The Czech Presidency, instead, decided not to apply the high-risk AI system requirements to general-purpose AI but lay down specific rules in a subsequent implementing act adopted by the European Commission[178]. In addition, the European Parliament proposed inserting specific, enhanced obligations for providers of foundation models[179] «regardless of whether it is provided as a standalone model or embedded in an AI system or a product, or provided under free and open source licences, as a service, as well as other distribution channels»[180].

Article 3(66) of the AI act finds that a general-purpose AI model is «an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market». Recital (97) of the AI act clarifies that general-purpose AI models are typically trained on large amounts of data via self-supervised, unsupervised, or reinforced machine learning[181], but what distinguishes the general-purpose AI model definition is also their capacity to perform numerous and distinct functions. Hence, a general-purpose AI model is defined by two elements: 1. generality; and 2. a wide range of distinct tasks[182]. The AI act does not concretise the range of these criteria, but

[174] Article 3(12) of the AI act. For a critic on the intended vs. general purpose dichotomy, see FERNÁNDEZ-LLORCA, «An interdisciplinary account of the terminological choices used by EU policymakers ahead of the final agreement on the AI Act: AI system, general purpose AI system, foundation model, and generative AI», *Artificial Intelligence and Law*, 2024, https://doi.org/10.1007/s10506-024-09412-y, p. 6.

[175] Cfr. the proposed recital (70a) and Title IVa are in EU Council, document 1427/21, 29 November 2021, pp. 26 and 68. Conversely, the person placing on the market, putting into service (under its own name or trademark), or using general-purpose AI made available on the market for an "intended purpose" should have been considered a provider of an AI system. Similarly, another person would be considered a provider if they integrate into an AI system a general-purpose AI model made available on the market by another person, with or without modifying it, for an "intended purpose".

[176] EU Council, document 13802/21, Brussels, 19 November 2021, p. 6.

[177] EU Council, document 8576/22, Brussels, 16 May 2022, p. 9.

[178] EU Council, document 14336/22, Brussels, 11 November 2022, p. 6.

[179] Foundational model is «any model that is trained on broad data (generally using self-supervision at scale) that can be adapted (e.g., fine-tuned) to a wide range of downstream tasks» according to BOMMASANI/HUDSON/ADELI et al., «On the Opportunities and Risks of Foundation Models», *Center for Research on Foundation Models (CRFM)*, 2021, p. 1. It differs from other general-purpose AI models because of its numerous capabilities according to the EU Council, document 13921/23, Brussels, 17 October 2023, p. 18.

[180] EU Council, document 13921/23, Brussels, 17 October 2023, p. 18.

[181] COBBE, «Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making», *Legal Studies*, n. 4, 2019, p. 3.

[182] CASTILLO PARRILLA, «Inteligencia artificial de uso general, modelos fundacionales (y "Chat GPT") en el Reglamento de inteligencia artificial», in SIMÓN CASTELLANO/COTINO HUESO (eds), *Tratado sobre el Reglamento de Inteligencia. Artificial de la Unión Europea*, pp. 757-777, p. 640.

under recital (98) some hints are given. General-purpose AI models are: «[…] models with at least a billion of parameters and trained with a large amount of data using self-supervision at scale should be considered to display significant generality and to competently perform a wide range of distinctive tasks». It is therefore interesting to note that the definition of general-purpose AI does not focus on the purposes pursued by the data controller while running the machine, as we are observing with the high-risk classification *infra*, but rather on the huge, different "technological" functionalities the machine can serve. Unsupervised machine learning using no-label data, like deep learning AI and neural networks, clearly fits into such a definition; for the rest of AI systems, which are simpler (like the MID), the analysis is more far-fetched. Pending further concretisation of this definition[183], we cannot discard the MID general-purpose nature. The latter can, for example, search and compare different categories of data, generate links of various colours based on predefined rules, and detect errors such as transliteration and inversions[184]. It is unclear, however, whether the MID will be able to deploy new tasks, possibly even induced ones, once placed on the market. This hypothesis forces us to look at the horizontal obligations foreseen in Chapter V of the AI act before jumping onto the AI act risk pyramid[185]. Indeed, providers[186] of general-purpose AI models are subject to *ad hoc* enhanced rules, following the discussions held within the EU Council regarding "very capable" foundation models and foundation models "at scale". By assigning the provider a proactive role in the AI value chain, these rules seek to temper the possible risks deriving from the use of general-purpose AI models as, nowadays, their understanding (and impact) remains almost unclear[187].

In concrete terms, Article 53[188] of the AI act introduces specific transparency obligations for providers of general-purpose AI models *ex post*, that is, after these are put on the market or into service. Even though no definition of an AI model is given, recital (97) AI act makes implicit reference to it while stating that: «AI models are essential components of AI systems, they do not constitute AI systems on their own». A "model" is the outcome learned from the data, that is, the mathematical or statistical representation tasked to infer the output based on the input data via a pattern-matching algorithm. Regulating general-purpose AI models (instead of systems) means tracing the value chain back *ab origine*–i.e., before the system is set up–and thus potentially involving other actors than eu-LISA[189], the agency responsible for designing and putting the MID into motion. It could be, for instance, a company to which development is (arguably) outsourced[190]. According to Article 53(1) of the AI act, the providers of general-

[183] Gutierrez/Aguirre/Uuk et al., «A Proposal for a Definition of General Purpose Artificial Intelligence Systems», *Digital Society*, n. 2, 2023, pp. 3 ff. fins that general-purpose AI systems is: «An AI system that can accomplish or be adapted to accomplish a range of distinct tasks, including some for which it was not intentionally and specifically trained».

[184] Cfr. the delegated act on same and similar identities.

[185] Recital (97) of the AI act.

[186] Article 3(3) of the AI act states that provider is the «natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge».

[187] Article 3(66) of the AI act adopts the European Parliament's definition of general-purpose AI which reads as follows: «an AI system which is based on a [general-purpose AI] model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems».

[188] Article 54 of the AI act applies to providers established in third countries that place general-purpose AI in the Union market; the AI act requires them to appoint a representative established in the Union.

[189] Article 13 of the eu-LISA regulation.

[190] Recital (15) of regulation (EU) 2018/1726.

purpose AI models must comply with the following four transparency obligations: draft and keep up to date the technical documentation of the model–including its training and testing process and the results of its evaluation–of Annex XI[191] of the AI act, which must be made available to the AI Office and the competent national authorities[192]; draft, keep up to date, and make available the information and documentation to providers of AI systems who intend to integrate the general-purpose AI model into their AI systems in order to understand whether the resulting general-purpose AI system complies with the risk-based approach of the AI act[193]; put in place a policy to comply with EU law on copyright and related rights[194], and in particular, to identify and comply with, including through state-of-the-art-technologies, a reservation of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790[195]; and draft and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to the template provided by the AI Office[196]. Compliance with these obligations may be proved by using a code of practice according to Article 56 of the AI act[197] until harmonised standards are published[198]. Alternatively, the provider must demonstrate that they will fulfil those obligations following an assessment headed by the European Commission[199]. Overall, understanding how the assembly line of the MID works is of crucial importance if we embrace its general-purpose AI nature. In case part of it is outsourced (e.g., the setting-up of the model), the parties involved should ensure respect not only to the greatly explored delegation doctrine[200] and the fundamental rights *continuum*, but precisely to the requirements established under the AI act to safeguard public interest (e.g., algorithm transparency) and fundamental rights.

b. Too far ahead? Highly capable foundation models and the MID

[191] Annex XI lays down the technical documentation for providers of general-purpose AI models. The European Commission was delegated the task to adopt an act to detail measurement and calculation methodologies to allow for comparable and verifiable documentation. Also, the European Commission may amend Annexes XI and XII in light of the evolving technologies [cfr. Article 53(5) and (6) of the AI act].

