COMPARATIVE LAW REVIEW

Comparative Law Review

VOL. 17 · N. 1 · 2026

SPECIAL ISSUE

European Law and Digital Technologies

ISSN
2038 – 8993

OPEN ACCESS JOURNAL

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE
LAW
REVIEW
VOL. 17/1 – 2026

SPECIAL ISSUE

European Law and Digital Technologies

Edited by Federica Giovanella

DATA PROTECTION AT THE GATE
PERSONAL DATA OF THIRD-COUNTRY NATIONALS IN THE EU ENTRY/EXIST SYSTEM

Alessandro Catano

TABLE OF CONTENTS:

Migration management has become a central issue for developed countries. In recent years, especially due to terrorism and the breaking out of new wars, the European Union (EU) has undertaken the fundamental task of effectively implementing digital technologies to control the flow of third-country nationals within its territory.
There is a growing body of legislation that strives to regulate each aspect of migration with the objective of coordinating freedom of movement and security. Within this hive of laws, back in 2017 the EU adopted Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES) to register entry and exit data and refusals of entry 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.
The aim of this essay is to explore how the newly operational EES impacts on the data protection framework outlined by the EU and on the main principles therein, in connection with the fundamental rights of third-country nationals.
The paper begins by exploring the main novelties introduced by the EES Regulation, first of all clarifying the role and scope of the EES with respect to the systems already in use (such as the EURODAC, the VIS, and the SIS II) and then dissecting its main contents. It will then go on to analyse the compliance of the EES with EU data protection law, diving into the consequences on the access to and processing of personal data. Given these insights, the essay will assess the limitations set by the new large-scale IT system to the main principles of data protection, especially investigating whether the EES creates the grounds for a violation of purpose limitation, the rights to information, access and transparency as well as the mandate of data accuracy.
The significance of the study cannot be underestimated, as it poses fundamental questions on the future of smart borders initiatives featuring mass data processing activities, the direction of EU law with respect to the rights of third-country nationals and the porous boundaries between the administrative and criminal sphere.

Keywords: Persona data ─ data protection ─ GDPR ─ migration ─ Entry/exit System ─ fundamental rights ─ purpose limitation ─ transparency ─ data accuracy ─ large-scale IT systems

I. INTRODUCTION

Typing a search query on a search engine in 2025 generates two particular phenomena. As for the first, it is very likely that an AI stemming from the search engine will automatically attempt to give a complete response to the question. The user may, however, decide to resort to the traditional list of websites recommended by the search engine. The second phenomenon unravels as soon as the user clicks on a specific website, as a banner will pop up asking for permissions. In order to access the information or the services provided by the website, the window will ask users to select whether they accept to relinquish the data

processed by the website, whether they would prefer the processing to be limited to the necessary data or whether they reject a collection whatsoever.

More and more frequently, this situation is mirrored at the borders of the richest countries in the world. In order to access the foreign territory, travellers are asked to relinquish their personal data to border authorities, with the difference that, in this case, travellers cannot but accept the conditions imposed by the State if they are determined to set foot in the country. In parallel, their actions, routes and information are processed by experimental artificial intelligence tools in order to predict their movements and prevent migratory emergencies.

In the past two decades, the EU has invested in a substantial number of technological projects and has created a handful of digital infrastructures in order to improve migration management and security at the borders. These digital infrastructures are mostly designed to store the personal data of travellers and use it to supplement border authorities in the identification of people on the move and in the prevention of potential threats.

The Smart Borders package[1] of the European Union promoted the implementation of a new Entry/Exit System (hereafter EES) that would collect the personal data of third-country nationals admitted for a short stay to register electronically the time and place of their entry and exit. To this goal, the Regulation (EU) 2017/2226 (hereafter EES Regulation) was adopted in 2017 to facilitate identification tasks, detect overstays and show entry bans connected to the travellers' identities. Almost 8 years after the act, nonetheless, the system has not yet become fully operative. In addition, the package includes the European Travel Information and Authorisation System (ETIAS), which will issue authorisations to visa-exempt third-country nationals planning a stay in the EU, working as a pre-border check to evaluate the existence of any security, high epidemic or illegal immigration risk. Over time, the two measures put together should replace the stamping of passports, aiming at the digitalisation of border controls[2].

The motives of interest related to these initiatives are manifold. Firstly, studying the digital infrastructures applied to migrations allows our society to better comprehend the phenomenon of "datafication" of borders, consisting in an amplified reliance on big data to direct resources for migration management and take decisions on third-country nationals[3]. Secondly, especially since the Snowden leaks, increasing attention has been devolved to the mass data processing activities performed by States, which risk paving the

[1] The initiative came from the Communication of the EU Commission of 6 April 2016 entitled 'Stronger and Smarter Information Systems for Borders and Security'.

[2] On the digitalisation of borders and bodies see F. Biondi Dal Monte, *Confini digitali e dati dei migranti nel Patto sulla migrazione e l'asilo*, in F. Biondi Dal Monte *et al.* (curr.), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa* (2024).

[3] "Datafication is not simply the process of collecting data about people, but that of transforming bodies, actions, and things into data that can be processed by algorithms" (A. Valdivia *et al.*, *Neither opaque nor transparent: A transdisciplinary methodology to investigate datafication at the EU borders*, in *Big Data and Society*, 9(2), 2 (2022)); see also M. Forti, *Errori algoritmici ai confini: questioni giuridiche e implicazioni politiche*, in F. Biondi Dal Monte *et al.* (curr.), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa*, cit., 109.

way for a new world order characterised by mass surveillance[4]. Thirdly, most scholars share the view that it would be erroneous to conceive large-scale IT systems as mere technical instruments to perform administrative tasks. Rather, databases generate their own semiotics which translates the identities of human beings into digitized figures, flagged and described by their own metrics and, thus, raise new significant political questions[5]. Fourthly, the ancillary yet ubiquitous purposes of law enforcement attached to EU databases speak for the dilution between the administrative and criminal sphere of migration management[6]. "Crimmigration"[7] is a neologism introduced to describe the contemporary geopolitical tendency to presume the foreigner as a source of threat which is due taming with the means necessary. Finally, if data protection can be regarded as non-other than a set of rules for a fair distribution of powers between those who have the authority and power to collect personal data and the people whose data are at stake[8], such asymmetry is all the more visible in the field of immigration, where travellers occupy a position of subordination and dependency towards State authorities and suffer the consequences of their own vulnerability[9]. In light of this asymmetry, the research provides useful evidence to judge whether the EES can be regarded as *proportionate*, in the technical terms developed by the CJEU pursuant to Art. 52 of the EU Charter of Fundamental Rights (EUCFR).

While a growing body of literature has examined most of the databases composing the architecture of the digitized EU borders – including the older European Dactyloscopy (Eurodac), the VISA Information System (VIS) and the Schengen Information System (SIS) –, little attention has been paid to the Entry/Exit System in particular. This study therefore aims to fill the gap in the literature and to contribute to the growing area of European research on digitized borders and data management by exploring the functionalities and the shortcomings of the new EES, in consideration of its start of operations in October 2025. The pages that follow assess the ways in which the EES relates to other databases and to the rest of the data protection framework.

This paper begins by providing the reader with a brief summary of the structure and content of the EES Regulation and a clarification of its role in the complex pool of EU IT systems (Section II). It will then examine the peculiar relationship between the EES

[4] For a thorough analysis of the mass surveillance programs in the EU see D. Bigo *et al.*, *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*, in *Liberty and Security in Europe*, 62, 1–60 (2013).

[5] On the ontological value of databases see R. Bellanova-G. Glouftsios, *Formatting European security integration through database interoperability*, in *European Security*, 31(3), 454–474 (2022); A. Pelizza-W. R. Van Rossem, *Scripts of Alterity: Mapping Assumptions and Limitations of the Border Security Apparatus through Classification Schemas*, in *Science, Technology, & Human Values*, 49(4), 794–826 (2024).

