Large-Scale Integration of Technical Systems in Cross-Border Police Cooperation Management: Challenges and Solutions for Public Administration[1]

PhD. **Iulian COMAN**[2]

Abstract

The study entitled 'Large-scale integration of technical systems in the management of cross-border police cooperation: challenges and solutions for public administration,' aims to analyse how the implementation and use of complex technical systems managed by EU-LISA influence the efficiency of police cooperation between states, highlighting the challenges encountered and possible solutions from the perspective of public administration. The objectives of the study include: 1. Assessing the impact of the main large-scale technical systems – the Schengen Information System (SIS), the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS) – on cross-border police cooperation; 2. Identifying the main administrative and operational challenges in integrating these systems, such as interoperability issues, legislative differences and concerns about personal data protection; 3. Proposing solutions to optimise the use of these technologies in support of international cooperation, taking into account the delays and technical difficulties reported in their implementation. To achieve these objectives, the research uses a mixed methodology based on qualitative analysis of relevant European policy documents and case studies on the implementation of the SIS, EES and ETIAS systems in several EU Member States. Preliminary results indicate that, although the advanced technical systems mentioned have the potential to improve information exchange and operational efficiency, there are significant obstacles related to interoperability, legislative differences and personal data protection. For example, the implementation of the EES has been delayed several times due to technical problems and concerns about border congestion. The implications of the study highlight the need for a coordinated approach at the European level to harmonise legislative frameworks and promote common standards for the effective integration of technical systems in cross-border police cooperation.

Keywords: *large-scale technical systems, cross-border police cooperation, public administration, interoperability, European security policies.*

JEL Classification: H83, K23, K24, O38

DOI: https://doi.org/10.62768/ADJURIS/2025/4/13

[1] The information and views expressed in this article are those of the author and do not necessarily reflect the official opinion of the institutions analysed in the context.

[2] Iulian Coman - „Alexandru Ioan Cuza" Police Academy, Romania, iulian.coman@academiade-politie.ro.

Please cite this article as:
Coman, Iulian, „Large-Scale Integration of Technical Systems in Cross-Border Police Cooperation Management: Challenges and Solutions for Public Administration", in Takemura, Hitomi & Steve O. Michael (eds.), *Public Law at the Crossroads of Technology, Jurisprudence and Governance in Contemporary Europe,* ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2025, p. 198-208.

1. Introduction

In an era of accelerated digitalisation and increased cross-border mobility, the internal security of the European Union (EU) has become increasingly dependent on the ability of Member States to cooperate effectively, particularly in the field of policing and border management. To respond to current challenges – from illegal migration to transnational crime – the EU has developed and operationalised several large-scale IT systems designed to facilitate the exchange of information between competent authorities[3].

The Schengen Information System (SIS), the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS) are part of the European technical and c e infrastructure and are managed by the EU-LISA agency. The effective implementation and use of these systems directly influence the ability of Member States to cooperate in real time, detect threats and take concerted action in situations of risk.

This research focuses on the Schengen Information System (SIS), the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS), as these are the central elements of the new European architecture for border security and police cooperation. Unlike other IT systems, such as VIS or Eurodac, these three tools directly integrate border control functions with operational prevention and law enforcement components, and are essential for the application of the interoperability rules recently adopted at the EU level. They are also the most advanced in terms of implementation and pose immediate administrative challenges for Member States.

However, integrating these systems into the administrative and operational processes of Member States requires overcoming complex challenges. These include the lack of interoperability between systems, differences in national legislation and concerns about personal data protection. Against this background, this paper aims to analyse the extent to which these difficulties affect

[3] Jose L. Wong Villanueva, Tetsuo Kidokoro, and Fumihiko Seta (2020) "Cross-Border Integration, Cooperation and Governance: A Systems Approach for Evaluating 'Good' Governance in Cross-Border Regions." *Journal of Borderlands Studies* 37 (5): 1047–70. doi: 10.1080/08865655.2020.1855227.

cross-border police cooperation and to propose sustainable solutions for optimising the use of these technological tools from a public administration perspective[4].

2. Assessment of the Impact of the Main Large-Scale Technical Systems – the Schengen Information System (SIS), the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS)

In the context of strengthening internal security and efficient border management, the European Union has developed and implemented a number of large-scale technical systems. These are designed to facilitate cross-border police cooperation and respond to the challenges of migration and transnational crime. Among the most significant are the Schengen Information System (SIS), the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS).