[192] Article 70(1) of the AI act refers to at least one notifying authority and at least one market surveillance authority, but for Union institutions, bodies, offices, or agencies the competent authority is the EDPS.

[193] The information and documentation must enable providers of an AI system to have a good understanding of the capabilities and limitations of the general-purpose AI model and to comply with their obligations under the AI act, and contain, at a minimum, the elements set out in Annex XII.

[194] In this regard, it is interesting to point out the recent judgment of the Regional Court of Hamburg in CARMONA/ÁLVAREZ, «El fallo de Hamburgo: ¿un punto de inflexión en la minería de datos para entrenamiento de la IA?», *Economist&Jurist*, 2024, https://www.economistjurist.es/articulos-juridicos-destacados/el-fallo-de-hamburgo-un-punto-de-inflexion-en-la-mineria-de-datos-para-entrenamiento-de-la-ia/ (access 9.12.2024).

[195] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, *OJ* L 130, 17.5.2019, pp. 92-125.

[196] See, e.g., the model of GALDON CLAVELL, «AI Auditing. Checklist for AI Auditing», *European Data Protection Board*, 2024, https://www.edpb.europa.eu/system/files/2024-06/ai-auditing_checklist-for-ai-auditing-scores_edpb-spe-programme_en.pdf (access 4.02.2024).

[197] Article 56 of the AI act regulates codes of practice at the Union level for both general-purpose AI and general-purpose AI with systemic risk.

[198] Article 53(4) of the AI act.

[199] Article 53(2) of the AI act exempts providers of AI models released under a free and open-source licence that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available unless they pose a systemic risk.

[200] KLABBERS, *The Law of International Organizations*, 2015, p. 76.

Due to their inestimable potential, highly capable foundation models (or foundational models at scale) were deemed to require enhanced obligations for the providers before they could be placed on the market or put into service[201]. Large generative AI models are presented as examples of general-purpose AI models with possible systemic risks «given that they allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks»[202]. The AI act does not provide for a definition of, or a specific regulation for generative AI[203]. Generally, Articles 51 and 52 of the AI act enhance the transparency obligations of general-purpose AI providers in the event that the model generates a systemic risk, for example, to counteract deepfakes and misinformation[204].

Firstly, Article 51(1) of the AI act clarifies when a systemic risk occurs. A systemic risk occurs when the general-purpose AI model has high-impact capabilities[205] evaluated based on appropriate technical tools and methodologies, including indicators and benchmarks; in addition, a systemic risk occurs based on a decision of the European Commission, *ex officio* or following a qualified alert from the scientific panel, testifying that the general-purpose AI system has the capabilities or an impact equivalent to those set out in Article 51(1)(a) of the AI act, in regard to the criteria set out in Annex XIII[206]. The two criteria are cumulative, meaning that the European Commission is solely in charge of establishing a general-purpose AI model as being of systemic risk, as per Article 52(3) of the AI act. Overall, a general-purpose AI model with systemic

[201] Worrisome surrounding these models promoted the establishment of a centralised structure for supervision, monitoring, and foresight, at the supranational level (the AI Office) in EU Council, document 13921/23, Brussels, 17 October 2023, pp. 21 and ff.

[202] Recital (99) of the AI act. For a critic see HACKER/ENGEL/MAUER, «Regulating ChatGPT and other Large Generative AI Models», VVAA (eds), *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, 2023, pp. 1112-1123, pp. 1114 ff.

[203] Recital (105) of the AI act highlights the challenges that generative AI models represent in terms of artists, authors, and other creators' copyrights, while Article 50(2) of the AI act adds that providers and deployers of generative AI models must comply with the transparency obligations of certain AI systems, and «ensure their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible taking into account acknowledged state-of-the-art». Specifically, the output should be detectable as artificially generated or manipulated.

[204] Recital (97) of the AI act and Article 3(65) defines systemic risk as «a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain».

[205] The proposed definition, which was not finally incorporated into the AI act, found that high impact capabilities meant «capabilities that match or exceed the capabilities recorded in the most advanced [general-purpose AI] models», see EU Council, document 16097/23, Brussels, 28 November 2023, p. 7.

[206] Annex XIII exemplifies: the number of parameters of the model; the quality or size of the data set, for example, measured through tokens; the amount of computation used for training the model, measured in floating points or indicated by a combination of other variables such as the estimated cost of training, the estimated time required for the training, or the estimated energy consumption for the training; the input and output modalities of the model, such as text-to-text (large language models), text-to-image, multi-modality, and the state-of-the-art thresholds for determining high-impact capabilities for each modality, and the specific type of inputs and outputs (e.g. biological sequences); the benchmarks and evaluations of capabilities of the model, including considering the number of tasks without additional training, adaptability in learning new, distinct tasks, the level of autonomy and scalability, the tools it has access to; whether it has a relevant impact on the internal market due to its reach, which will be presumed once it has been made available to at least 10,000 registered business users established in the Union; and the number of registered end-users.

risk is defined based on its scale[207] which is measured on two quantitative thresholds: 1. the amount of computing used for its training and 2. the number of business users of the model[208].

To the best of our knowledge, possible factors in favour of classifying the MID as a general-purpose AI system with a systematic risk could be the input and output modalities of the model; its adaptability to learn new, distinct tasks, as well as its autonomy and scalability; the huge number of registered end-users is also relevant. Secondly, Article 51(2) of the AI act introduces the presupposed compliance of general-purpose AI models with high impact capabilities «when the cumulative amount of computation used for its training measured in floating point operations[209] is greater than 10^{25}»[210]. Hence, such a presupposition would be fulfilled in the case that the MID is known to comply with those parameters, which are not publicly available. According to recital (98) of the AI act: «Whereas the generality of a model could, inter alia, also be determined by a number of parameters, models with at least a billion of parameters and trained with a large amount of data using self-supervision at scale should be considered to display significant generality and to competently perform a wide range of distinctive tasks»[211]. Even more alluring is the hypothesis in which colour-coded links could be classified as a content-based output, turning the MID into a more sophisticated generative AI system. Nevertheless, this interpretation might be too strained as far as the MID is concerned, as Article 50(2) of the AI act refers to synthetic audio, image, video, or text content which depicts more elaborated outputs than colour-coded links[212]. In contrast, the MID seems to limit itself to assigning a specific colour when a certain percentage threshold is reached following a match.

Systematising the MID as a general-purpose AI system with systemic risk means, from a data governance perspective, complying with the obligations set down in Article 52 of the AI act in addition to the horizontal, transparency obligations listed in Article 53 of the AI act[213]. In concrete terms, the provider of such a model (or models) must notify the European Commission without delay if it meets the quantitative thresholds highlighted above; indeed, the latter keeps the last word as to whether the general-purpose AI model poses a systemic risk or not[214]. Alternatively, the European Commission itself may, *ex officio* or following a qualified alert, declare that a general-purpose AI model poses a systemic risk based on Annex XIII. Notably, a list of general-purpose AI models with a systemic risk should be made public and kept up to date,

---

[207] GSTREIN/HALEEM/ZWITTER, «General-purpose AI regulation and the European Union AI Act», cit., p. 5.