[6] On the topic, *inter alia*, V. Mitsilegas, *The Digital Border and the Rule of Law*, in M. Bergström-V. Mitsilegas (eds.), *EU law in the digital age* (2025); T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, (2024); D. N. Vavoula, *The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection* (2019).

[7] J. Stumpf, *The Crimmigration Crisis: Immigrants, Crime, and Sovereign Power*, in *American University Law Review*, 56(2), 367-419 (2006).

[8] T. Naef, *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*, vol. XXVIII (2023).

[9] S. Penasa, *Intelligenza artificiale e diritti: verso un diritto "algoritmico" dell'immigrazione?,* in F. Biondi Dal Monte *et al.* (curr,), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa,* cit., 23-25.

and the EU data protection framework (Section III), exploring how the powers of designated authorities shift according to the applicable legislative act and highlighting the fundamental principles underlying the data protection regime. Section IV will assess the principles of data protection in relation to the limitations set by the EES. The main issues addressed in the Section will be: whether the EES creates the grounds for a violation of the purpose limitation principle (a); whether it guarantees the rights to information, transparency and access to the data subject (b); whether it respects the mandate of data accuracy (c). Section V will briefly deal with the potential collision between the EES and the regulation of artificial intelligence and summarise the findings of the research with some final remarks.

II. THE ENTRY/EXIT SYSTEM

The EES is no lone wolf in the digitalisation process of EU migration management; rather, it is comprised in an intricate web of separate databases, each one provided with an own fundamental purpose (or, more realistically, multiple purposes), but jointly processing the personal data of all non-EU nationals coming to the EU.

The first wave of large-scale IT systems mainly concerned asylum applicants and criminal suspects and led to the creation of the Schengen Information System (SIS) and of the European Dactyloscopy (Eurodac). The SIS has been operative since 1995 and serves both the purposes of border management[10] and police and judicial cooperation in criminal matters[11]; it additionally facilitates the return of illegally staying TCNs[12]. Eurodac, by contrast, was created in 2002[13] as a fingerprint database used to find the Member State responsible for each asylum application but has now been expanded to become the main asylum large-scale IT system in the New Pact on Migration and Asylum[14]. The most recent addition to the EU databases for law enforcement and judicial cooperation is the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN), which should facilitate exchange of criminal records information on people on the move between Member States[15].

A second category of IT systems is mainly involved with supporting border checks, albeit preserving the possibility of law enforcement access as an additional purpose[16]. In 2008

[10] Regulation (UE) 2018/1861.
[11] Regulation (UE) 2018/1862.
[12] Regulation (UE) 2018/1860.
[13] Regulation (EC) 407/2002.
[14] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Pact on Migration and Asylum, COM/2020/609 final (23.9.2020).
[15] Regulation (EU) 2019/816.
[16] For an analysis of EU databases as multi-purpose tools, see D. N. Vavoula, *The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection*, cit.; see also European Union Agency for Fundamental Rights (hereafter EUFRA), *Under watchful eyes: biometrics, EU IT systems and fundamental rights* (2018).

the EU instituted the VISA Information System (VIS)[17] as a tool to share information on applications and previous decisions on short-stay visas and extended its scope to cover long-stay authorisations in 2021[18]. The EES and ETIAS were included in the Smart Borders Package as separated tools created to cooperate and fill the gaps on short stays in the VIS. While the EES records entries and exits in the Schengen Area, stores entry bans and detects overstayers, ETIAS issues pre-border, short-stay authorisations to visa-exempt TCNs based on shared and already available information. Both fill the gap of control over visa-exempt travellers, thereby achieving the registration into a database of every category of travellers coming to the EU.

Driven by the urgency to respond to growing security pressures – or, as Bellanova and Glouftios would refer to these and other causes, *database anxieties*[19] –, the EU opted for abandoning the compartmentalisation of databases and adopt the Interoperability Regulations[20]. Interoperability consists in creating a common portal[21] containing all the existing EU large-scale IT systems, which would be accessible to all the competent authorities based on their permissions related to each system, in order to allow communication among the databases and, hence, improve cooperation and accelerate information exchange.

The Union's EES is a large-scale IT system containing a repository storing the personal data of TCNs authorised for a short stay. It is equipped to record and show their entries and exits and entry bans and to calculate the duration of their stay in the EU, aiming at automatically identifying overstayers and alert authorities about them. The data subjects of the EES are represented by three categories of travellers[22], authorised to stay in the Schengen Area for 90 days within a period of 180 days, i.e. short-stay visa holders, visa-exempt TCNs and family members of EU citizens or citizens of an equivalent country enjoying free movement but not provided with a residence document. The EES automated calculator is not applied to the latter. Access to personal data is provided to national visa, border and immigration authorities determined by each Member State based on their own assessment of necessity and proportionality[23]. In addition, law enforcement authorities (described as designated authorities in the EES Regulation) and Europol may access the database for law enforcement purposes, precisely in relation to terrorist offences or other serious criminal offences[24]. Carriers have access to a separate daily-updated, read-only version of the database in order to verify short-stay visas[25].

It is not entirely clear whether the European Border and Coast Guard Agency (Frontex) will also be able to process personal data. On the one hand, the text of Art. 63(1) EES

[17] Regulation (EC) 767/2008.
[18] Regulation (EU) 2021/1134.
[19] R. Bellanova-G. Glouftsios, *Formatting European security integration through database interoperability*, in *European Security*, cit.
[20] Regulation (EU) 2019/817 and Regulation (EU) 2019/818.
[21] Specifically, the Interoperability Regulations introduce four new tools with the purpose of connecting the existing databases, i.e, the Common Identity Repository (CIR), the Multiple Identity Detector (MID), the Biometric Matching Service (BMS), the European Search Portal (ESP).
[22] Art. 2, Regulation (EU) 2017/2226.
[23] Arts. 9(1) and 10(1), Regulation (EU) 2017/2226.
[24] Art. 1(2), Regulation (EU) 2017/2226 laying down the legal basis for access to national LEAs and Europol.
[25] Art. 13(3), Regulation (EU) 2017/2226.

Regulation allows the agency to consult the data contained in the EES database "solely for the purposes of reporting and statistics without allowing for individual identification" and lists the information that can be transmitted for these exclusive purposes. On the other hand, the same disposition allows Frontex to process data for risk analysis and vulnerability assessments *as referred to* in Arts. 11 and 13 of its own Regulation and the Frontex Regulation includes risk analysis in Art. 11 among the specific activities that allow the Agency to process personal data[26].

The EES applies to all external borders of the EU (air, sea and land) and to some borders within the EU, namely (a) between a Schengen country and a country applying only the EES, (b) between countries applying only the EES and (c) between a Schengen and a non-Schengen country[27].

One of the most relevant and debated aspects of the system concerns which information its repository is going to store. The database distinguishes the information the authorities should collect based on whether or not the TCN holds a visa[28]. Short-stay visa holders will be first required to declare name, nationality, sex and date and place of birth. Secondly, they will provide a document or a travel document to the database, which registers their expiry date as well. Lastly, visa holders are asked to record their biometric data, hence, a facial image. Fingerprints, by contrast, are assumed to be already present in the VIS database; the Regulation therefore prevents the system from reiterating the registration of the same personal data.

Information varies according to the time of registration. At each entry, the authority signals date and time of entry, border crossing point, traveller category (whether family member of a EU citizen, visa-exempt or visa holder), number of entries authorised, duration and visa sticker number. If present, limited territorial validity of the visa, national facilitation programmes and Facilitated Transit Documents are recorded in this phase as well. On exit, by contrast, date, time and border crossing point are considered relevant and registered.

