ADiM BLOG
November 2021
ANALISES & OPINIONS

The Management of Migrants' Identities at the EU External Borders: Quo vadis *Interoperability?*

Francesca Tassinari[1]

Ph. D. candidate in Public International Law and International Relations
University of Grenade & University of Ferrara

Keywords

Interoperability – Third Country Nationals – Multiple Identity Detection – Automated Decision Making – Data Protection

Abstract

Regulations 2019/817 and 2019/818 establish a framework for the interoperability between EU information systems in the field of borders, visa, police and judicial cooperation, asylum, and migration. These systems are: the Schengen Information System (SIS); the Visa Information System (VIS); the Entry Exit System (EES); the European Travel Information and Authorisation System (ETIAS); the European Criminal Records Information System for third-country nationals (ECRIS-TCN), and the European Dactyloscopy system (Eurodac). The sister Regulations add new objectives to the underlying systems, among which the multiple-identity detection procedure stands out as the prominent novelty of the whole reform. This post glosses how this mechanism is expected to support the "correct identification" of third country nationals at the European Union (EU) external borders while

[1] The author is grateful to the ADiM editorial team for its few adaptations. The content of this post is opinion of the own author. Any errors must be attributed to her.

questioning the guarantees set forth for migrants' right to the protection of personal data.

1. Introduction

Regulations 2019/817 and Regulation 2019/818 (IO Regulations) establish a framework for the interoperability between EU information systems in the field of borders, visa, police and judicial cooperation, asylum, and migration. Such a reform aims at interconnecting six freedom, security and justice large-scale IT systems: two recently renovated – the Schengen Information System (SIS) and the Visa Information System (VIS); three currently under implementation – the Entry Exit System (EES), the European Travel Information and Authorisation System (ETIAS), and the European Criminal Records Information System for third-country nationals (ECRIS-TCN) –, and a last one whose adoption has been blocked by the co-legislators since 2016 and it is currently under (re)negotiation – i.e., the European Dactyloscopy system (Eurodac). The huge amount of migrants' personal data processed within these systems confirms that interoperability will weigh most heavily, though not exclusively, on third country nationals, raising questions about how their fundamental right to the protection of personal data – i.e., Article 8 of the EU Charter of Fundamental Rights (EUCFR) – is safeguarded. This post introduces the most relevant objective pursued by the IO Regulations, that is, the detection of multiple identities set forth under Article 21. After illustrating its content and functioning, we will analyse some of the guarantees envisaged by the co-legislators to assess whether migrants' rights to information, access, rectification, and erasure of personal data are duly guaranteed.

2. The new IT infrastructure

The majority of the norms set forth by the sister Regulations is dedicated at regulating the interoperability components: the European Search Portal (ESP); the shared Biometric Matching Service (sBMS); the Common Identity Repository (CIR), and the Multiple-Identity Detector (MID). The ESP is a one-stop shop or massage broker that will facilitate the access to the systems and the interoperability components while enabling the cross-matching among the data stored therein. The sBMS will store the biometric templates of the corresponding data stored in the underlying systems and the CIR – i.e., fingerprints and facial images –, thus excluding the ETIAS. The CIR is the true "beating heart" of this new infrastructure and it will gather some of the categories of personal data stored in the underlying IT systems at stake, namely: identity, travel document, and biometric data. The MID will support the CIR by creating, establishing, and storing color-coded links among the data – or even better the individual files – stored in the CIR or in the SIS, laying the latter outside the CIR.

3. The multiple-identity detection procedure

The multiple-identity detection procedure is launched each time an individual file is created

or updated in one of the six large-scale IT systems integrating the interoperability architecture (Article 27 IO Regulations). Thus, the authorities involved in this procedure may be: borders guards, consular authorities, and immigration authorities as for the EES; authorities competent for visa and residence permits for the (revised) VIS; the ETIAS Central and National Units for the ETIAS; the SIRENE Bureau of the Member State creating or updating a SIS alert, and the central authorities of the Member States in charge of inputting data in the ECRIS-TCN (Article 29(1) IO Regulations). The multiple-identity detection procedure pursues two main goals: facilitating *bona fide* travellers' checks at the external borders and detecting fraudulent identities used to access the Schengen area. The latter is especially important to fight organised crime, terrorism, smuggling of migrants, and trafficking in human beings, as the European Migrant Smuggling Centre points out. However, the use of "other" identities also characterises groups of migrants that should not be associated with criminal activities such as irregular migrants and asylum seekers, as the European Union Agency for Fundamental Rights claims.