[208] Under Article 51(3) of the AI act the European Commission is delegated the power to rectify those thresholds according to the evolving technological developments, and must specify the technical elements of general-purpose AI models with a systemic risk while keeping the benchmarks up to date through market and technological development. It is, therefore, an ongoing valuation that buys intrinsic uncertainty: what may be systemic risk today may not be so tomorrow, and vice versa.

[209] Article 3(67) of the AI act states that floating points mean «any mathematical operation or assignment involving floating-point numbers, which are a subset of the real numbers typically represented on computers by an integer of fixed precision scaled by an integer exponent of a fixed base».

[210] The calculation is straightforward for general-purpose AI systems provided through an Application Programming Interface (API). For general-purpose AI systems provided through a library, a methodology needs to be developed. Notably, the agreed threshold is higher than what the European Parliament wanted to achieve, but lower than the EU Council's mandate–10^{26} according to the EU Council, document 5662/24, Brussels, 26 January 2024, p. 6.

[211] Recital (98) of the AI act.

[212] NOVELLI/CASOLARI/HACKER, «Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity», *Working Paper*, n. 55, 2024.

[213] See our analysis in section 4.2.a.

[214] Article 52 of the AI act.

«without prejudice to the need to observe and protect intellectual property rights and confidential business information or trade secrets in accordance with Union and national law»[215]. It is important to note that, unlike the high-risk AI systems regulation we are dealing with *infra*, there are no transparency exceptions for the AFSJ; the confidentiality obligation set down in Article 78 of the AI act applies instead[216]. In addition, the provider should accomplish a set of new obligations, namely: performing model evaluation by means of standardised protocols and tools reflecting the state-of-the-art, including conducting and documenting adversarial testing of the model to identify and mitigate the risks; assessing and mitigating possible systemic risks at Union level, including their sources, that may stem from the development, market placement or use of general-purpose AI models with a systemic risk; keeping track of, documenting, and reporting, without undue delay, to the AI Office and, as appropriate, to the competent national authorities relevant information about serious incidents and possible corrective measures in order to address them; and ensuring an adequate level of cybersecurity protection for the general-purpose AI model posing a systemic risk and the physical infrastructure of the model[217]. Also in this case, the provider may rely on codes of practice with the meaning given in Article 56 of the AI act to demonstrate compliance until harmonised standards are published.

4.3. What risk does the MID pose?

The AI act sets forth that when a provider of a general-purpose AI model integrates that model into an AI system, that is placed on the market or put into service, then, that general-purpose AI model should be considered placed on the market or put into service as well[218]. In other words, any operator specifying an "intended purpose" of a general-purpose AI model, and placing it on the market or putting it into service for such a purpose, should be considered a provider[219] according to the AI act; or if a person integrates the general-purpose AI system on the market into another AI system subject to the AI act[220], then, that person would be considered a provider of both. Providers who exclude the use of a general-purpose AI model for high-risk purposes should introduce measures to detect and prevent such use; providers who allow it should make sure that the general-purpose AI system complies with the requirements applicable to high-risk AI systems for each allowed high-risk use[221].

In the following section, we propose inspecting two situations: either eu-LISA is the provider of the general-purpose AI model(s) whose integration results into an AI system (the MID), or eu-LISA integrates the general-purpose AI model previously designed, trained, and tested by another party into an AI system (the MID). In both cases, the MID may be found to be a high-risk

[215] Article 52 of the AI act.

[216] Article 55(3) of the AI act. Article 78(1)(c) of the AI act imposes the European Commission, the market surveillance authority, the notified bodies, and any other natural or legal person involved to respect the confidentiality of information and data obtained in carrying out their tasks and activities to safeguard public and national security interests.

[217] Article 55 of the AI act.

[218] Article 25(1)(c) of the AI act.

[219] Article 3(3) of the AI act.

[220] Article 3(13) of the AI act.

[221] Article 16 of the AI act and our analysis *infra*.

AI system, or a component of another high-risk AI system[222], causing adverse impacts on the individuals concerned[223].

a. The MID as a high-risk AI system

The first hypothesis (MID = high-risk AI system) calls for an assessment of the MID under Article 6(2) of the AI act. Unlike Article 6(1) of the AI act, which refers to AI systems used as safety components of specific products as per its Annex I, Article 6(2) of the AI act gives a list of domains detailed under Annex III. Annex III–whose list is subject to a yearly review by the European Commission[224], that may also add or modify it via a delegated act[225]–details high-risk AI systems used for specific policy purposes, like law enforcement, migration, asylum, border control management, and administration of justice where the MID clearly fits in[226]. Such high-risk is presumed[227] and calculated «[…] taking into account both the severity of the possible harm and its probability of occurrence»[228].

Chapter III of the AI act includes one important derogation to the general regime: Article 6(3) of the AI excludes any high-risk hazard if the AI system «[…] does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making»[229]. The derogation applies when[230]: the AI system is intended to perform a narrow procedural task; the AI system is intended to improve the result of a previously completed human activity; the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously-completed human assessment, without proper human review; or the AI system is intended to perform a preparatory task to an assessment relevant for the use cases listed in Annex III. A narrow procedural task is, for example, an AI system that transforms unstructured data into structured data, or classifies incoming documents. Instead, an improvement of human activity occurs when the AI system is used to improve the language used in a previously drafted document, or to align it to the messaging of a certain brand. Decision-making patterns or deviations from prior decision-making patterns are estimated to be low-risk as long as the AI system is used to check *ex post* a previously completed human assessment. Last

[222] Recital (85) and Article 25(1)(c) of the AI act.

[223] Recital (48) of the AI act. Subsidiarily, Chapter IV of the AI act would apply if the MID was a limited-risk AI system.

[224] Article 112(1) of the AI act.

[225] Article 7 of the AI act.

[226] Article 113 of the AI act sets forth that these high-risk AI systems must align to the AI act as of 2 August 2027. The MID does not fit under point 1 of Annex III, regulating remote biometric identification systems, biometric categorisation systems, and AI systems intended to be used for emotion recognition as we have already analysed *supra*.

[227] Article 6(4) of the AI act, resulting in a reversal of the burden of proof on the provider of the AI system according to COTINO HUESO, «Los sistemas de inteligencia artificial de alto riesgo: delimitación y análisis de algunos ámbitos», in COTINO HUESO/SIMÓN CASTELLANO (eds), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, 2024, pp., 231-252, pp. 248 ff.

[228] Recital (52) of the AI act.

[229] Article 6(3) of the AI act.

[230] These criteria are useful in case the assessment is conducted by the providers of high-risk AI systems, but also for the European Commission to modify these requirements with a delegated act «[…] where there is concrete and reliable evidence of the existence of AI systems that fall under the scope of Annex III, but do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons», as per Article 6(6) of the AI act.

but not least, an AI preparatory task consists of indexing, searching, text and speech processing or linking data to other data sources, or translations[231].