Visa-exempt travellers are required to relinquish the same data as for visa holders except for the additional obligation to provide four fingerprints from the right hand[29]. The temporary impossibility to provide fingerprints for visa-exempt travellers does not determine a refusal of entry, yet it is registered in the EES. The remaining data are registered *mutatis mutandis*, that is without the information deriving from the visa. Further information is specified when the authorisation is extended, revoked or annulled[30], when entry is rejected to the TCN[31] and when the TCN has no file or EES record[32].

[26] Art. 46, Regulation 2016/1624.
[27] Art. 4, Regulation (EU) 2017/2226.
[28] Arts. 16-17, Regulation (EU) 2017/2226. Art. 16 regulates the personal data processed on visa holders while Art. 17 regulates the personal data processed on visa-exempt TCNs.
[29] Art. 17 (1)(c), Regulation (EU) 2017/2226.
[30] Art. 19, Regulation (EU) 2017/2226.
[31] Art. 18, Regulation (EU) 2017/2226.
[32] Art. 20, Regulation (EU) 2017/2226.

Once the entry procedure is completed, the information regarding the stay of travellers is connected to an automated calculator[33]. The calculator informs travellers and the authorities of the maximum or the remaining duration of authorised stay or the number of remaining entries and, on exit, it alerts authorities on overstays[34]. Once the duration of the stay is exceeded, overstayers are automatically identified and inserted in a list which is provided to the competent national authorities of each Member State, including the personal data processed at their entry[35].

Following the principle of storage limitation, the personal data are stored in the EES central repository for a pre-determined period of time depending on the subject and on the registration of an exit[36]. In general, data is retained in the database for 3 years or only one year for family members of EU nationals. Yet, if the EES displays no exit record, the data of the traveller can be retained for 5 years, thus interpreting overstaying as a just cause to prolong the retention of the traveller's personal data.

Responsibilities in relation to the database are shared between Member States and eu-LISA[37]. For data protection monitoring, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security and integrity, eu-LISA and Member States have an obligation to keep logs, that is documented information regarding access requests and processing operations performed by authorities[38]. National supervisory authorities and the European Data Protection Supervisor (EDPS) are granted access to the logs to enable them to monitor the processing of data and ensure full compliance with applicable data protection rules[39].

III. LEGAL REGIMES COLLIDING: THE DATA PROTECTION FRAMEWORK

The emergence of a market of personal data resulted in the attempts of EU lawmakers as well as the CJEU to find the balance between the desire to ensure the free circulation of such data and the need to protect individuals from harm. As far as the CJEU is concerned, the Court has progressively developed its own dynamic scrutiny of proportionality to analyse the balance between the respect for the fundamental rights to private life (Art. 7 EUCFR) and the right to data protection (Art. 8 EUCFR) and objectives of general interest related to security and crime prevention. In several cases[40], the CJEU examined whether the legislative measures restricting data subjects' prerogatives respected the

33 Art. 11, Regulation (EU) 2017/2226.
34 Art. 12(1), Regulation (EU) 2017/2226.
35 Art. 12(3), Regulation (EU) 2017/2226.
36 Art. 34, Regulation (EU) 2017/2226.
37 Eu-LISA is the European agency for the operational management of large-scale information systems in the area of freedom, security and justice, established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council.
38 Art. 46, Regulation (EU) 2017/2226.
39 Arts. 56(3)-59(3), Regulation (EU) 2017/2226.
40 Cf CJEU, joint cases C-293/12 and C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources*, 08.04.2014; CJEU, case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 06.10.2015; CJEU, joint cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson*, 21.12.2016; CJEU, joint cases C-511/18, C-512/18, C-520/18, *Quadrature du Net and Others v Conseil des ministres*, 27.11.2020.

essence of the fundamental rights, the quality of law requirement and could be considered appropriate as well as the least intrusive means for achieving a legitimate objective (*strict necessity*).

As far as legislative measures are concerned, as Art. 16(2) TFEU entitled the EU to legislate on the matter, the EU established a data protection framework as a common substratum shared by the EES Regulation and the regulations of the other migration databases. The framework consists primarily of three acts: the General Data Protection Regulation (Reg. (EU) 2016/679, hereafter GDPR), the Law Enforcement Directive (Dir. (EU) 2016/680, hereafter LED) and the EU Data Protection Regulation (Reg. (EU) 2018/1725, hereafter EUDPR). These legislative acts constitute a bedrock on which the regulations of EU IT systems can thrive in fairness, each act regulating the processing of personal data as performed by different subjects and for different purposes. The GDPR is the main legislative reference in the field of data protection, as it dictates rules on the conduct of controllers and processors to safeguard the rights and interests of data subjects. The LED provides a framework for Member States governing the processing activities carried out by national law enforcement authorities (hereafter LEAs) for tasks related to criminal offences, criminal penalties or threats to public security. The EUDPR serves as data protection regulation for EU agencies, bodies and institutions. Considering its role, its content appears as a bond between the previous two pieces of legislation, setting rules for the general processing of personal data as well as for the processing in the fields of judicial and police cooperation (operational personal data).

The EES Regulation makes reference to each one of these acts in relation to cases not directly handled within its text[41]. Immigration, visa and border authorities will apply the GDPR when processing personal data for the purposes of verifying the identity and previous registrations of the TCNs, verifying whether they fulfil the conditions for their stay, accessing the automated calculator, examining and deciding on visas and national facilitation programmes[42]. The LED, by contrast, will be applied by national LEAs when they process personal data to prevent, detect or investigate terrorist acts or serious criminal offences[43]. For the same purposes, Europol will apply its own recast Europol Regulation[44], which derogates and prevails over the EUDPR as a *lex specialis*. The rules of the EUDPR will therefore only govern the processing of personal data performed by eu-LISA.

The scheme that has been described illustrates the intricacy of such a system, with a variety of standards which apply to specific sets of circumstances to cope with the different tasks and powers of each authority[45]. Interoperability will arguably complicate the picture even

41 Art. 49, Regulation (EU) 2017/2226.

42 Such uses of the EES by each category of authorities are regulated by Arts. 23-29, Regulation (EU) 2017/2226.

43 See Art. 1(2), Regulation (EU) 2017/2226, then specified by Art. 32 of the same Regulation.

44 The main text is Regulation (EU) 2016/794, which was recently modified by Regulation (EU) 2022/991.

45 E. Kosta, *The Proposed Anti-Money Laundering Authority and the Future of FIU Collaboration in Europe*, in M. Bergström-V. Mitsilegas (eds.), *EU law in the digital age*, cit., 126; see also V. Mitsilegas, *The Digital Border,* in M. Bergström-V. Mitsilegas (eds.), *EU law in the digital age*, cit., 363; T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, 178 ff. (2024).

further, by streamlining access to LEAs and other authorities and consequently challenging the permissions given by each Regulation[46].

The data protection framework contains the necessary legal grounds justifying processing activities on such data. The LED requires LEAs to process personal data only when such activity is based on Member State or Union law and it is necessary and proportionate for purposes related to criminal penalties, criminal offences or public threats. The EES Regulation restricts this possibility even further, limiting processing only to terrorist offences or another serious criminal offence and requiring evidence or reasonable grounds that it would contribute to the case.

The GDPR, by contrast, enlists a series of alternative legal grounds for the controller to process personal data legitimately. In particular, the collection of data for the EES is based on the provision of the GDPR which allows authorities to process personal data when it is necessary to perform a task carried out in the public interest or to comply with a legal obligation stemming from EU or Member State law[47] and laying down the purpose of the processing[48].

Considering that the functioning of the IT system is based on the use of fingerprints and facial images, the EES data fits the special categories of personal data, whose processing is only legitimate in the specific circumstances specified by Art. 9(2) GDPR and Art. 10 LED. Art. 9(2)(g) GDPR allows collecting biometric data for reasons of substantial public interest and on the basis of Union law. The LED requires that such data be processed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject and authorised by Union or Member State law.