3.1. The automated generation of white and yellow links

As soon as an individual file is created or updated in one of the underlying IT systems, the multiple-identity detection procedure is automated started. The data input or modified are compared with those stored in the CIR and the SIS, as well as with the templates held by the sBMS. Comparisons occur among data belonging to the same category, that is: identity data are compared with identity data; travel document data are compared with travel document data; fingerprints are matched with fingerprints, and facial images are matched with facial images. Such an automated phase may flow into the generation of a white or yellow link among individual files stored in different IT systems (Article 27(5) IO Regulations).

A white link (Article 33 IO Regulations) indicates that the data inputs are identical or similar to the ones already stored in the CIR – eventually in the SIS – and match with the templates held by the sBMS: in other words, the data belong to the same person. It would be the case of a person seeking for the first time a visa to enter the Schengen area who is registered in the EES upon his/her arrival at the EU external borders. Provided that no other system contains data related to that person, the multiple-identity detection procedure would be launched twice, by the VIS and the EES, but only the latter would create a white link against the VIS.

A yellow link, instead, is notified when the data stored in the individual files compared cannot be considered identical or similar (Article 30 IO Regulations). The yellow link is provisional and calls on a competent authority to "resolve" it, that is, to resolve the identity issue stemming from the automated comparison. It would be the case, for instance, of a third country national that had been issued a refusal of entry alert provided with fingerprints and biometrics in the SIS and subsequently obtains a genuine passport in another country of origin subjected to a visa requirement to access the Schengen area. As soon as the consular authority

enters the data in the VIS, the multiple-identity detection procedure is launched and a yellow link is generated since the identity and the travel document data are detected to be different, while the biometrics match with the ones stored in the SIS – i.e., the corresponding template within the sBMS.

3.2. The manual verification procedure

As a general rule, the authorities creating or modifying an identity file in one of the IT systems decide the cases they are dealing with. An important exception is given for the SIS "sensitive alerts" whose yellow links are to be resolved by the SIRENE Bureau of the Member State creating the alert (Article 29(2) IO Regulations). The authority in charge of the manual verification shall turn the yellow link into a:

- white link, when s/he finds that the linked files belong to the same person;
- green link, if s/he considers that the linked files pertain to different persons, though sharing some patterns;
- red link, when there is a risk that the person at stake is using different identities in an unjustified manner – be them false or stolen.

For the purpose of resolving the yellow link, the competent authority is allowed to access the set of data linked contained in the CIR – and eventually the SIS – and the previously generated or established links that are registered in MID – i.e, in the so-called "identity confirmation file" (Article 34 IO Regulations). This implies, as the European Data Protection Supervisor (EDPS) highlights, that new access rights are granted to resolve the yellow links and, consequently, that individuals' personal data are subjected to new processing activities. The choice among a white, green, or red link lies in the hands of the authority competent for the manual verification; yet, the European Commission is expected to support them in this task with a practical handbook (Articles 77 and 73 IO Regulations). For example, a red link may be established when a third country national has a refusal of entry alert in the SIS and submits in the ETIAS a request for a travel authorisation with false or stolen identity data. In this situation, the multiple identity detection procedure launched by the EES against the SIS generates a yellow link since the biometric data match, but the identity data are neither the same nor similar. The border guard concerned is expected to turn the yellow link into a red one since the individual has used a false or someone else's identity to access the Schengen area, as it is recorded in the ETIAS.

4. Migrants/data subjects' right to the protection of personal data

According to the EU data protection *acquis*, the link generated or established within the multiple-identity detection procedure is "information relating to an identified or identifiable

natural person" or, simply, personal data – see, e.g., Article 4(1) General Data Protection Regulation (GDPR). Therefore, the IO Regulations insert important provisions on the right to be informed, to access, rectify, and delete personal data before the national authorities and Union agencies' staff involved in the multiple-identity detection procedure.

4.1. The right to information

The right to information is guaranteed in case a white or a red link is established by the competent authority in charge of the manual verification procedure (Articles 33(4) and 33(4) IO Regulations) thanks to the handover of a standard form containing the references to: the single identification number (Article 34(c) IO Regulations); the authority responsible for the manual verification of different identities (Article 34(d) IO Regulations), and the website address of a web portal (Article 49 IO Regulations). The EDPS has recently commented that the standard form drafted by the European Commission should better detail the range of cases envisaged to justify the establishment of a white or a red link. We believe that the difficulties surrounding the explanation of the functioning of a (semi-)automated decision-making procedure consisting in the combination of enigmatic algorithms and human interventions should have been evidenced too. Also, no form seems to be provided in case white links are generated in an automated manner, or when green links are established. The former gap is especially worrisome if we consider the right not to be subject to a decision based solely on automated processing, including profiling – e.g., Article 22 GDPR. Although this right is subject to derogations, full-automated decision-making based on sensitive data – like biometrics – is always called on to respect the limits imposed by virtue of Article 52(1) EUCFR. It seems to us that in these cases the right to information is not suppressed *tout court*, and that the general provision of Article 47 IO Regulations applies. According to it, the individual must be informed each time an individual file is created in SIS, VIS, EES, ETIAS, Eurodac, or ECRIS-TCN. However, it is not clear why the IO Regulations foresee a different treatment among, on the one hand, the white links generated in an automated manner and the green links and, on the other hand, the white and red links established following the manual verification procedure. On closer inspection, also the former types of links may be erroneously or illegally established and, beware, these errors may result from a machine decision. In any case, no information at all is given to the individual in case this prejudices security and public order, crime prevention, and national investigation which seems to be the case of the SIS "sensitive alerts", though the IO Regulations are silent on this point.