In our view, arguing that the MID meets any of these conditions would require a controversial interpretation of the abovementioned clauses, against the AI act safeguards. The MID link searching functionality, for example, is not limited to interconnecting the Common Identity Repository-individual files, but also to generating a result based on the probabilities of coincidence (i.e., colour-coded links). This reasoning is self-evident for the automated white links generated by the MID for the reasons that have been explained in detail above[232]. Besides, Article 6(3) *in fine* of the AI act adds that the high-risk AI systems referred to in Annex III «shall always be considered to be high-risk where the AI system performs profiling of natural persons»[233]. Back in 2023, we advanced the idea that the generation or establishment of links «could help to evaluate certain aspects relating to natural persons»[234], with interoperability being the implementation of case management and not only an identity management system. Returning to our example of the Turkish citizen seeking a long-stay visa for studying in Spain, we have explained how the generation of a white link in an automated manner against the Schengen Information System from the Visa Information System allows the competent authority to access these two systems and acknowledge that said foreign citizen has infringed the Schengen Borders Code's[235] rules for entry and/or stay in the Schengen area, and subsequently those of the Visa Code; in addition, the consular authority would know that the third country national has committed one or more crimes, e.g. by forging an official document. Classifying the MID as an AI profiling system would definitively remove any doubt as to its high-risk nature. However, this study warns that profiling is not an explicit objective of the MID, but the result of a broad interpretation of its functioning given the lack of an express prohibition.

b. The MID as a component of a high-risk AI system

The second hypothesis (MID = component of another high-risk AI system) requires assessing whether the six underlying large-scale information technology systems and the other three interoperability components (namely the European Search Portal, shared Biometric Matching Service, and Common Identity Repository) can be systematised as AI systems and, after that, if they are high-risk.

This assumption is not disproportionate if we consider that the concept of "component"–which is common to both the AI act and interoperability regulations–is not clarified legally[236]. If by "component" we are referring to an essential part of an AI system, then, the MID will not turn out to be a component of the six large-scale information technology systems. Indeed, even

[231] ibidem.

[232] Recital (53) of the AI act.

[233] Article 4(4) of the AI act states that profiling means «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 that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements».

[234] TASSINARI, «ADM in the European Union: An Interoperable Solution», cit., p. 10.

[235] 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) (codification), *OJ* L 77, 23.3.2016, pp. 1-52.

[236] See the definition of interoperability in the International Organisation for Standardisation (ISO) 25964-2:2013(en) Information and documentation — Thesauri and interoperability with other vocabularies — Part 2: Interoperability with other vocabularies.

though the MID adds value to the new information technology infrastructure, it is not mandatory for the (technical) functioning of the Schengen Information System, Visa Information System, European Dactyloscopy Database, Entry/Exit System, European Travel Information and Authorisation System, and European Criminal Records Information System for Third-Country Nationals. If, on the other hand, we use "component" to refer to an ancillary or separable tool, then, the MID should be considered as a "component" when complementing the functions pursued by the underlying large-scale information technology systems.

Contextualising the MID functioning in light of its interaction with the other large-scale information technology systems of high-risk envisages the following picture: the MID, despite having been designed as "neutral" by the provider, is conferred an "intended purpose" in its implementation stage. If so, the MID-provider should estimate and evaluate that this component might be used for one or more purposes of Annex III, «[...] under conditions of reasonably foreseeable misuse»[237]. Moreover, if the distributor, importer, or deployer of the MID brings substantial changes[238] to it, they are considered as the (new) providers[239]. Nevertheless, and pending further elaboration on the meaning of the "component" concept under the AI act, in the previous section we concluded that the MID is a standalone high-risk AI system in light of Article 6(2) of the AI act. This assumption reassures us to proceed with our analysis henceforth without delving into the study of the whole interoperability architecture.

c. Temptingly governing the MID-risks

Classifying the MID as a high-risk AI system means complying with most of the rules provided for by the AI act, namely its Chapter III, Section II[240]. Thus, the MID must be supervised throughout its lifecycle based on a risk management system[241]; trained, validated, and tested with quality data sets[242]; technically documented[243]; traceable via log registers[244]; sufficiently transparent[245]; designed and developed so as to be overseen by a natural person (human-in-command)[246]; and safe in terms of accuracy, robustness, and cybersecurity[247]. Compliance with these requirements should be proved by the providers and deployers[248] of the MID: the former being in charge of ensuring that the system is compliant with the requirements imposed by the

[237] Article 9(2)(b) of the AI act and COTINO HUESO, «Los sistemas de inteligencia artificial de alto riesgo: delimitación y análisis de algunos ámbitos», cit., p. 249.

[238] Article 3(23) of the AI act.

[239] Article 25(1)(c) of the AI act. Also, the responsibility would shift to the distributor, importer, or deployer making substantial modifications to the MID, in case the latter is considered as a high-risk AI system by virtue of Article 25(1)(b) of the AI act.

[240] If no high-risk is detected, the provider must document this assessment and register it according to Article 49(2) of the AI act [cfr. Article 6(4) of the AI act].

[241] Article 9 of the AI act.

[242] Article 10 of the AI act.

[243] Article 11 of the AI act.

[244] Article 12 of the AI act, and specifically for the Annex III domains, paragraph (3) thereof.

[245] Article 13 of the AI act.

[246] Article 14 of the AI act.

[247] Article 15 of the AI act.

[248] Article 3(4) of the AI act states that a deployer is «a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity». There is a need to understand who is deploying the MID as this is "used" by many authorities, albeit by a sometimes fully automated process.

AI act, Chapter III, Section II, via the so-called conformity assessment[249], and must demonstrate such conformity at the request of the competent authority, or take corrective actions[250]; the latter should verify that the system is used in accordance with the instructions given by the provider (human-on-the-loop), assign human oversight to natural persons who have the necessary competence, keep the logs automatically generated, and carry out an assessment on the impact on individuals' fundamental rights, including their protection in case of personal data processing[251]. We limit our analysis below to a few salient points of this set of norms, which we estimate relevant in the MID context.

First of all, the conformity assessment of high-risk AI systems listed under Annex III, points 2 to 8[252], is not delegated to a notified body[253] but is self-made, based on internal controls in accordance with Annex VI of the AI act[254]. In other words, the *ex ante* conformity assessment, which is deemed to ensure a high level of trustworthiness in high-risk AI systems[255], is not conducted by a third, independent body[256, 257], as the EDPS wished[258], but is self-regulated by the provider. As a result, the conformity assessment, which should be ready before the MID is placed on the market or put into service, could be criticised for considerably reducing the guarantees ensured by the engagement of a notified body, while burdening the provider of liability entirely. This derogation distinguishes the majority of Annex III-AI systems from Annex I-AI systems[259], e.g. as per Regulation (EU) 2017/745[260] where the self-assessment is reserved to medical devices of low-risk (i.e., class I) while the ones of higher risk (classes IIa, IIb, and III) are always certified by a third-party body[261]. Specifically, Annex VI of the AI act imposes the provider to verify compliance with: Article 17 (quality management system); Chapter III, Section 2 (essential requirements); and Article 72 (post-market monitoring). Though not specified, the provider might rely on the presumption of conformity based on the harmonised standards or common specifications that the European standardisation organisations or the European Commission

[249] Article 43 of the AI act.

[250] Article 16 of the AI act.

[251] Articles 26 and 27 of the AI act.

[252] Point 1 refers to biometrics and Article 43(1) of the AI act imposes the provider to opt for a notified-body conformity assessment when: harmonised standards referred do not exist, and common specifications are not available; the provider has not applied, or has applied only part of, the harmonised standard; the common specifications exist, but the provider has not applied them; and one or more of the harmonised standards has been published with a restriction, and only on the part of the standard that was restricted.

[253] Article 3(22) of the AI act.

[254] Annex VI delegates to the AI system provider the tasks of verifying the quality management system, examining the information contained in the technical documentation, and verifying the design and development process of the AI system, and its post-market monitoring.

[255] Recital (123) of the AI act.

[256] Which is the general rule under Article 31(4) of the AI act.