Furthermore, the data protection framework places the focus on the responsibility of controllers towards data subjects. Controllers are represented by whoever determines the purposes and means of the processing[49] and, in this case, are impersonated by the subjects authorised to access the database by the EES Regulation. Data subjects, who surrender their personal data, are conferred a crucial series of rights, some of which directly exercisable against controllers. The rights of data subjects are mostly rooted in the principle of transparency and entitle the subject to gain information, access data and amend inaccuracies. While the principle of transparency is shared between the general rules of the EUDPR and the GDPR, it disappears in the LED and Chapter IX of the EUDPR, as ensuring transparent access to the information held by LEAs to the individual would disrupt police investigations.

Besides transparency, the framework establishes a common series of principles that are foundational in order to guarantee data protection. LED, GDPR and EUDPR require the processing of personal data to be lawful and fair (lawfulness), limited to a specific purpose (purpose limitation), adequate and relevant (data minimisation[50]), accurate (data accuracy),

---

[46] V. Mitsilegas, *The Digital Border*, in M. Bergström-V. Mitsilegas (eds.), *EU law in the digital age,* cit., 363; T. Quintel, *Data protection: the GDPR, the law enforcement directive and beyond*, cit., 178, 216, 218.

[47] Art. 6(c) and (e), Regulation (EU) 2016/679.

[48] Art. 6(3), Regulation (EU) 2016/679.

[49] Art. 4(7), Regulation (EU) 2016/679.

[50] It is noteworthy that while the principle limits the processing of personal data to what is necessary in the GDPR, it simply invites to a non-excessive processing in the LED.

limited to a specific time period (storage limitation) and secure (integrity and confidentiality) and require controllers to be responsible for compliance with these principles (accountability)[51]. Section IV will explore the tension between these principles and the EES, analysing whether the infrastructure is in fact able to guarantee the respect of data protection principles and the fundamental rights to private life and data protection.

IV. THE CHALLENGES AHEAD: FUNDAMENTAL RIGHTS AND DATA PROTECTION PRINCIPLES UNDER PRESSURE

This study is unable to encompass the entire list of principles of data protection in connection with the EES Regulation. The analysis of the relationship between the EES and data protection presented here is based on the principles of purpose limitation, transparency and data accuracy, in light of their fundamental role in preserving the integrity of the framework. Subsection (a) considers the implications of a multi-purpose tool uniting law enforcement and migration management objectives on the obligation to connect processing activities to a specified, lawful purpose. Subsection (b) reviews the EES provisions on transparency, the right to information and the right to access, analysing the challenges to their effectivity. Subsection (c) is concerned with the precision of the EES database, aiming to shed light on the progress, inherent obstacles and practical issues to data accuracy. The elements gathered in the analysis of these three principles provide valuable insights into whether the EES would withstand the scrutiny of proportionality stemming from Art. 52 EUCFR.

a. *Purpose Limitation Principle*

An episode of the TV series "Black Mirror" shows a dystopian future in which government-approved drone insects, which were originally equipped for pollination tasks substituting for extinct real bees, are hacked with the goal of killing targeted people[52]. Halfway through the episode, it is revealed that facial image recognition tools had been secretly installed in each and every high-tech bee for urgent cases undermining national security.

The principle of purpose limitation is on the front line to prevent events of function creep like those described in the episode, i.e. the expansion of a system or technology beyond its original purposes[53]. By introducing purpose limitation, fundamental rights[54] and the EU data protection framework[55] require personal data to be processed for specified, explicit

[51] Art. 4(1)(2), Directive (EU) 2016/680; Art. 5(1)(2) Regulation (EU) 2016/679; Art. 4(1)(2), Regulation (EU) 2018/1725.
[52] Reference is made to "Hated in the Nation", the sixth episode of the third season of Black Mirror, aired for the first time in 2016.
[53] B.J. Koops, *The concept of function creep, in Law, Innovation and Technology*, 13(1), 29–56 (2021).
[54] "[D]ata must be processed fairly for specified purposes" (Art. 8(2), Charter of Fundamental Rights of the European Union).
[55] See Section III.

and legitimate purposes and not be processed in a manner that is incompatible with those purposes[56]. The principle is strictly connected with the mandate to process personal data only when strictly necessary (strict necessity) and only in the relevant and adequate amount (data minimisation), preventing excessive and potentially detrimental processing activities. To the same end, controllers are asked to put in place organisational and technical measures to ensure that the systems exclusively authorise access to designated staff and for predetermined purposes (privacy by design)[57].

As mentioned in Section II, the EES pursues the parallel objectives of improving border management and tackling irregular immigration, on the one hand, and contributing to the prevention, detection and investigation of serious crimes and terrorism, on the other hand[58]. While European Union acts with multiple purposes are not illegitimate, the CJEU clarified that the purposes should be inextricably linked and connected to the appropriate legal bases and the procedures for adopting them should not be incompatible with one another[59]. The legal bases chosen for the EES Regulation are Art. 77(2)(b) and (d), allowing for measures establishing controls for the crossing of external borders, and Art. 87(2)(a) TFEU, allowing for measures concerning police cooperation to prevent and combat crime[60]. While the legal bases and their procedures for adoption are arguably reciprocally compatible, it is questionable whether the law enforcement and migration management purposes exhibit the *inextricable link* required by the CJEU[61]. In any case, the association of these legal bases incarnates the increasing dilution between criminal and migration law.

While the uses of personal data may be justified for administrative purposes, studies show a growing concern that the involvement of LEAs in data management activities would pose significant risks to the individual, causing a spillover effect[62]. To address the issue, the efforts of the EES Regulation are directed at articulating the access permissions of each authority depending on the task they are carrying out and compartmentalising purposes for access in different chapters of the Regulation[63]. The EES Regulation enlists the specific search goals, the authorities authorised to start the search for that goal, the data that can be inserted to start the search and the data that can be consulted as a consequence[64]. Law enforcement access further depends on a written and motivated

[56] AG Pitruzzella, Opinion of the Advocate General in *Criminal proceedings against V.S. Request for a preliminary ruling from the Spetsializiran nakazatelen sad.*, 30.06.2022, case C-205/21, para. 56.
[57] Art. 25, Regulation (EU) 2016/679.
[58] Art. 1, Regulation (EU) 2017/2226.
[59] CJEU, *Opinion 1/15* (EU-Canada PNR Agreement), 26.07.2017, paras 77-78.
[60] Surprisingly, the EU lawmakers omitted Art. 16 TFEU despite its compatibility being confirmed by the CJEU in *Opinion 1/15*. The choice reflects the focus of the legal instrument on its components for migration management more than data protection.
[61] *Id.*
[62] D. N. Vavoula, *The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection*, cit., 28; see also T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit.
[63] Access rules are included in Chapter II (entry and use of data by competent authorities), Chapter III (use of the ees by other authorities) and Chapter IV (procedure and conditions for access to the ees for law enforcement purposes).
[64] Consider, for instance, Art. 27 (Regulation (EU) 2017/2226) firstly specifying authorised staff, data for the search and purpose and then mentioning the information open for consultation.

request sent to an independent access point, although the procedure can be delayed in urgent cases[65].

Despite these procedural barriers, the margins for access to LEAs are so broadly defined by the EES Regulation that they can easily breach the *precise purpose* requirement in data protection law. Consultation of the EES database is granted to LEAs anytime it would contribute to the prevention, detection and investigation of terrorist or serious criminal offences and for identification purposes of unknown suspects, perpetrators or suspected victims related to these cases. On the one hand, the provision does not represent a large step forward compared to the requirements set forth by the LED[66]. In particular, while the Directive calls on Member States to further specify the criminal activities which would justify processing activities, the EES makes reference to serious criminal offences if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years[67]. On the other hand, defining when a purpose is, indeed, *precise* is no straightforward operation[68]. European courts have historically preferred evaluating the specific purposes provided by state authorities rather than dictating how precise the purpose should be formulated ex ante, and Member States have so far received little guidance on the meaning of the requirement[69].

