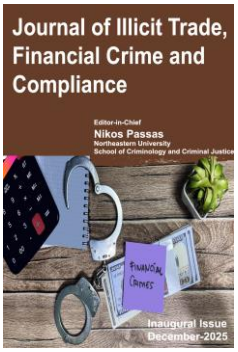
Journal of Illicit Trade, Financial Crime, and Compliance

ISSN (online): 3070-6122



Eurojust's Resource Paradox: Mandate-Resource Misalignment in Digital Judicial Cooperation

Nikos Passas*

Northeastern University, Boston, MA 02115, USA

ARTICLE INFO

Article Type: Research Article

Keywords:
Eurojust
Judicial cooperation
Digitalization of justice
JIT collaboration platform
Criminogenic asymmetries
Multi-annual financial framework

Timeline:
Received: October 25, 2025
Accepted: November 29, 2025
Published: December 10, 2025

Citation: Passas N. Eurojust's resource paradox: Mandate-resource misalignment in digital judicial cooperation. J Illicit Trade Financ Crime Compli. 2025; 1: 50-57.

DOI: https://doi.org/10.65879/3070-6122.2025.1.06

ABSTRACT

The Eurojust Single Programming Document (SPD) 2026–2028 articulates a forward-leaning vision for the agency as a central, digital, and globally connected hub for judicial cooperation. It simultaneously reveals a widening gap between an expanding mandate and constrained resources [1]. Drawing on the SPD's workload projections, budgetary trajectory, and programmatic priorities, this article argues that Eurojust's strategy is appropriately diagnostic but operationally reactive, primarily because it is tethered to demand-driven caseloads and capped by the current Multi-Annual Financial Framework (MFF). The result is a "resource paradox": new tasks without commensurate funding, a ceiling on efficiency gains, and negative priorities that directly affect complex case support, cybersecurity posture, external cooperation, and the integrity of core digital initiatives. The article examines the risks embedded in Eurojust's digitalization program (notably CMS integration, JUDEX, and interoperability) and in expanded third-country cooperation, and proposes actionable reforms: (i) treat the SPD as an investment-grade business case; (ii) establish a realistic resource baseline in the forthcoming Eurojust Regulation revision; (iii) fund cybersecurity to the level of systemic risk; and (iv) embed robust safeguards for data protection, fundamental rights, and accountability across interoperable systems and external partnerships.

*Corresponding Authors
Emails: n.passas@northeastern.edu

1. Introduction

Eurojust's SPD 2026–2028 is notable for its candor and ambition [1]. It sketches the contours of a transformed operational environment: cross-border organized crime increasingly digitalized; networks that extend well beyond EU borders; and rising complexity across cybercrime, terrorism, and Core International Crimes (CIC) [1]. The SPD's strategic bet - accelerated digitalization, enhanced data cross-matching, and reinforced external partnerships - is conceptually sound [1,2]. Yet the same document reveals critical constraints: the agency has "effectively reached the limits of efficiency gains," the caseload-to-staff ratio rose by 46.1% between 2020 and 2024, and substantial human and financial reinforcements requested for 2026 (32 staff and €14.8 million) were not supported [1]. This article interrogates that tension and explores its implications for the EU's internal security architecture.

The contemporary landscape of transnational crime reflects a broader phenomenon: the emergence of "criminogenic asymmetries" produced by globalization—structural disjunctions, mismatches, and inequalities in the spheres of politics, culture, the economy, and the law that create opportunities for cross-border criminality [3,4]. These asymmetries fuel demand for illegal goods and services, generate incentives for criminal enterprise, and crucially, reduce the capacity of law enforcement and judicial authorities to mount effective responses [5]. Eurojust operates precisely at the nexus where these criminogenic asymmetries manifest most acutely, rendering its resource constraints not merely an administrative inconvenience but a structural vulnerability in the EU's internal security architecture.