4.2. The right to access, rectify, and erase personal data and to restrict the processing

The right to access, rectify, and erase personal data may be exercised through the interoperability web portal when the standard form is handed in to the individual, or by addressing the competent authority of each Member State a request to access, rectify, and erase

personal data as well as to exercise the right to restrict the processing. In the latter case, Article 48(2) IO Regulations foresees that the Member State examining such a request shall reply, including through a central office, in any event within 45 days from the receipt of the request – extendable by 15 further days. Yet, in case the request concerns the rectification or suppression of personal data, Article 48(3) IO Regulations sets forth a cooperation procedure between the authority addressed and the one responsible for the manual verification procedure. Specifically, the Member State to which the request has been submitted shall contact the authorities of the Member State responsible for the manual verification of different identities within 7 days. It is the latter authority that is in charge of checking the accuracy of the data and the lawfulness of the data processing within 30 days – extendable by 15 further days. Now, the authority responsible for the manual verification may:

- rectify or erase those data and inform in writing the individual concerned, or
- adopt an administrative decision explaining in writing to the person concerned why the rectification or the erasure has not been executed.

Article 48(8) IO Regulations specifies that the latter decision must indicate the means for challenging it at court or before the national supervisory authority, though we should not exclude the possibility that the validity or regularity of the decision taken in the former situation may also be questioned. Besides, Article 48 raises two main concerns: one related to white links generated in an automated manner in which cases there is no competent authority designated; another one concerning the ETIAS Central Unit's responsibility for resolving yellow links. In both cases, Article 48(5) IO Regulations establishes that the Member State to which the request has been made shall decide whether to rectify or erase those data or not. This implies that the Member State addressed take the responsibility not only for the white links generated in an automated manner, but also for the links established by the ETIAS Central Unit – i.e., the European Border and Coast Guard (EBCG) Agency. We believe that this solution shall be appreciated since it guarantees the individual the right to an effective remedy against administrative decisions according to Article 47 EUCFR. However, it should be also criticised as it de-regulates the EBCG Agency's responsibility in the frame of multiple-identity detection procedure. In this regard, we cannot avoid mentioning the crucial role played by the ETIAS Central Unit in the resolution of yellow links stemming from the data stored in the systems before the interoperability components are put into operation, which is also labelled as "MID transitional period" (Articles 69 and 65 IO Regulations). We assume that in none of these circumstances the individual could challenge an EBCG Agency's act in the light of Article 263 of the Treaty of the Functioning of the EU (TFEU) since the Agency never issues a writing decision. Considering that the ETIAS Central Unit gives its "opinion" without undue delay and in any event within 30 days since it has been contacted by the Member State to which the request is made (Article 48(4) IO Regulations), a complaint by virtue of the third

paragraph of Article 265 TFEU would also be rejected. Conversely, the ETIAS Central Unit's decision stemming from the manual verification procedure could be challenged incidentally before the national court that may refer a question to the CJEU for a preliminary ruling – i.e., Article 267 TFEU. All in all, our assumptions leave open the debate on the protection of migrants' fundamental rights against that EU agency's activities.

5. Conclusions

Article 21 IO Regulations provides for a new interoperability objective consisting in the detection of migrants' multiple identities based on the generation/establishment of links among the individual files stored in the CIR. Aiming at fostering checks over persons at the EU external borders, the multiple-identity detection provides for full- or semi-automated decision-making procedures that will impact migratory flows toward, within, and from the Schengen area. Although laying down specific safeguards for the individual to exercise his/her rights to be informed, access, erase, and delete the links, the sister Regulations do not justify why different treatments are granted depending on the generated/established coloured-links. Arguably, IO Regulations blur the responsibility of the authorities and staff involved in the procedure which may risk disarming the individual *vis-à-vis* the decisions taken, for example, by the EBCG Agency.

SUGGESTED READINGS

Doctrine:

- B. VAN ALSENOY, *Data protection Law in the EU: Roles, Responsabilities and Liability*, Cambridge, 2019.

- C. BLASI CASAGRAN, "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU", *Human Rights Law Review*, n. 2, 2021, pp. 433–457.