Further questions emerge as to the extent of powers of LEAs after consulting the database. LEAs may reuse the information consulted for different subsequent purposes or store the information on their own national databases, *de facto* prolonging the data retention period. As for the change of purpose, the LED applies "to all the subsequent treatment of data obtained from the EES"[70] and requires the further processing to be necessary and proportionate and the controller to be authorised for the second use[71]. These conditions reverberate the EES Regulation's conditions for first access, with the consequence that, once LEAs are provided access for the first time, they could use the same information for a number of purposes without any additional written request. A deeper interpretation of *reasonable expectation* by the Courts when testing subsequent uses might be necessary to avoid redundancy[72].

As for the transfer of EES data to national databases, the Regulation foresees that the retrieved data may be kept "in national files only where necessary in an individual case, in accordance with the purpose for which they were retrieved […] and for no longer than strictly necessary in that individual case"[73]. Therefore, verifications on whether the strict necessity principle is observed can only be performed *ex post*. In addition, an official

[65] Art. 31, Regulation (EU) 2017/2226.
[66] See Art. 1(1), Directive (EU) 2016/680.
[67] Reference is made to the list of criminal activities in Art. 2(2) of Framework Decision 2002/584/JHA.
[68] R. Te Molder *et al.*, *The principle of purpose limitation in data-driven policing: A guiding light or an empty shell?*, in *New Journal of European Criminal Law*, 14(4), 525 (2023).
[69] *Id.*.
[70] Recital 40, Regulation (EU) 2017/2226.
[71] Art. 4(2), Directive (EU) 2016/680.
[72] R. Te Molder *et al.*, *The principle of purpose limitation in data-driven policing: A guiding light or an empty shell?*, in *New Journal of European Criminal Law,* cit., 529.
[73] Art. 28, Regulation (EU) 2017/2226.

assessment conducted before the publication of the EES Regulation, the Impact Assessment of 2016, justified the transfer of the overstayers' data directly to the SIS, affirming that "it is only further processing of a percentage-wise small amount of the EES data" and that by doing so "overstayers are not criminalised" but remain identifiable to be removed or banned[74]. These arguments cannot but raise concern, because they consciously bypass the purpose limitation test on part of the Regulation and do not consider the chilling effect the transfer might have on travellers. Although the final text of the EES Regulation does not explicitly mention such a provision, it did not sink without trace, as the Regulation foresees the automatic communication to the Member States of the scheduled erasure of data on overstayers three months in advance "in order to enable them to adopt the appropriate measures"[75].

By streamlining access in favour of LEAs, interoperability might endanger the respect of purpose limitation even further, to the point of compromising it. For instance, if responsible agents are aware that additional information is contained in Eurodac, they might infer that the individual is an irregular immigrant or applied for asylum[76]. False information might encourage false suspicions in authorities, which might assume the travellers are trying to deceive them[77]. This risk is particularly tangible after the Interoperability Regulations abolished the cascading system of mandatory checks in national databases[78]. Finally, criticism on the feasibility of interoperability highlights that the project might lead to a circumvention of access rules, a reconceptualization of databases and a frustration of both *ex-ante* and *ex-post* supervisory activities[79].

Even setting aside the impact of interoperability, in spite of declarations not to add any new functionality to the passport checks, the central storing of personal data *per se* implies a risk for the traveller to lose control of their own data, which would not be present for stamped passports[80]. In the history of IT systems so far, function creeps within the single IT systems have already been spotted and compartmentalisation has not been able to contrast their inherent frictions. In 2018 the Fundamental Rights Agency of the EU (EUFRA) stated that the "EU IT systems increasingly serve purposes that were not originally envisaged"[81] and mentioned an Irish case, in which fingerprints were found to be stored in searches carried out during investigations regardless of a suspected involvement in any crime of the immigrant or asylum seeker[82].

---

[74] European Commission, Impact Assessment Report on the establishment of an EU Entry Exit System, 2016, 123.

[75] Art. 34(3), Regulation (EU) 2017/2226.

[76] D. N. Vavoula, *The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection*, cit., 28.

[77] EUFRA, *Fundamental rights and the interoperability of EU information systems: borders and security*, 95 (2017).

[78] The cascading system represents a procedural barrier to enhance privacy protection. It forces authorities to check the presence of matching data on their own databases before requesting access to the EU IT system. On the importance of the cascading system see EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 67.

[79] T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit.

[80] D. N. Vavoula, *The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection,* cit., 28.

[81] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights,* cit., 58.

[82] *Id.*, 61.

In sum, a thorough examination of the EES Regulation suggests that the IT system is not orphan of general rules and technical measures to satisfy the corollaries of the purpose limitation principle. Nonetheless, pending questions and grey areas emerge especially as far as access by LEAs is concerned, potentially creating the grounds for a violation of the principle. In addition, attention needs to be paid to the provisions of the Interoperability Regulations, which might disrupt the already unstable equilibrium the EES Regulation was seeking. It will ultimately depend on national and European supervisory authorities to monitor the use of EES data by LEAs and impede any abuse, especially after access has been authorised.

b. *Transparency, right to information and right to access*

Under the data protection framework and the migration databases foreigners approaching the EU for a short stay are categorised as data subjects, as their personal data is collected by national and EU authorities to fill large-scale IT systems. As such, TCNs are entitled to legal protection in the form of rights which they can exercise against the responsible authorities of Member States. The principle of transparency mentioned in Art. 5(1)(a) GDPR is the key to unlock the door of these rights to data subjects, who would otherwise wield a blind power, unaware of who is accessing which of their data and for what reason. The objective of transparency is translated in data protection into the main rights to be informed on the processing activities and to access the personal data held by the controller, in order to request rectifications, erasure, ask to complete incomplete data or restrict the processing.
The EES Regulation is founded on these rights as framed in data protection law and is additionally provided with special provisions that distinguish the rules applying to the database with respect to the general rules. Repercussions based on the application of one or the other legal regime differ considerably, and it is not difficult to get disoriented among the different applicable legal regimes. On the one hand, the GDPR sets out to ensure the highest protection possible at any moment for the data subject, adopting a policy of full transparency. On the other hand, the LED excludes transparency from its principles and provides controllers with more options to conceal the processing activities to the advantage of smoother and undisturbed investigations. This subsection identifies the rules shaping access and information rights of TCNs subject to the EES Regulation and examines some issues concerning the tasks of informing travellers responsibly allowing their access to improve transparency.

Despite the significance of the right of access[83] and its inclusion in the most prominent data protection legislation[84], in practice data entries are rarely challenged[85]. This phenomenon could have several origins, from a disbelief by people on the move on the actual effectiveness of their right, to a lack of interest and a cultural shift waiting to occur or to a simple inefficiency in the information provided by institutions and authorities.

Art. 52 of the EES Regulation allows TCNs to request access to their personal data to the competent authorities of Member States for the purposes of gaining information, restricting the use of their data, rectifying, completing or erasing incorrect data[86]. The responsible Member State shall check the accuracy of the data within 30 days and answer within 45 days from receiving the request, specifying to TCNs the action taken with respect to the data and explaining how to bring an action against their administrative decision. The requests might require fingerprints from the individual in order to identify them and such data must be erased immediately after the procedure. The request is documented by Member States and Europol and is made available to the supervisory authorities within 7 days to facilitate monitoring activities. Moreover, national supervisory authorities may assist and advise the data subject in exercising their rights to rectify, complete or erase personal data or to restrict the processing[87].