[257] Articles 28-49 of the AI act. The standardisation procedures are also used for general-purpose AI models.

[258] EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)* (18 June 2021), p. 13.

[259] Article 6(1) of the AI act.

[260] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, *OJ* L 117, 5.5.2017, p. 1.

[261] LAZCOZ MORATINOS/DE MIGUEL BERIAIN, «Is more data always better? On alternative policies to mitigate bias in Artificial Intelligence health systems», *Bioethics* (forthcoming).

would elaborate on, respectively[262]. Otherwise, the provider must justify complying with the AI act regulation on high-risk AI systems by implementing appropriate technical solutions[263]. Only one conformity assessment procedure is needed, even when the high-risk AI system has a self-learned capacity as it happens with the MID, unless changes and performances are not pre-determined[264]. Hence, the assessment is to be repeated if even one of these occurs. Actually, the European Commission may also decide to subject the MID to the conformity assessment procedure of Annex VII by making use of delegated powers for «[…] preventing or minimising the risks to health and safety and protection of fundamental rights posed by such systems, as well as the availability of adequate capacities and resources among notified bodies»[265]. A hetero-evaluation would be more transparent and reassuring than a self-made one, but external supervision might not be welcome in the (old) justice and home affairs area.

Moving on Chapter III, Section II, of the AI act we note that Article 49 imposes the providers of high-risk AI systems listed in Annex III to register them in a specific EU database[266] before their placing on the market or putting into service (except for critical infrastructures)[267]. Such EU database stores valuable information on the provider and deployer[268] of a high-risk AI system, together with the circumstances surrounding the conformity assessment carried out. The EU database must remain accessible and publicly available in a user-friendly manner[269]. Nevertheless, for high-risk AI systems in the areas of law enforcement, migration, asylum, and border control management[270] the registration is performed in a secure non-public section of the EU database mentioned[271]. Access to this secret section is not granted to the market surveillance authorities[272], but to the European Commission, national data protection supervisory authority, or any other designated authority pursuant to Articles 41 to 44 of the LED that act on their behalf[273]. Despite the unfortunate drafting of Article 74(8) and (9) of the AI act, we believe that the EDPS would be granted access to that section as far as large-scale information technology systems and interoperability components are concerned[274]. However, we cannot forget that the

[262] Articles 40(1) and 41(3) of the AI act.

[263] Article 41(5) of the AI act.

[264] Article 43(4) of the AI act.

[265] Article 43(6) of the AI act: «[…] taking into account the effectiveness of the conformity assessment procedure based on internal control referred to in Annex VI in preventing or minimising the risks to health and safety and protection of fundamental rights posed by such systems, as well as the availability of adequate capacities and resources among notified bodies».

[266] Article 71 of the AI act. The information to be included in the database is set out in Annex VIII.

[267] SEGURA SERRANO, «Cybersecurity: Towards a Global Standard in the Protection of Critical Information Infrastructures», *European Journal of Law and Technology*, n. 3, 2015.

[268] Articles 26(8) and 49(3) of the AI act states that deployers that are public authorities, Union institutions, bodies, offices or agencies shall register themselves in the EU database as well.

[269] Article 71 of the AI act.

[270] Article 49(4) of the AI act does not mention justice administration and democracy which would cover the European Criminal Records Information System for Third-Country Nationals.

[271] For a critic see EDPB-EDPS, *Joint Opinion 5/2021*, cit., p. 20.

[272] Article 74(9) of the AI act.

[273] EDPB, EDPB adopts statement on DPAs role in AI Act framework, EU-U.S. Data Privacy Framework FAQ and new European Data Protection Seal (17 July 2024) https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_en (access 5.02.2025).

[274] Article 74(8) of the AI act, namely, the *Agencia Española de Protección de Datos* (AEPD) and the *Consejo General del Poder Judicial* (CGPJ) in Spain.

EDPS' powers have been limited to the data protection field originally[275]. Thus, its competence is quite limited compared to the huge control required under the AI act. If so, the EDPS may request and access any document created or maintained under the AI act–e.g., the technical documentation of Annex IV of the AI act that remains on the premises of law enforcement, immigration, and asylum authorities[276]–for auditing purposes[277] within the limits of its jurisdiction[278]. Overall, the information to be included in the EU database secret section is fragmentated and it does not contemplate, for example, a description of the information used by the system (input data) and its operating logic, a summary of the findings of the fundamental rights impact assessment, or a summary of the main characteristics of the plan for testing in real world conditions[279].

Testing of high-risk AI systems in the areas of law enforcement, migration, asylum, and border control management in real-world conditions, and outside the AI regulatory sandbox[280], is, therefore, not registered for accountability purposes[281]. We should recall that the training, validation, and testing of high-risk AI systems (like the MID) is an indispensable step for detecting the most appropriate and targeted risk management measures[282], for example, to protect children and vulnerable groups of people[283]. If performed in real-world conditions, freely-given informed consent shall be obtained from the subjects affected[284] since testing may require using sets of personal data, which ensures that the AI system performances are of quality once placed on the market or put into service. Thus, Article 10(5) of the AI act, on the governance and management of the information used for training purposes, legitimises the secondary use of special categories of personal data (like biometric data) for bias detection and correction, «[...] subject to appropriate safeguards for the fundamental rights and freedoms of natural persons»[285, 286]. In short, migrants' data hitherto stored in the six underlying large-scale information technology systems could be lawfully reused (without their consent) to train the MID unless

[275] Article 57 of the EUDPR. It is therefore not clear to date whether this body is sufficiently competent to supervise AI on a broad scale.

[276] Article 78(3), paragraph 2, of the AI act.

[277] Article 16(k) of the AI act. Article 80 of the AI act empowers the market surveillance authority to examine an AI system in case it suspects that it poses a high-risk despite the provider's initial assessment.

[278] Article 77(1) of the AI act. For Spain, cfr. the list of authorities published by the *Ministerio para la Transformación Digital y de la Función Pública,* https://digital.gob.es/dam/es/portalmtdfp/DigitalizacionIA/AuthoritiesFundamentalRights-Spain.pdf (access 10.12.2024).

[279] Article 49(4) of the AI act and the selected information of Annexes VIII and XIX.

[280] For an overview, cfr. RANCHORDÁS, «Experimental Regulations and Regulatory Sandboxes: Law without Order?», *University of Groningen Faculty of Law Research Paper Series*, n. 10, 2021, https://ssrn.com/abstract=3934075; specific in the border controls sector, instead, MOLNAR, «Technological Testing Grounds and Surveillance Sandboxes: Migration and Border Technology at the Frontiers», *Fletcher F. World Aff.*, n. 2, 2021.

[281] Article 60(4)(c) of the AI act.

[282] Article 9(6) of the AI act.

[283] Article 9(9) of the AI act.

[284] Article 61 of the AI act.

[285] E.g., for public interest, scientific or historical research purposes as per RECUERO LINARES, «La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado», *AEDPS*, 2019, pp. 26 ff. In case of using the research and innovation legal basis, the AI act might not apply until the model is being placed on the market or put into service as per Article 2(8) of the AI act.