Schengen Information System (SIS). The SIS is the most extensive information exchange system in the field of security and border management in Europe. It allows competent authorities to enter and consult alerts on persons and objects, facilitating police and judicial cooperation between Member States. The system operates through a centralised database accessible to national authorities and is essential for the rapid identification of wanted persons, missing persons or stolen objects.[5]

The implementation of the SIS has had a significant impact on cross-border police cooperation, enabling the rapid exchange of information and the effective coordination of actions between Member States. However, the effective use of the system depends on the constant updating of data and interoperability with other IT systems.

Entry/Exit System (EES). The EES is an automated system that records the entry and exit data of third-country nationals visiting the Schengen area. It replaces manual stamping of passports and helps prevent illegal migration, identify those who overstay their legal stays and detect false documents. The system collects biometric data, such as fingerprints and facial images, and stores them in a central database.

Migration and Home Affairs

The EES improves the security of the EU's external borders and facilitates border control by reducing processing times and increasing efficiency.

[4] For an international and comparative perspective see Alessandra Russo, Eva Magdalena Stambøl (2022). "The External Dimension of the EU's Fight against Transnational Crime: Transferring Political Rationalities of Crime Control." *Review of International Studies* vol. 48, no. 2: 326–45. https://doi.org/10.1017/S0260210521000358.

[5] Online source: https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_ro, accessed on 17 April 2025.

However, its implementation has faced technical and logistical challenges, including delays in launch and concerns about personal data protection.[6]

European Travel Information and Authorisation System (ETIAS). ETIAS is a pre-travel authorisation system for third-country nationals who do not require a visa to enter the Schengen area. It allows for the assessment of security and migration risks prior to travel by checking the information provided by travellers against various European databases, including the SIS, EES and Eurodac. The authorisation is valid for a period of three years or until the expiry of the passport.[7]

ETIAS contributes to strengthening the EU's internal security by enabling the identification of potential threats before they reach the external borders. However, the success of the system depends on interoperability with other IT systems and strict compliance with data protection rules.

Preliminary Conclusions. The impact assessment of SIS, EES and ETIAS highlights the crucial role of these systems in facilitating cross-border police cooperation and strengthening the EU's internal security. The effective implementation and use of these technologies require a coordinated approach at the European level, harmonisation of the legislative framework and continued investment in technological infrastructure and staff training. It is also essential to ensure interoperability between the different systems and strict compliance with personal data protection rules.

3. Identify the Main Administrative and Operational Challenges in Integrating These Systems, Such as Interoperability Issues, Legislative Differences and Concerns About Personal Data Protection

The large-scale integration of technical systems within the European Union, such as the Schengen Information System (SIS), the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS), is an ambitious initiative aimed at strengthening security and cross-border police cooperation. However, the integration process faces significant challenges, particularly with regard to the interoperability of systems, the harmonisation of the legislative framework and the protection of personal data[8].

Interoperability challenges. The SIS, EES and ETIAS systems were developed independently, each with different purposes and structures. This diversity has led to difficulties in ensuring effective interoperability between them.

[6] Online source: https://www.sterlinglexicon.com/immigration-blog/eu-further-postpones-the-implementation-of-etias-and-ees-systems/, accessed on 19 April 2025.

[7] Online source: https://travel-europe.europa.eu/etias/what-etias_en, accessed on 19 April 2025.

[8] Tim Legrand, Christian Leuprecht (2021), „Securing cross-border collaboration: transgovernmental enforcement networks, organized crime and illicit international political economy", *Policy and Society*, Volume 40, Issue 4: 565–586, https://doi.org/10.1080/14494035.2021.1975216

The lack of effective interconnection can lead to gaps in information exchange and delays in the decision-making process of the competent authorities. To address these issues, the European Union has adopted regulations (EU) 2019/817 and 2019/818, which establish a framework for interoperability between large-scale IT systems in the areas of borders, visas, police and judicial cooperation, asylum and migration.[9]

The implementation of interoperability is based on four main technical components: the European Search Portal (ESP), the Shared Biometric Matching Service (sBMS), the Common Identity Repository (CIR) and the Multiple Identity Detector (MID). These tools are designed to facilitate access to relevant information for authorities and improve the identification of individuals, combat identity fraud and ensure data security.[10]

Legislative differences. Another major obstacle to the integration of these systems is the legislative differences between EU Member States. Each country has its own regulations on data protection, access to information and the use of IT systems, which can hinder effective cooperation and the uniform use of systems. For example, some countries may have stricter restrictions on access to biometric data or impose additional conditions for sharing information with other countries.