The short timing selected for authorities to respond in the EES is in line with many national administrative procedures and more ambitious with respect to the LED or to previous provisions[88]. EUFRA reports that this short deadline might be unrealistic due to heavy caseloads, administrative obstacles, necessary cooperative activities among Member States and doubts on the identity of the applicant too[89]. While requests to the SIS II can take from 10 days to four months to process, the VIS requests have so far taken on average 30-60 days, suggesting that EES requests might follow a similar pattern, with a lengthier timing in the early period of force[90].

While Art. 52 EES Regulation certainly refers to the data registered by visa, immigration or border authorities, its binding force arguably vanishes as soon as the same data comes in the hands of LEAs. Art. 58 EES Regulation governs the protection of personal data accessed by LEAs, specifying that the recast Europol Regulation or the LED might apply alternatively.

---

[83] See D. Dimitrova-P. De Hert, *The Right of Access Under the Police Directive: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, vol. 11079, 111–130 (2018).

[84] The rights of access, correction and deletion of one's own stored data are included in Arts. 15-17 GDPR and Arts. 16 and 17 LED, as well as in Art. 8(2) of the EU Charter of Fundamental Rights, Art. 8 of the Council of Europe Convention No. 108. On this point, see EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 99.

[85] *Id.*, 99-100.

[86] The access right in the EES Regulation refers to the uses in Arts. 15-18, Regulation (EU) 2016/679. The rights to data portability and to object the processing are excluded in the EES.

[87] Art. 53(2), Regulation (EU) 2017/2226.

[88] "Articles 12 and 14 Directive 2016/680 do not impose hard limits on the data controller to respond to a request by the data subject, unlike some AFSJ instruments" (D. Dimitrova-P. De Hert, *The Right of Access: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, cit., 125).

[89] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 103–104.

[90] *Id.*

This architecture is criticised for its complexity due to three issues in particular, i.e. the variety of LEAs processing personal data, the different information systems they operate with and thus the applicability of several legal instruments on data protection[91]. Borrowing an example made for SIS II[92], if, upon request by TCNs, national LEAs disclose information to them, it is not clear whether the disclosure would also comprise the data acquired in the EES for law enforcement purposes or whether the data subject should make an explicit reference in the request. The EUFRA argues that interoperability might solve the ambiguity and simplify the procedure by allowing the data subject to gain access to the links stored in the MID by only applying once[93].

On the one hand, exercising access rights on the basis of the Europol Regulation has been described as a "lengthy and complex procedure"[94]. On the other hand, the LED is considered *prima facie* a progressive and quite protective legal act, a step forward for data protection. However, application of the LED means that the rights of access of the data subject will exhibit considerable variation depending on the Member State[95]. While the main rule in the Directive allows full access to TCNs, national laws will be decisive in providing legal bases for controllers to limit access rights in different forms and deciding when the TCN might only receive confirmation of access by LEAs or exclusively receive instructions on how to lodge a complaint[96]. Furthermore, as the Directive excludes public authorities from the definition of 'recipient', competent authorities might transfer data to migration authorities concealing information about recipients[97]. Moreover, scholars highlight that more often than not the provisions of the LED are less effective in practice than they are in the book[98]. Limitations to information on the processing activities operated by LEAs, together with the low level of expertise and the low probability of reward for lawyers might make lodging a complaint inconvenient, undermining real chances of an effective remedy[99]. Scholars appear further sceptical of the transposition of the LED in national laws. Supervisory authorities are not provided with effective investigatory and sanctioning powers to challenge controllers in national laws, with the consequence of compromising the option of indirect access[100]. Undeniably, the

[91] D. Dimitrova-P. De Hert, *The Right of Access: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, cit., 125.
[92] *Id.*
[93] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 102.
[94] D. Dimitrova-P. De Hert, *The Right of Access: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, cit., 126.
[95] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 100.
[96] Art. 15(3), Directive (EU) 2016/680.
[97] T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit., 136.
[98] C. M. Feoli - A. D. Modigliani, *Il sis fra trattamento illecito di dati, paradossi applicativi e deficit di tutela*, in F. Biondi Dal Monte *et al.* (curr.), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa*, cit., 69; T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit., 145.
[99] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 104.
[100] D. Dimitrova-P. De Hert, *The Right of Access: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, cit., 123; T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit., 145.

circumstances seen so far cause "frictions, which take away from the effectiveness of the right of access"[101].

All this is hardly surprising. The exercise of access rights directly depends on the application of the right of information, and in particular on the capacity of controllers to inform the data subject on their entitlements. As far as the right of information is concerned, Art. 50 of the EES Regulation specifies the detailed pieces of information that are to be given to the TCN prior to data registration. The information provided to the data subjects can be summarised in four main groups. First, travellers are informed of their rights, i.e. the right to lodge a complaint to the supervisory authorities (l)[102], the right to request access for rectification purposes (h) and the right to request erasure from the list of identified persons in case of justified overstay (k). The second group of information includes the travellers' obligations, i.e. the obligation to provide general personal data as well as fingerprints and facial image to access the EU territory (b, c, d, e). Third, the traveller should obtain some pieces of information regarding their stay, e.g. the remaining duration of the stay and any entry ban or refusal of entry (f). Finally, a fourth group concerns information on the life of their personal data, i.e., the data retention period (j), the authorities provided with access and their purposes (a, i), the possibility that personal data are transferred to other parties (g) or automatically transferred to a list of identified persons in case of overstaying (k).

Choosing which pieces of information to provide to the traveller can be a tricky task, especially if priority is given to avoiding confusion more than achieving completeness. Moreover, it is how the message is conveyed which mostly determines efficacy in transparency. The EES Regulation dictates information to be given "in writing, by any appropriate means, in a concise, transparent, intelligible and easily accessible form, and it shall be made available, using clear and plain language"[103]. The information will be made available on the official website of the EES[104] and inserted in a template produced by the EU Commission to facilitate the transmission to Member States[105]. Additionally, information campaigns should be conducted regularly to inform TCNs "about the objectives of the EES, the data stored in the EES, the authorities having access and the rights of persons concerned"[106].

Notwithstanding the responsiveness of the EES, in 2018 the EUFRA revealed a general "dissociation between the duty to inform asylum applicants and how they are informed in practice" and concluded that "[t]his raises the question of how the quality of information affects procedures and on the trust in the system as a whole"[107]. The contribution by the FRA is precious to highlight the practical problems which do not emerge by merely

[101] D. Dimitrova-P. De Hert, *The Right of Access: Small Steps Forward*, in M. Medina *et al.* (curr,), *Privacy Technologies and Policy*, cit., 125.
[102] The letters in the paragraph refer to Art. 50(1), Regulation (EU) 2017/2226.
[103] Art. 50(2), Regulation (EU) 2017/2226. The formulation could already be found in a similar fashion in Art. 12(1), Directive (EU) 2016/680 and Art. 12(1), Regulation (EU) 2016/679.
[104] Art. 50(3), Regulation (EU) 2017/2226.
[105] Art. 50(5), Regulation (EU) 2017/2226.
[106] Art. 51, Regulation (EU) 2017/2226.
[107] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 29.

reading the regulations[108]. For instance, although the information should be shared at the moment in which fingerprints are taken in order to safeguard the TCN's rights, the latter often appear to learn about their rights later on in the procedure in fact. Most TCNs (67%) do not recall receiving any information regarding their personal data and those receiving information were mostly only informed on how data was going to be processed[109]. It should additionally be stressed that people on the move are likely to lack the linguistic and legal skills to autonomously exercise their rights to access, rectification and deletion and might well be oblivious on their existence[110]. Language barriers remain the most difficult to overcome as well as the main reason preventing a complete and clear spread of information [111] and the use of legal jargon often further complicates the content reception[112]. The workload impacts the quality of information too, as the higher the number of TCNs crossing borders is, the more difficult it is to ensure their complete understanding of the procedure[113]. Moreover, research shows that most TCNs ignore the leaflets handed by authorities due to a chronic lack of trust or interest, as they tend to prioritise other matters, are unaware of the consequences of the processing activities on the decision-making or are convinced that the information conveyed by family members or even smugglers might be more trustworthy[114]. The FRA recommended "providing information through the digital application process, in addition to including information on the application form"[115].