[286] Article 10(5) of the AI act.

synthetic or anonymised data are usable[287], and without encroaching upon Articles 22 of the GDPR and 11 of the LED. However, training the MID on real, historical personal data (e.g., fingerprints) could be risky in view of the poor quality of old data[288]. Personal data must be complete, exempted from errors, and «reflecting the specific geographical, behavioural, contextual or functional setting within which they are intended to be used» in order to benefit from the AI act presumption of conformity[289]. The recent opinion of the EDPB deserves special attention in this regard[290]: by describing the whole algorithm life-cycle, the EDBP opts for a case-by-case evaluation of the interests and rights of the data subjects at stake–e.g., their legitimate expectation to retain control over the processing of personal data–on the one hand, and the need to train and validate algorithm technology on high-quality data sets, on the other. Accordingly, testing plans are extremely important to build a trustworthy high-risk AI system, and limiting the EDPS' access to them may be detrimental to guaranteeing migrants' rights.

Obligations incumbent on the providers of high-risk AI systems in the design stage–i.e., before they are placed on the market or put into service–, aim to ensure transparency through the AI value chain and, specifically, they converge into a series of instructions favoring deployers and the AI system human oversight[291]. Deployers occupy a privileged position for watching over the real functioning of high-risk AI systems and, consequently, must ensure compliance with the instructions received by the provider. Specifically, the deployer of a high-risk AI system must elaborate a fundamental rights impact assessment[292], contemplating how the AI system is used in line with the intended purposes, with which frequency, which impact it would have on specific persons or groups, as well as the mitigation measures employed to combat the risks detected. Because of their proximity to the end-user, deployers are expected to watch over both AI and data protection rules. Hence, the fundamental rights impact assessment is deemed to complement the data protection one[293] and, as a last resource, supports the deployer's obligation of informing the individual about the risks they are subjected to[294]. Specifically, deployers must give «[…] clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken» if they consider that the automated decision-making has an adverse impact on their health, safety, or fundamental rights[295]. The explainability requirement–whose link with the EU's automated decision-making regulation is clear[296]–aims to reduce the black box dilemma and implies the possibility of interpreting the

[287] Article 54(3), last paragraph, of regulation (EU) 2019/817 confers such competence to eu-LISA. On this subject, cfr. EU-LISA, «Artificial Intelligence in the Operational Management of Large-scale IT Systems», *Research and Technology Monitoring Report*, 2020, p. 12.

[288] EUROPEAN COURT OF AUDITORS, *Artificial Intelligence initial strategy and deployment roadmap*, 2024, https://www.eca.europa.eu/ECAPublications/ECA-AI-Strategy-2024-2025/ECA-AI-Strategy-2024-2025_EN.pdf (access 5.02.2025), pp. 14 ff.

[289] Article 42(1) of the AI act ensures a presumption of compliance with Article 10(4) of the AI act if this requisite is met.

[290] EDPB, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models* (17 December 2024), p. 16

[291] Articles 3(15) and 16 of the AI act.

[292] Article 27 of the AI act.

[293] Article 27(4) of the AI act.

[294] Article 26(11) of the AI act.

[295] Article 86(1) of the AI act.

[296] Again, the link with the EU's automated decision-making regulation is clear since Article 86(3) of the AI act limits its application to the extent that such a right is not already guaranteed under Union law, clearly hinting at existing automated decision-making regulation.

machine's output[297] and the provision of instruction on its functioning[298]. Brought to our field of analysis means understanding why the MID generates a link of a specific colour, including when this follows the machine's self-learning capability. In the same vein, MID-deployers[299] should acknowledge how this component performs with specific persons or groups of persons affected so as to prevent racial bias[300] while reducing false and error rates. Back in 2018, the EU Agency for Fundamental Rights (FRA) advanced some of these concerns, pointing out that: «The risk of discrimination is highest with the Multiple Identity Detector, which needs to be carefully assessed from different perspectives. The first one relates to sex. Women more frequently change their last name than men [...] Also other groups of individuals – for example people from societies where certain names are very frequent (e.g. Mr/Ms Lee; Mohammed; etc.) – are likely to face more problems than others when their identities are verified»[301]. Although welcoming Article 5 of the interoperability regulations, the FRA noted that this specific provision recalls the imperative prohibition of discrimination[302] without mentioning colour as discrimination grounds in case of false biometric matches. Exempting the interoperability framework from the AI act means circumventing these safeguards as the preparatory stage of the MID would end before 2 August 2027.

5. Final remarks and steps forward

From the very beginning, the use of new advanced technologies in the AFSJ has been questioning the compatibility of the interoperability framework with the EU's rules affording protection to the individual. The focus of attention is now channeled onto the recently adopted AI act, and the underlying safeguards agreed upon to counteract the interferences caused by smart computer tools. According to Article 111(1) of the AI act, the EU's freedom, security, and justice systems and components are not exempt from the prohibition of Article 5, while their submission to the other rules of the AI act is exempted until 31 December 2030 if they are placed on the market or put into service before 2 August 2027. Our study attempted to conduct a pre-evaluation framing the MID within the AI act dispositions. In concrete terms, we questioned the intelligent nature of interoperability in the AFSJ by taking into consideration the MID, and its correlated procedure, in light of the rules concerning general-purpose and high-risk AI systems.

Our study elucidated that the MID can be considered an AI system according to the (albeit criticised) definition foreseen in Article 3(1) of the AI act. The AI act considers that any AI system

---

[297] Article 13(1) of the AI act.

[298] Article 13(2) and (3) of the AI act.

[299] According to the definition in the AI act, Article 3(4), deployers means «a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity». Strictly speaking, all those authorities entering or rectifying personal data in the underlying large-scale information technology systems and the Common Identity Repository (on which the MID feeds) should be considered deployers in the AI act jargon. Human oversight over the MID, instead, might be delegated to a competent authority to monitor it and interpret given outputs.

[300] DELOITTE, «Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security. Volume 2: Addendum», *Study for the European Commission*, 2020, https://op.europa.eu/en/publication-detail/-/publication/c8823cd1-a152-11ea-9d2d-01aa75ed71a1/language-en (access 4.02.2025), p. 26.

[301] FRA, «Interoperability and fundamental rights Implications», *Opinion of the European Union Agency for Fundamental Rights*, 2018, https://fra.europa.eu/en/publication/2018/interoperability-and-fundamental-rights-implications (access 4.02.2025), p. 13.

[302] Article 21 of the CFREU.

shall be made up of three main elements (machine-based, certain autonomy, and inferring capacity) that the MID meets, with it being a machine learning system with a supervised learning model. Afterwards, we analysed whether the MID is configured to pursue generality and different purposes, since general-purpose AI systems must fulfil *ad hoc* transparency rules under the AI act, which tries to mitigate their inherent opacity. We ruled out the possibility of the MID being a generative AI system (such as ChatGPT) because the link-colours generated are associated with pre-tuned probabilistic thresholds, despite its large-scale rank and high capabilities. Yet, an examination of the MID link searching and error detection functions prompted us to disclose its general-purpose AI nature and, consequently, its regulation under Chapter V of the AI act.

In concrete terms, the MID may be considered a general-purpose AI system with systemic risks under Article 51(1) of the AI act, considering the input and output modalities of its model; its adaptability to learn new, distinct tasks, as well as its autonomy and scalability; and, finally, the huge number of registered end-users. In addition, the MID is estimated to be a general-purpose AI system when the cumulative amount of computation used for its training, measured in floating point operations, is greater than 10^{25}. If so, eu-LISA (that plays the MID provider role) must respect the transparency obligations set down in Article 53 of the AI act, notify the European Commission about its systemic risk general-purpose AI nature, and comply with the enhanced safeguards set down in Article 52 of the AI act. These rules do not provide for exemptions for the AFSJ, which means that eu-LISA should engage with the AI Office at an early stage to anticipate the adversarial effects of the MID and, also, that the agency would be in charge of assessing and mitigating the MID-risk continuously following its release on the market. Moreover, the MID would be included in the European Commission's public list of general-purpose AI systems with systemic risk, without restrictions other than confidentiality.