To overcome these differences, harmonisation of the legislative framework at the European level is needed to ensure a balance between security needs and respect for citizens' fundamental rights. This involves developing common rules and setting uniform standards for data protection and access to information.

Personal data protection. The protection of personal data is a central concern in the context of the integration of the SIS, EES and ETIAS systems. These systems collect and store a significant amount of sensitive data, including biometric information, which raises questions about the confidentiality, security and appropriate use of such data.

There are concerns that the interoperability of the systems could lead to excessive use of data and breach the principle of purpose limitation, according to which data should only be collected and used for specific and legitimate purposes. There is also a risk that individuals may not be adequately informed about how their data is processed and may not be able to exercise their rights, such as access to data, rectification or erasure.[11]

[9] European Commission. (2017). Interoperability of EU information systems for security, border and migration management. Online source: https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_17_5241, accessed on 20 April 2025.

[10] Ibid.

[11] Cristina Blasi Casagran (2021), „Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU", *Human Rights Law Review,* Volume 21, Issue 2: 433–457, https://doi.org/10.1093/hrlr/ngaa057.

To address these concerns, the Interoperability Regulations include provisions on data protection, such as establishing the responsibilities of data controllers, implementing security measures and ensuring supervision by national authorities and the European Data Protection Board.[12]

Preliminary conclusions. The integration of the SIS, EES and ETIAS systems within the European Union brings significant benefits in terms of security and cross-border police cooperation. However, the integration process faces considerable challenges related to interoperability, legislative differences and personal data protection. To ensure the success of this initiative, a coordinated approach at the European level is essential, including the harmonisation of the legislative framework, the implementation of common technical standards and the guarantee of respect for citizens' fundamental rights.

4. Proposed Solutions for Optimising the Use of These Technologies in Support of International Cooperation

The effective use of large-scale IT systems such as SIS, EES and ETIAS depends not only on technological capacity, but also on strategic, legal and institutional alignment between EU Member States. As the literature shows, the impact of these systems is determined by how they are integrated into national processes, in a manner that is clear to us, by the clarity of the rules for their use and by the ability of public administrations to respond to the challenges of rapid digitalisation.[13]

Strengthening institutional capacity and specialised training. One of the most important gaps identified at the current stage of implementation relates to the level of preparedness of national institutions. Law enforcement authorities in several Member States do not have sufficient qualified human resources or standardised procedures for using European systems. To improve this situation, a multi-level training strategy is needed, including:

- continuous technical training in the use of the SIS, EES and ETIAS;
- practical exercises on information exchange in cross-border situations;
- joint training sessions for police, border guards and the judiciary.[14]

[12] Online source: https://home-affairs.ec.europa.eu/policies/schengen/interoperability_en, accessed on 30 April 2025.

[13] Dimitra Markopoulou, Paul De Hert, Vagelis Papakonstantinou (2019), „The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation”, *Computer Law & Security Review*, vol. 35, issue 6, art. 105,336, https://doi.org/10.1016/j.clsr.2019.06.007. Also see Cristina Elena Popa Tache, Cătălin-Silviu Săraru (2025), “Dual Mandate of Digital Leadership or Upholding International Law Within Sovereign Constitutions,” in Javier Cremades and Cristina Hermida (eds.) *Encyclopedia of Contemporary Constitutionalism*, Cham: Springer Nature, https://doi.org/10.1007/978-3-319-31739-7_236-1.

[14] European Union Agency for Law Enforcement Training, *European Union strategic training needs assessment 2022–2025,* Publications Office of the European Union, Budapest, 2021, pp. 19–

Although CEPOL, EU-LISA and Frontex already offer relevant programmes, these need to be expanded and adopted at the national level, particularly in countries with systemic delays.

Legislative harmonisation and clarification of access rights. Legal fragmentation continues to affect the coherent functioning of the systems. A clearer and more harmonised European legislative framework is needed, based on common rules on access to data, the purpose of its use and the conditions for its storage. A tiered access model could define:

- who has the right to access data;
- for what purpose;
- under what conditions of supervision and accountability?