In sum, on paper the EES Regulation takes the rights of data subjects very seriously. Yet, its application might amplify the practical problems found in relation to similar migration databases as well as highlight the most problematic aspects with the application of the LED and consequential expansions of the LEAs' powers in the field of migration. In light of these issues, the looming rollout of the Smart Borders package will be useful to assess the readiness of the operators concerned and of the new access and information rules aiming at improving transparency and build reciprocal trust between controllers and data subjects in the migration context.

c. *Data Accuracy*

The EES is part of the vaster phenomenon of digitization of borders and datafication of migration management occurring in the European Union. The driving force behind this change is the political belief (or illusion[116]) that the use of large-scale IT systems leads to

[108] *Id.*, 33.
[109] *Id.*, 38.
[110] C.M. Feoli-A.D. Modigliani, *Il sis fra trattamento illecito di dati,* in F. Biondi Dal Monte *et al.* (curr,), *Migrazioni e governance digitale. Persone e dati alle frontiere dell'Europa*, cit., 84.
[111] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 34.
[112] *Id.*
[113] *Id.*, 32-34.
[114] *Id.*, 41.
[115] *Id.*, 36.
[116] M. Leese-S. Pollozek, *Not so fast! Data temporalities in law enforcement and border control*, in *Big Data & Society*, 10(1), 1–12 (2023).

the facilitation and acceleration of controls and to a consequent quality improvement due to a greater possibility of prioritization. Travellers are embedded within a rigid digital structure based on a predetermined set of information, which is replicable for each of them. Their raw data shape an identifying image carved within a digital system, with the inevitable consequence that the more erroneous the starting data is, the more dissimilar the digital result will be from the actual identity and the more pathological will be the reactions of authorities who base their decisions on such results.

Thus, accurate data is a *conditio sine qua non* for trusting the ability of digital identities to enable authorities to manage flows more efficiently and to allow an intrusion into privacy that would otherwise be futile and deleterious. The principle of data accuracy is an essential part of data protection[117] and of each migration database and sets the objective of eliminating errors and keeping data complete and up to date. Accountability for these tasks is shared between Member States, which have an obligation to ensure the accuracy and quality of biometric identifiers, and eu-LISA, which monitors whether the quality standards are followed[118].

By definition, however, large-scale IT systems, cannot be completely accurate[119]. First, it is noteworthy that the so-called *matches*, enabling the recognition of TCNs crossing the borders multiple times, are the result of a probabilistic process, which can only aim for the lowest error rate possible[120]. Secondly, the two elements of operational speed and data quality tend to be inversely proportional[121]. If, on the one hand, eu-LISA sets the aim of a response time equivalent to one second each 10 million of gallery size for the EES[122]; on the other hand, "large biometric data and low response time often translate into lower accuracy"[123].

Inaccuracies are not acknowledged exclusively in theory. In 2018 the FRA argued that "[m]ore than half of the border guards surveyed indicate that they at least sometimes experienced inaccurate, incorrect or not updated personal data in VIS or SIS II"[124]. In contrast, some experts indicate that encountering mistakes in the underlying databases happens quite often[125] and among responsible authorities "only 5 % had never encountered problems when trying to check fingerprints against VIS in the past 12 months"[126]. In the VIS, "mistakes can occur if, for example, the fingerprints are attached to the wrong person or if there are double registrations of the same person"[127]. In addition,

[117] Both Art. 5(1)(d) GDPR and Art. 4(1)(d) LED mention data accuracy among the main goals of lawful processing.
[118] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 88.
[119] CJEU, Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministers*, 21.06.2022, para. 106.
[120] *Id.*; see also EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 88.
[121] M. Leese-S. Pollozek, *Not so fast! Data temporalities in law enforcement and border control*, in *Big Data & Society* cit., 8.
[122] A. Valdivia *et al.*, *Neither opaque nor transparent: A transdisciplinary methodology to investigate datafication at the EU borders*, in *Big Data & Society*, cit., 13.
[123] *Id.*
[124] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 83.
[125] T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit., 56.
[126] EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 90.
[127] *Id.*, 96.

"persons who should be included in VIS because of having applied for a visa frequently could not be found in the system. More than 60 % of respondents indicate that this happened at least once in […] 12 months"[128].

In considering the relatively small error rates of these databases, it is worth noting that "given the large amount of data stored, even a low percentage of mistakes may affect a significant number of people"[129]. Nevertheless, in 2022 the CJEU argued that, in spite of a substantial number of false positives, databases have proved efficient for the objectives of general interest of the EU, e.g. to prevent terrorist or other serious criminal events[130].

Fingerprints and facial image recognition tools are the most debated technologies in the system[131]. The use of facial images for identification purposes is an innovation of the EES which will be applied to each migration IT system and should ensure the same level of accuracy in spite of reducing the number of fingerprints recorded[132]. The EES Regulation dictates that facial images should be taken preferably live[133], that Member States should prepare yearly reports on the exceptional case of use of e-MRTD images and that the Commission should produce reports on the quality standards of facial images stored in the VIS every two years[134]. Although both fingerprint and facial image recognition tools have made considerable progress in the last decade, the cases of racial or gender discriminations caused by the latter and the impact of the ageing effect on both suggest there is plenty of room for research and improvement[135]. Furthermore, episodes of self-harm lowering the quality of biometrics stress the importance of building reciprocal trust among TCNs and authorities regardless of technical adequacy[136].

Errors are not limited to the automated processing of biometric data *per se*. In their analyses of data temporalities, Leese and Pollozek noticed that the efficiency of databases is influenced by at least three main factors: trade-offs, technological inscriptions and social rhythms[137].

Trade-offs refer to conflicting priorities modulating the efficiency of IT systems. A case in point is the notable difference in accuracy rate between the VIS and the SIS. While

---

128 *Id.*, 83.
129 *Id.*, 88.
130 CJEU, Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministers*, 21.06.2022, para. 124.
131 On the reaction by travellers and society to the use of these data, see European Commission, Joint Research Centre, *Study on face identification technology for its implementation in the Schengen Information System* (2019); see also EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit.
132 Recital 20, Regulation (EU) 2017/2226.
133 The facial images extracted from passports have a lower resolution and might as well belong to someone else. This provision applied Recommendation no. 8, formulated in European Commission, Joint Research Centre, *Study on face identification technology for its implementation in the Schengen Information System*, cit.
134 Art. 15, Regulation (EU) 2017/2226.
135 See Recommendation 12 (Accuracy evaluation across ethnicities and gender) and Recommendation 15 (Corrective measures for the ageing effect) in European Commission, Joint Research Centre, *Study on face identification technology for its implementation in the Schengen Information System*, cit.
136 EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 50.
137 M. Leese-S. Pollozek, *Not so fast! Data temporalities in law enforcement and border control*, in *Big Data & Society* cit.

registration in the VIS prioritizes speed over accuracy[138], authorities report being more cautious when recording data in the SIS, as those data relate to a judicial or administrative national decision with respect to a specific person[139]. It does not surprise that cases of mistakes due to insufficient verification before entering data and deficiencies in updating and correcting the data are reported more frequently in the VIS with respect to the SIS[140]. Thus, a relevant factor for data accuracy appears to be linked to the perceived importance of the single IT system. The EES could not only share the same experience of the VIS but also suffer from the higher amount of mistakes originated in that database.

Technological inscriptions refer to how data is organised in the digital spaces (datastructuring), i.e. the intrinsic boundaries and limitations of these systems which influence the outputs of the inserted data, their accuracy and their expansion[141]. The EES automated calculator may exemplify a peculiar functionality potentially leading to inaccurate knowledge. By automatically labelling TCNs exceeding the authorised stay as overstayers and *blacklisting* them, the EES sets irregularity as the rule and consequently marks TCNs as irregulars. As their legitimate reasons for overstaying are only entered *ex post*, the knowledge produced by the automated calculator risks amplifying a smaller issue and reaching the wrong target.