- D. J. LIÑÁN NOGUERAS, "El Espacio de Libertad, Seguridad y Justicia", in A. MANGAS MARTÍN and D. J. LIÑÁN NOGUERAS (ed.), *Instituciones y Derecho de la Unión Europea*, Madrid, 2020.

- E. BROUWER, "Large-Scale Databases and Interoperability in Migration and Border Policies: The Non- Discriminatory Approach of Data Protection", *European Public Law*, n. 1, 2020, pp. 71-92.

- E. HOFFBERGER-PIPPAN, "The Interoperability of EU Information Systems and Fundamental Rights concerns", *Spanish Yearbook of International Law*, n. 23, 2019, pp. 426-250.

- E. TROISI, "AI e GDPR: L'Automated Decision Making, la Protezione dei Dati e il Diritto alla 'Intellegibilita' dell'Algoritmo", *European Journal of Privacy Law & Technologies*, n. 41, 2019.

- F. ESTEVE, "El Control Judicial de las Agencias del Espacio de Libertad, Seguridad y Justicia", in C. BLASI CASAGRAN and M. ILLAMOLA DAUSÁ (ed.), *El control de las agencias del Espacio de Libertad, Seguridad y Justicia*, Madrid, 2016, pp. 81-104.

- F. TASSINARI, "La transizione digitale dell'UE nello spazio di libertà, sicurezza e giustizia: le sfide dell'interoperabilità dei sistemi IT su larga scala", *Idee d'Europa*, Ferrara, 2021.

- F. TASSINARI, "The externalisation of Europe's data protection law in Morocco: an imperative means for the management of migration flows", *Peace & Security - Paix et Sécurité Internationales (Euromediterranean Journal of International Law and International Relations)*, n. 9, 2021.

- J. A. DEL VALLE GÁLVEZ, "Inmigración, derechos humanos y modelo europeo de fronteras: Propuestas conceptuales sobre "extraterritorialidad", "desterritorialidad" y "externalización" de controles y flujos migratorios", *Revista de Estudios Jurídicos y Criminológicos*, n. 2, 2020, pp. 145-210.

- J. ALBERTI, *Le Agenzie dell'Unione Europea*, Milano, 2018.

- J. SANTOS VARA, *La gestión de las fronteras exteriores de la UE Los nuevos poderes de la Agencia Frontex*, Valencia, 2021.

- M. LEESE, "Fixing State Vision: Interoperability, Biometrics, and Identity Management in the EU", *Geopolitics*, 2020, pp. 1-21.

- N. VAVOULA, "Interoperability of EU Information Systems: The Deathblow to the Right to Privacy and Personal Data Protection of Third Country Nationals?", *European Public Law*, n. 1, 2020, pp. 131-156.

- P. HANKE AND D. VITIELLO, "High-Tech Migration Control in the EU and Beyond: The Legal Challenges of "Enhanced Interoperability", in E. CARPANELLI and N. LAZZERINI (ed.), *Use and Misuse of New Technologies. Contemporary Challenges in International and European Law*, Switzerland, 2019.

- S. FORLATI, "L'ingresso dei migranti irregolari nell'Unione europea – Fra controllo dell'immigrazione clandestina ed esigenze di protezione", in V. MILITELLO and A. SPENA (ed.), *Il traffico di migranti – Diritti, tutele, criminalizzazione*, Turin, 2015, pp. 37-59.

- T. FAJARDO DEL CASTILLO, "El derecho humano a abandonar un país, incluido el propio: las excepciones a la regla", *Revista Española de Derecho Internacional*, n. 2, 2021, pp. 85-100.

Other Materials:

- COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, Accompanying the document Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 and Proposal for a Regulation of the European Parliament and the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) SWD/2017/0473 final - 2017/0351 (COD), Strasbourg, 12.12.2017.

- 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 April 2016.

- EUROPEAN DATA PROTECTION SUPERVISOR, Opinion 4/2018 on the Proposals for two Regulations on the establishing a framework for interoperability between EU large-scale information systems, Brussels, 16 April 2018.

- EUROPEAN MIGRANT SMUGGLING CENTRE, 4th Annual Activity Report, The Hague, 2020.

- EUROPEAN PARLIAMENT, Interoperability between EU information systems for security, border and migration management, PE 628.267, Brussels, 2019.

- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, Interoperability and Fundamental Rights Implications, Brussels, 19 April 2019.

- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, Under watchful eyes – biometrics, EU IT-systems and fundamental rights, Brussels, 28 March 2018.

Suggested citation: F. TASSINARI, *The Management of Migrants' Identities at the EU External Borders:* Quo vadis *Interoperability?,* ADiM Blog, Analisi & Opinioni, November 2021.