Our final thoughts focused on the possibility that the MID is classified as a high-risk AI system by virtue of Article 6 of the AI act. Indeed, as soon as general-purpose AI systems are attributed a specific purpose–even through their integration with other AI systems–these must be considered as having been placed on the market or put into service according to the AI act risk-based pyramid. Considering that interoperability is a freedom, security, and justice cross-cutting reform, we have considered that the MID is a high-risk AI system due to falling under the scope of Annex III of the AI act, points (6) to (8). This classification is straightforward if we consider that the MID assists in evaluating certain aspects related to natural persons, that is, it profiles individuals, as per Article 6(3) of the AI act. Consequently, the MID providers and deployers must comply with Chapter III, Section II, of the AI act which requires, for example, training, testing, and validating the high-risk AI models with updated, corrected, and sufficiently representative sets of personal data. Given that this "pre-operational" phase contemplates the processing of migrants' data already centrally stored, we concluded that the MID provokes significant interferences in their privacy and data protection rights, with fallouts on the whole algorithm value chain. Overall, our study found that ignoring the AI act from the outset as per the Article 111(1) exemption means disregarding the real impact the MID will have on third-country nationals, provided that the whole upstream preparation phase falls out of its scope.

6. Bibliography

ALPAYDIN, Ethem, *Machine Learning*, revised and updated ed., The MIT Press, Cambridge/Massachusetts, 2021.

BELLANOVA, Rocco/GLOUFTSIOS, Georgios, «Formatting European security integration through database interoperability», *European Security*, n. 3, 2022, pp. 454-474.

BIGO, Didier/CARRERA, Sergio/HAYES, Ben et al., «Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals (December 18, 2012)», *CEPS Papers in Liberty and Security in Europe*, 2012, pp. 1-90.

BOEHM, Franziska, «Information Sharing in the Area of Freedom, Security and Justice—Towards a Common Standard for Data Exchange Between Agencies and EU Information Systems», in GUTWIRTH, Serge/LEENES, Ronald/DE HERT, Paul et al. (eds) *European Data Protection: In Good Health?*, Springer, Berlin, 2012, pp. 143-183.

BOMMASANI, Rishi/HUDSON, Drew A./ADELI, Ehsan et al., «On the Opportunities and Risks of Foundation Models», *Center for Research on Foundation Models (CRFM)*, 2021, pp. 1-212.

BUTTERFIELD, Andrew/EKEMBE NGONDI, Gerard/KERR, Anne, *A Dictionary of Computer Science*, ed. 7th, OUP Oxford, Oxford, 2016.

CAGGIANO, Giandonato, «L'interoperabilità fra banche-dati dell'Unione sui cittadini degli Stati terzi», *Diritto, Immigrazione e Cittadinanza*, n. 1, 2020, pp. 170-184.

CASTILLO PARRILLA, José Antonio, «Inteligencia artificial de uso general, modelos fundacionales (y "Chat GPT") en el Reglamento de inteligencia artificial», in SIMÓN CASTELLANO, Pere/COTINO HUESO, Lorenzo (eds), *Tratado sobre el Reglamento de Inteligencia. Artificial de la Unión Europea*, Aranzadi, Navarra, pp. 757-777.

CATANZARITI, Mariavittoria/CURTIN, Deirdre «Beyond Originator Control of Personal Data in EU Interoperable Information Systems: Towards Data Originalism», in CURTIN, Deirdre/CATANZARITI, Mariavittoria (eds), *Data at the boundaries of European law*, Oxford University Press, Oxford, 2023, pp. 133-174.

COBBE, Jennifer, «Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making», *Legal Studies*, n. 4, 2019, pp. 636-655.

DE HERT, Paul, «What are the Risks and What Guarantees Need to be Put in Place in View of Interoperability of Police Databases?», *Area of Justice, Freedom & Security, Collection of Standard Bri*, 2006, pp. 169-183.

DE MIGUEL BERIAIN, Iñigo, «¿Explicar o predecir?», *Investigación y ciencia*, n. 538, 2021, pp. 52-53.

DE MIGUEL BERIAIN, Iñigo, «La utilización de datos con fines de investigación científica (XXI)», in COTINO HUESO, Lorenzo (ed), *La Carta de Derechos Digitales,* Tirant lo Blanch, Valencia, 2022, pp. 299-326.

DE MIGUEL BERIAIN, Iñigo/LAZCOZ MORATINOS, Guillermo/SANZ ECHEVARRÍA, María Begoña, «Machine learning in the EU health care context: exploring ethical, legal and social issues», *Information Communication & Society*, n. 8, 2020, pp. 1139-1153.

DEL VALLE GÁLVEZ, Alejandro «La Fragilidad de los Derechos Humanos en las fronteras exteriores europeas, y la Externalización / Extraterritorialidad de los controles migratorios», in SOROETA LICERAS, Juan/ALONSO MOREDA, Nicolás (eds), *Anuario de los cursos de derechos humanos de Donostia-San Sebastián Vol. XVIII*, Tirant lo Blanch, Valencia, 2019, pp. 25-49.

EBERS, Martin/R.S. HOCH, Veronica/ROSENKRANZ, Frank et al., «The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)», *Multidisciplinary Scientific Journal*, n. 4, 2021, https://doi.org/10.3390/j4040043, pp. 589-603.

EL NAQA, Issam/MURPHY, Martin J., *What is Machine Learning?*, Springer, Berlin, 2015.

ESCAJEDO SAN-EPIFANIO, Leire, «El reconocimiento biométrico en el Reglamento de inteligencia artificial: exenciones, prohibiciones y especialidades de alto riesgo», in SIMÓN CASTELLANO, Pere/COTINO HUESO, Lorenzo (eds), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi, Navarra, 2024, pp. 183-235.

FERNÁNDEZ-LLORCA, David/GÓMEZ, Emilia/SÁNCHEZ, Ignacio et al., «An interdisciplinary account of the terminological choices used by EU policymakers ahead of the final agreement on the AI Act: AI system, general purpose AI system, foundation model, and generative AI», *Artificial Intelligence and Law*, 2024, https://doi.org/10.1007/s10506-024-09412-y.

FERRARIS, Valeria, «Eurodac e i limiti della legge: quando il diritto alla protezione dei dati personali non esiste», *Diritto, Immigrazione e Cittadinanza*, n. 2, 2017, pp. 1-15.

FINOCCHIARO, Giusella, «The regulation of artificial intelligence», *AI & Society*, n. 39, 2024, pp. 1961-1968.

FLORIDI, Luciano, «The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU», *Philosophy & Technology*, vol. XXXIII, 2020, pp. 369-378.

FORLATI, Serena, «L'ingresso dei migranti irregolari nell'Unione Europea – Fra controllo dell'immigrazione clandestina ed esigenze di protezione» in MILITIELLO, Vincenzo/SPENA, Alessandro (eds), *Il traffico di migranti – Diritti, tutele, criminalizzazione*, Giappichelli, Torino, 2015, pp. 37-59.

FORTI, Mirko, «Flussi migratori e protezione dei dati personali: alla ricerca di un punto di equilibrio tra sicurezza pubblica e tutela della privacy dei migranti e dei rifugiati all'interno del territorio europeo», *Rivista di Diritto dei Media*, n. 2, 2020, pp. 212-230.