Social rhythms refer to how IT systems come in contact with the sociotemporal ordering of phenomena, in other words how they interact with the contingencies of reality, as only in the abstract can databases guarantee full efficacy[142]. To this category we may ascribe the majority of error sources. Human errors in the procedures typically result from poor guidance or poor training. As alien alphabets and spelling difficulties have a direct impact on data quality[143], training human beings to work at borders does not only imply conveying skills of technological know-how but should also comprehend an effort of cultural mediation[144]. Increased workload and strain on the staff recording and dealing with data[145] represent further factual limitations in border management. A substantial minority of controllers stated that they did not appoint or did not know if a data quality officer was present in their organisation[146]. Travellers may communicate false data on purpose in order

---

138 Eu-LISA promoted a "zero failure to enrol" policy with regard to VIS, preventing fingerprints to be rejected because of lack of quality. See eu-LISA, *Biometrics in Large-Scale IT: Recent trends, current performance capabilities, recommendations for the near future* (2015).

139 EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 85.

140 *Id.*, 82.

141 R. Bellanova-G. Glouftsios, *Formatting European security integration through database interoperability*, in *European Security*, cit.; M. Flyverbom-J. Murray, *Datastructuring—Organizing and curating digital traces into action*, in *Big Data & Society*, 5(2), 2018; A. Pelizza-W. R. Van Rossem, *Scripts of Alterity: Mapping Assumptions and Limitations of the Border Security Apparatus through Classification Schemas*, in *Science, Technology, & Human Values,* cit., 794–826.

142 M. Leese-S. Pollozek, *Not so fast! Data temporalities in law enforcement and border control*, in *Big Data & Society* cit., 2.

143 To stress this point, some people on the move have claimed that "when they transited other Member States, they did not have access to an interpreter when stating their name and date of birth, despite being unable to use or understand Latin letters" (EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 96).

144 *Id.*

145 *Id.*, 84.

146 M. Leese-F. Marugg, *Data quality in European law enforcement and border control cooperation: Findings from survey research*, in *CURATE Report no.1,* 9 (2023).

to escape a potential registration in the SIS II or Eurodac[147]. Moreover, mistakes can emerge due to procedural or substantial errors during national administrative or judicial proceedings[148].

In addition, although interoperability might be useful to rectify wrong data, some argue that it is likely to amplify the present flaws of each database[149], such as the massive presence of erroneous data, and therefore have heavier consequences on the fundamental rights of the individuals in question[150].

The EES Regulation adopted a series of measures to apply data accuracy. Member States spotting inaccuracies have an obligation to correct them immediately[151] and to examine the requests of access and rectification by data subjects[152]. Eu-LISA, as data quality observer, is tasked with creating data quality control mechanisms and common data quality indicators using anonymised data[153]. In addition, a Biometric Test Engineer is called to perform local and performance tests and accuracy tests[154].

Some additional legislative measures sharpen the focus on data quality for the rollout of the EES. The European Commission has adopted technical specifications for the quality, resolution and use of the biometric data in the EES, whereby, *inter alia*, ICAO standards are used as a reference for data quality[155]. The Data Quality Roadmap[156] examines the capacity of Member States to feed high-quality data into the relevant EU information systems and the Commission's Implementing Decisions no. 2224 and 2225 of 2021 set the quality standards for the interoperability framework[157].

Measures to improve accuracy also originate from Member States or even local initiatives and some of them can be regarded as recommended practices. In order to lower the volume of transliteration issues, some Member States ask the traveller to cross-check the transcribed personal data, fostering participation and building reciprocal trust[158]. Authorities are then invited to use accurate and transparent tools to quantify the level of uncertainty of a match and to minimise manual entries by using electronic readers and automatic verification against other data entries[159]. At the same time, the subsequent

147 EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 77.
148 *Id.*
149 EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 105.
150 T. Quintel, *Data protection, migration and border control: the GDPR, the law enforcement directive and beyond*, cit., 88.
151 Art. 35, Regulation (EU) 2017/2226.
152 Art. 52, Regulation (EU) 2017/2226.
153 Art. 12, Regulation (EU) 2017/1726.
154 The obligation comes from the tender documents that eu-LISA produced in relation to the creation of the Entry/Exit System: *Annex I. Executive summary LISA/2019/RP/05 EES BMS and sBMS. Contract notice.* Available at https://etendering.ted. europa.eu/cft/cft-display.html?cftId=4802 (last visited July 07, 2025).
155 Commission Implementing Decision (EU) 2019/329; see also European Commission, Joint Research Centre, *Study on face identification technology for its implementation in the Schengen Information System, cit.*
156 Council of the EU, *Roadmap for standardisation for data quality purposes*, 11824/20, Brussels, 11 November 2020, 5.
157 M. Leese-F. Marugg, *Data quality in European law enforcement and border control cooperation: Findings from survey research*, in *CURATE Report no.1,* cit., 18.
158 EUFRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, cit., 85.
159 *Id.*, 88.

verification of results by non-automated means is essential to ensure the proper functioning of the system[160].

V. FINAL REMARKS: THE FUTURE OF THE EES

This study set out to explore the relationship between the EES and the principles stemming from the data protection framework. After summarising the features of this new large-scale IT system and comparing it to the structure of the most important pieces of legislation of the EU on data protection, Section IV has identified three main principles which are put under pressure by the system.

The investigation of the purpose limitation principle in the EES has shown the inherent ambiguities of multi-purpose tools, potentially causing spillover effects or function creeps. In spite of the rules separating access authorisations and the procedural barriers of privacy by design, the defective definition of precise purposes and, most of all, the upcoming interconnection among all migration databases constitute a risk for the integrity of the principle. The analysis of the transparency principle revealed that obstacles in conveying information and building trust with non-EU nationals concern both how to inform and what information to share. The exercise of the right to access personal data is obstructed by practical obstacles as well as by complexity in the application of both national and EU law. The findings of the study further suggest that datafication does not mean data accuracy. The contact with reality, technological inscriptions and trade-offs are among the factors impacting on the efforts by the EU to achieve the highest level of data reliability and should be taken into account in the shift towards the digitization of borders.

This paper presented some theoretical criticalities that might be confirmed once data on the rollout of the EES is available. Hence, natural progression of the research should include an examination of the new data coming from surveys at the borders.

Room for further research lies in the relationship between the EES and the newly adopted AI Act. The initial exclusion of migration databases from the scope of the AI Act suggests that functions such as the facial recognition tools are likely to include AI features which the EU is reluctant to sacrifice. The final version of the Act classifies AI tools in migration databases as *high-risk*, thus subjecting their use to specified obligations. AI is likely to add pressure to each one of the principles of data protection mentioned in Section IV. For instance, the CRRS (a component of interoperability) will be able to collect data from the EES and other databases and process it through algorithms to assist the selection of risk indicators, thus expanding the role of EES data beyond its original purpose. The opacity characterising algorithms, which are often described as "black boxes", might be detrimental to the principle of transparency and constitute an obstruction to information duties. Finally, data accuracy will be affected by algorithm biases, which could amplify errors in the databases, foster false suspicions and reinforce discrimination.

This research has provided the opportunity to gain knowledge on the provisions the EES is equipped with to protect personal data. However, these findings suggest that the system

[160] CJEU, Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministers*, 21.06.2022, para. 124.

is far from perfect and highlight the future need to monitor how authorities apply these provisions in practice. The integrity of personal data at the borders will depend on the willingness of institutions to strengthen cooperation with the EDPS, enhance the powers of supervisory authorities and implement good practices to empower TCNs and build reciprocal trust.