The European Data Protection Supervisor (EDPS) has emphasised the importance of legal predictability and transparency, in particular in the case of biometric data and risk profiling.[15]

Application of privacy principles and independent supervision. The dilemmas between security and fundamental rights can be overcome by applying the principle of 'privacy by design'. The integration of technological solutions that protect privacy, such as pseudonymisation and data minimisation, should become a mandatory norm. At the same time, independent oversight is essential, both at the national and European level, through data protection authorities and judicial mechanisms.[16]

Promoting interoperability through open and scalable standards. Interoperability should not be imposed exclusively through legislation, but also promoted through open, modular technical solutions. Agencies such as EU-LISA should develop standard interfaces (APIs) that can be adapted to the existing infrastructure of each Member State. This would reduce costs, accelerate integration and encourage local innovation.[17]

Facilitating near real-time data exchange and crisis response. Europe's response to recent crises – the COVID-19 pandemic, the conflict in Ukraine and hybrid attacks – has demonstrated the need for real-time cooperation. Even though the SIS and the EES were not designed for live data transmission, a transition to accelerated operational interoperability is needed, especially in the context of risk management and rapid response.[18]

20.

[15] Online source: https://artificialintelligenceact.eu/wp-content/uploads/2022/05/AIA-EDPBEDPS-Opinion-18-June-21.pdf, accessed on 1 May 2025.

[16] González Fuster, Gloria, Rosamunde Van Brakel and Paul De Hert (eds.) (2022), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics,* Research Handbooks in Information Law series, Edward Elgar Publishing, pp 1-8.

[17] Online source: https://data.europa.eu/en/news-events/news/embracing-open-standards-open-data-ecosystem-interoperability-across-europe, accessed on 1 May 2025.

[18] Dunja Duić, Marijo Rošić, (2022), "Interoperability between the EU information systems – from an idea to the realisation", *Police and Security*, Vol. 31, No. 2: 118-148, https://hrcak.srce.hr/2809

Investments in secure communications infrastructure and rapid-response capabilities must be prioritised to enable the use of systems not only for administrative purposes but also as proactive operational tools.

5. Comparative Case Study: Romania, Germany and the Netherlands in the Context of the Implementation of the EES, ETIAS and the Use of the SIS

Romania. Schengen status: Romania became a member of the Schengen area on 1 January 2025, following the removal of air and sea border controls on 31 March 2024 and land border controls at the beginning of 2025, following a decision by the EU Council.[19]

Implementation of the EES and ETIAS: With a view to accession, Romania has made sustained efforts to prepare the technical and legislative grounds for the integration of the EES and ETIAS systems. According to the Ministry of Internal Affairs, the national infrastructure is interoperable with the platforms developed by EU-LISA and staff are trained in their use. However, like other Member States, Romania is following the updated EU implementation timetable: the EES is planned for October 2025 and ETIAS for the end of 2026.[20]

Use of SIS: Romania actively uses SIS for alerts on wanted persons, stolen or missing objects and refusal of entry. According to EU-LISA reports, Romania contributes consistently to the volume of alerts and ranks among the top Member States in Central and Eastern Europe in terms of police cooperation through SIS.

Germany. EES and ETIAS implementation: Germany is one of the countries that has officially requested a postponement of the EES implementation, citing technical and infrastructure difficulties, as well as concerns about border bottlenecks. The European Commission has accepted these arguments, updating the timetable to 2025 and 2026. The federal authorities are currently working with Frontex and EU-LISA to test the new operational flows.

Use of the SIS: Germany is one of the largest contributors to and users of the SIS. The German federal police and immigration services consult the system daily and the data is constantly updated. According to EU-LISA, Germany entered over 850,000 alerts in 2023, a large proportion of which relate to wanted persons or entry bans.

The Netherlands. EES and ETIAS implementation: The Netherlands

93.

[19] Online source: https://hungarian-presidency.consilium.europa.eu/en/news/bulgaria-and-romania-fully-join-the-schengen-zone/, accessed on 30 April 2025.

[20] Online source: https://travel-europe.europa.eu/etias/news-corner/revised-timeline-ees-and-etias-2025-04-14_en, accessed on 30 April 2025.

faces similar challenges to Germany, mainly due to the complexity of its decentralised IT infrastructure and the need for interoperability with other internal systems (e.g. migration and justice databases). Although the Dutch authorities are well prepared, they have supported postponing the implementation of the EES to prevent possible traffic disruptions at border points.

Use of the SIS: The Netherlands makes extensive use of the SIS, including for sharing alerts on missing persons, minors in danger and wanted items (vehicles, documents, weapons). It cooperates actively with other Member States through the SIRENE channels and is considered a model for the application of good practices in the standardisation of alerts.[21]

Preliminary conclusion. All three countries analysed – Romania, Germany and the Netherlands – are aware of the importance of the SIS, EES and ETIAS systems for strengthening the internal security of the European Union and effective police cooperation. However:

- **Romania**, which recently joined Schengen, is taking a proactive approach to implementation and is successfully aligning itself with European technical requirements;
- **Germany**, although it has the technological capacity, has reported logistical and staffing vulnerabilities that justify a delay;
- **The Netherlands**, with its advanced infrastructure, supports the postponement to ensure the stability of operational flows.