The threat landscape has been comprehensively documented by Europol's Serious and Organised Crime Threat Assessment (EU SOCTA), which identifies increasingly networked, transnational, and digitally-enabled criminal organizations operating across EU borders [6,7]. The most threatening criminal networks affecting the EU comprise 112 different nationalities and operate across more than 45 countries, with activities spanning drug trafficking, money laundering, cybercrime, and human trafficking [7]. Responding effectively to these threats requires robust judicial coordination mechanisms—precisely Eurojust's core mandate.

2. Reactive Strategy in a Fast-Moving Threat Landscape

The SPD correctly identifies the drivers of Eurojust's workload: Member State demand for coordination meetings (CMs), coordination centres (CCs), and joint investigation teams (JITs), alongside growth in priority crime areas such as swindling/fraud, money laundering, drug trafficking, cybercrime, and migrant smuggling [1]. However, a demand-driven model is inherently reactive; it lags behind emerging criminal dynamics and does not capitalize fully on Eurojust's legal capacity to act on its own initiative (including where prosecution on common bases is required) under the Eurojust Regulation [8,1]. While the SPD presents steps to strengthen proactive actions, link analysis through the Counter-Terrorism Register (CTR), "hit/no-hit" systems, and enhanced CMS link reviews, the realization of these steps is limited by resource constraints and by the complexity of multi-system interoperability [9,1].

This reactive posture must be understood against the backdrop of how criminal enterprises have evolved. Processes of globalization have multiplied cross-border links and intensified interconnectedness, and criminal enterprises have inevitably become global as well, exploiting weaknesses in the existing regulatory patchwork [10]. The interface between legal and illegal actors has grown increasingly complex, with criminal networks operating through symbiotic relationships with legitimate businesses and institutions—relationships that can be collaborative, parasitical, or predatory in nature [10,11]. This complexity demands proactive judicial coordination, yet Eurojust's resource constraints push it toward reactive modes of operation.

Scholars of EU criminal law have emphasized that effective cross-border cooperation requires not merely formal legal instruments but sustained institutional capacity and mutual trust among judicial authorities [12-14]. The principle of mutual recognition, which underpins the European Arrest Warrant and the European Investigation Order, functions effectively only when supported by adequate resources and genuine inter-institutional cooperation [15]. Eurojust's resource constraints thus threaten to undermine the broader architecture of EU criminal justice cooperation.

The risk of a reactive posture is not theoretical. In a digitalized criminal ecosystem, the advantage lies with actors who exploit latency in investigative coordination, jurisdictional conflicts, and data siloing. The phenomena of "global anomie" and "dysnomie", the normlessness and regulatory dysfunction that accompany rapid globalization, further compound these challenges, creating environments where criminal actors can operate with relative impunity across borders [16]. Without adequate resourcing, Eurojust's strategic edge – with proactive link detection, early-stage legal and analytical assistance, and rapid convening - may be blunted precisely when it is most needed [1].

3. The Resource Paradox Under the Current MFF

The SPD surfaces a structural paradox: ambition meets austerity. Despite prior deviations above initial MFF allocations (including reinforcements in 2021–2025), Eurojust now reaches the efficiency frontier; further gains can only marginally offset workload increases or staff absences [1]. The non-approval of requested reinforcements for 2026 structurally constrains core operations. The immediate effects are captured in the SPD's "negative priorities," which include capped support to complex cases, limited ability to increase JIT financial assistance, elevated audit and contract risks for digital projects (new CMS, DCJ program, JIT Collaboration Platform), and reduced capacity to bolster cybersecurity and external cooperation (including the EJCN and EJOCN) [1].

Compounding the paradox, several new tasks lack accompanying legislative financial statements (LFS), notably Eurojust's role as ECRIS-TCN contact point for third countries and international organizations, and the establishment of a dedicated EJCN secretariat, even as technical and governance requirements intensify under new cyber and information security regulations [1,17,18]. Mandates without funding make for risk migration: where legal obligations spur technical exposure (interfaces, data flows, user access), unfunded tasks can degrade performance elsewhere or generate systemic vulnerabilities [1].