GALLI, Francesca «Interoperable law enforcement: cooperation challenges in the EU area of freedom, security and justice», *Working Paper EUI RSCAS*, 2019, pp. 1-20.

GÓMEZ-CARMONA, Oihance/CASADO-MANSILLA, Diego/LÓPEZ-DE-IPIÑA, Diego et al., «Human-in-the-loop machine learning: Reconceptualizing the role of the user in interactive approaches», *Internet of Things*, n. 25, 2024, pp. 1-17.

GONZÁLEZ FUSTER, Gloria/DE HERT, Paul/Gutwirth, Serge, «Privacy and Data Protection in the EU Security Continuum», *CEPS Papers in Liberty and Security in Europe,* 2011 pp. 1-11.

GSTREIN, Oskar J./HALEEM, Noman/ZWITTER, Andrej, «General-purpose AI regulation and the European Union AI Act», *Internet Policy Review: Journal on internet regulation*, n. 3, 2024, https://doi.org/10.14763/2024.3.1790, pp. 1-26.

GUTIERREZ, Carlos I./AGUIRRE, Anthony/UUK, Risto et al., «A Proposal for a Definition of General Purpose Artificial Intelligence Systems», *Digital Society*, n. 2, 2023, https://doi.org/10.1007/s44206-023-00068-w, pp. 1-8.

HACKER, Philipp/ENGEL, Andreas/MAUER, Marco, «Regulating ChatGPT and other Large Generative AI Models», VVAA (eds), *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency,* Association for Computing Machinery, New York, 2023, pp. 1112-1123.

HAMON, Ronan/JUNKLEWITZ, Hendrik/SANCHEZ, Ignacio et al., «Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making», *IEEE Xplore*, n. 1, 2022, pp. 72-85.

JANIESCH, Christian/ZSCHECH, Patrick/KAI, Heinrich, et al., «Machine learning and deep learning», *Electron Markets*, Springer, Berlin, 2021, pp. 685-695.

KLABBERS, Jan, *The Law of International Organizations*, Cambridge University Press, United Kingdom/United States, Cheltenham/Northampton, 2015.

KURIAN, Nomisha, «'No, Alexa, no!': designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models», *Learning, Media and Technology*, 2024, https://doi.org/10.1080/17439884.2024.2367052, pp. 1-14.

LAZCOZ MORATINOS, Guillermo*, Gobernanza y supervisión humana de la toma de decisiones automatizada basada en la elaboración de perfiles*, Universidad del País Vasco UPV/EHU, Leioa, 2022.

LAZCOZ MORATINOS, Guillermo/DE MIGUEL BERIAIN, Iñigo, «Is more data always better? On alternative policies to mitigate bias in Artificial Intelligence health systems», *Bioethics* (forthcoming).

LEESE, Matthias, «AI and interoperability», in PAUL, Regine/CARMEL, Emma/COBBE, Jennifer (eds), *Handbook on Public Policy and Artificial Intelligence*, Edward Elgar Publishing, Cheltenham/Camberley, 2024, pp. 146-157.

LODGE, Juliet, *Are You Who You Say You Are? The EU and Biometric Borders,* W.L.P. (Wolf Legal Publishers), Oisterwijk, 2007.

MALGIERI, Gianclaudio, «Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations», *Computer Law & Security Review*, n. 35, 2019, pp. 1-26.

MALGIERI, Gianclaudio, «Vulnerable data subjects», *Computer Law & Security Review*, vol. XXXVII, 2020, pp. 1-22.

MANGAS MARTÍN, Araceli, «Las competencias de la Unión Europea», in MANGAS MARTÍN, Araceli/LIÑÁN NOGUERAS, Diego Javier (eds), *Instituciones y Derecho de la Unión Europea*, Tecnos, Madrid, 2024, pp. 77-94.

MARTÍN JIMÉNEZ, Francisco Javier, «Inteligencia artificial y ética: hacia una aplicación de los principios éticos en el ámbito de la UE», *Cuadernos Europeos de Deusto*, n. 68, 2023, https://doi.org/10.18543/ced.2699, pp. 89-115.

MOLNAR, Petra, «Technological Testing Grounds and Surveillance Sandboxes: Migration and Border Technology at the Frontiers», *Fletcher F. World Aff.*, n. 2, 2021, pp. 109-118.

NOVELLI, Claudio/CASOLARI, Federico/HACKER, Philipp et al. «Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity», *Working Paper*, n. 55, 2024, pp. 1-16.

PALMA ORTIGOSA, Adrián, *Decisiones automatizadas y protección de datos: Especial atención a los sistemas de inteligencia artificial*, Dykinson, Madrid, 2022.

QUINTEL, Teresa, «Interoperable Data Exchanges within different Data Protection Regimes - The case of Europol and the European Border and Coast Guard Agency», *European Public Law*, n. 1, 2020, pp. 205-206.

RANCHORDÁS, Sofia, «Experimental Regulations and Regulatory Sandboxes: Law without Order?», *University of Groningen Faculty of Law Research Paper Series*, n. 10, 2021, https://ssrn.com/abstract=3934075, pp. 1-39.

SAVINO, Mario, «Global administrative law meets "soft" powers: The uncomfortable case of Interpol red notices», *N.Y.U. J. Int. L. & Pol.*, n. 43, 2010, pp. 263-336.

SEGURA SERRANO, Antonio, «Cybersecurity: Towards a Global Standard in the Protection of Critical Information Infrastructures», *European Journal of Law and Technology*, n. 3, 2015, pp. 1-24.

SMUHA, Nathalie/AHMED-RENGERS, Emma/HARKENS, Adam et al., «How the EU can achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act», *LEADS Lab @University of Birmingham. For a Legal, Ethical & Accountable Digital Society*, 2021, pp. 1-59.

TASSINARI, Francesca «La institucionalización de la competencia operativa de la Unión Europea para la gestión y la interoperabilidad de los sistemas informáticos de gran magnitud del Espacio de Libertad, Seguridad, y Justicia: eu-LISA», *La Ley Unión Europea*, n. 111, 2023, pp. 1-38.

TASSINARI, Francesca, «ADM in the European Union: An Interoperable Solution», in LEGIND LARSEN, Henrik/MARTIN-BAUTISTA, María J./RUIZ, M. Dolores et al. (eds), *Flexible Query Answering Systems. FQAS 2023. Lecture Notes in Computer Science*, Springer, Cham, 2023, pp. 290-303.

TASSINARI, Francesca, *Data Protection and Interoperability in EU External Relations*, Brill/Nijhoff, Leiden/Boston, 2024.

VALLS PRIETO, Javier, *Inteligencia artificial, derechos humanos y bienes jurídicos*, Aranzadi, Navarra, 2021.

VAVOULA, Niovi, *Immigration and Privacy in the Law of the European Union*, Brill/Nijhoff, Leiden/Boston, 2022.

VEALE, Michael/ZUIDERVEEN BORGESIUS, Frederik, «Demystifying the Draft EU Artificial Intelligence Act», *Computer Law Review International*, n. 22, 2021, https://ssrn.com/abstract=3896852, pp. 97-112.

YANG, Luodongni, «Research on the legal regulation of Generative Artificial intelligence Take ChatGPT as an example», *SHS Web of Conferences*, n. 02017, 2023, https://doi.org/10.1051/shsconf/202317802017, pp. 1-10.

ZHOU, Zhi-Hua, *Machine Learning*, Springer, Berlin, 2021.