This comparison demonstrates that large-scale system interoperability depends not only on technology, but also on administrative capacity, political will and strategic synchronisation between Member States.

6. General conclusions

This paper has highlighted that the large-scale technical systems developed at the EU level – SIS, EES and ETIAS – offer considerable potential for strengthening cross-border police cooperation and European internal security. However, realising this potential is conditional on a number of administrative, legal and technical factors that need to be carefully managed.

The analysis has shown that the lack of functional and semantic interoperability, legislative fragmentation and data protection concerns remain major obstacles. At the same time, the lack of institutional capacity – in particular in terms of staff training and standardisation of procedures – affects the operational efficiency of these systems.

[21] Schengen Information System (SIS) statistics. (n.d.). [Data set]. European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. Online source: http://data.europa.eu/88u/dataset/schengen-information-system-sis-statistics, accessed on 1 May 2025.

To overcome these difficulties, coordinated action at the European level is needed, including:

- harmonising legislative frameworks on data access and use;
- expanding specialised training for operators and decision-makers;
- applying uniform standards on data protection and cybersecurity;
- encouraging the development of open and scalable interoperable solutions.

Ultimately, cross-border police cooperation is not just a matter of IT infrastructure, but one of the shared administrative visions, political responsibility and respect for fundamental rights. Only through an integrated and balanced approach will the European Union be able to transform these technical systems into genuine tools for prevention, security and solidarity between Member States.

Bibliography

1. Casagran, Cristina Blasi (2021), „Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU", *Human Rights Law Review,* Volume 21, Issue 2: 433–457, https://doi.org/10.1093/hrlr/ngaa0 57.
2. Duić, Dunja & Marijo Rošić, (2022), "Interoperability between the EU information systems – from an idea to the realisation"*, Police and Security*, Vol. 31, No. 2: 118-148, https://hrcak.srce.hr/2809 93.
3. European Commission. (2017). *Interoperability of EU information systems for security, border and migration management*. Online source: https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_17_5241, accessed on 20 April 2025.
4. European Union Agency for Law Enforcement Training, *European Union strategic training needs assessment 2022–2025,* Publications Office of the European Union, Budapest, 2021.
5. González Fuster, Gloria, Rosamunde Van Brakel and Paul De Hert (eds.) (2022), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics,* Research Handbooks in Information Law series, Edward Elgar Publishing.
6. Legrand, Tim & Christian Leuprecht (2021), „Securing cross-border collaboration: transgovernmental enforcement networks, organized crime and illicit international political economy", *Policy and Society*, Volume 40, Issue 4: 565–586, https://doi.org/10.1080/14494035.2021.1975216.
7. Markopoulou, Dimitra, Paul De Hert & Vagelis Papakonstantinou (2019), „The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation"*, Computer Law & Security Review*, vol. 35, issue 6, art. 105,336, https://doi.org/10.1016/j.clsr.2019.06.007.
8. Popa Tache, Cristina Elena & Cătălin-Silviu Săraru (2025), "Dual Mandate of Digital Leadership or Upholding International Law Within Sovereign Constitutions," in Cremades, Javier and Cristina Hermida (eds.) *Encyclopedia of Contemporary Constitutionalism*, Cham: Springer Nature, https://doi.org/10.1007/978-3-319-31739-7_236-1.

9. Russo, Alessandra & Eva Magdalena Stambøl (2022). "The External Dimension of the EU's Fight against Transnational Crime: Transferring Political Rationalities of Crime Control." *Review of International Studies* vol. 48, no. 2: 326–45. https://doi.org/10.1017/S0260210521000358.
10. Schengen Information System (SIS) statistics. (n.d.). [Data set]. European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. Online source: http://data.europa.eu/88u/dataset/schengen-information-system-sis-statistics, accessed on 1 May 2025.
11. Wong Villanueva, Jose L., Tetsuo Kidokoro, and Fumihiko Seta (2020) "Cross-Border Integration, Cooperation and Governance: A Systems Approach for Evaluating 'Good' Governance in Cross-Border Regions." *Journal of Borderlands Studies* 37 (5): 1047–70. doi: 10.1080/08865655.2020.1855227.