This resource-mandate mismatch reflects a broader pattern observable in international efforts to combat transnational crime and terrorism financing. As research on informal value transfer systems has demonstrated, effective regulatory responses require not only legal frameworks but sustained investment in analytical capacity, inter-agency coordination, and specialized expertise [5,19,20]. The failure to match mandates with resources is particularly consequential in domains requiring technical sophistication and cross-border coordination, precisely Eurojust's operating environment.

The Council of Europe's White Paper on Transnational Organised Crime similarly emphasized that effective responses require sustained investment in cooperation mechanisms, noting that many issues and obstacles in judicial cooperation can be resolved through properly resourced coordinating mechanisms [21]. The European Parliament has reinforced this message, calling for enhanced resources to match expanded mandates for EU Justice and Home Affairs agencies [22].

4. Digitalization: Benefits and Embedded Risks

Eurojust's digitalization roadmap centers on a new Case Management System (CMS) with enhanced interoperability, connection to external systems (JUDEX, ECRIS-TCN, e-CODEX, SIS), and improved tools and reporting for JIT practitioners [1,2]. The SPD rightly embraces "data protection by design and default" and highlights fundamental rights (e.g., access to justice, defense rights, non-discrimination) as part of system redesign [1,8].

The digitalization imperative is driven in part by the evolving nature of transnational financial crime, which increasingly exploits technological capabilities and requires sophisticated analytical responses. Trade-based money laundering, cybercrime, and identity-related offenses all leverage digital systems in ways that demand equally sophisticated investigative and prosecutorial tools [23]. The emergence of cryptocurrencies and blockchain-based financial systems has added new dimensions to this challenge, creating novel opportunities for money laundering, fraud, and terrorism financing that require specialized expertise and technological capability to investigate effectively [24]. The pseudo-anonymous nature of cryptocurrency transactions, combined with the use of mixers, tumblers, and cross-chain bridges, presents significant challenges for judicial cooperation, challenges that Eurojust must be equipped to address [25,26].

The consolidation of data across systems can enable the kind of link analysis and pattern detection that is essential for disrupting complex criminal networks. The recently adopted e-Evidence Regulation represents a significant step toward more efficient cross-border access to electronic evidence, allowing judicial authorities in one Member State to request data directly from service providers in another without engaging intermediary authorities [27,28]. However, as scholars have noted, such instruments raise fundamental questions about the privatization of mutual trust and the role of private actors in law enforcement [12,29].

4.1. Two Risk Vectors Warrant Emphasis

4.1.1. Cybersecurity Maturity and Business Continuity

Implementing a zero-trust architecture, a security operations center, updated governance, and risk-control frameworks will require not only capital expenditure but specialist staffing and continuous monitoring. The SPD sets 2026 milestones but flags resource gaps that jeopardize timely implementation [1,19]. Under-delivery here risks cascading impacts: incident response delays, audit findings, and reputational damage in highly sensitive casework [1]. Given that criminal networks have demonstrated sophisticated capabilities in exploiting regulatory and technological gaps [10], cybersecurity vulnerabilities in judicial cooperation systems represent an attractive target. The increasing sophistication of cryptocurrency-enabled crime, including ransomware attacks that generated over $1 billion in payments in 2023 alone, underscores the urgency of robust cybersecurity measures [25].

The intersection of criminal justice and cybersecurity has become increasingly complex, with law enforcement agencies requiring not only technical capabilities but also legal frameworks that address novel threats in the digital environment [50]. The EU has advanced comprehensive cybersecurity frameworks including the Network and Information Systems Directive (NIS2), Cybersecurity Act, and Critical Entities Resilience Directive, all requiring substantial organizational investment [30]. Fundamental rights implications of cybersecurity measures require careful calibration to ensure proportionality and necessity [31].

4.1.2. Interoperability, Function Creep, and Rights Protection

The push for interoperability (CTR, hit/no-hit, JUDEX, ECRIS-TCN) is essential to operational effectiveness. But increasing reciprocal access and cross-matching can engender function creep or over-collection, in the event of absent granular access controls, robust minimization, and transparent oversight. The SPD points to safeguards; however, explicit guardrails against mission expansion beyond statutory boundaries, together with strong accountability mechanisms, must be codified as systems scale [1,2]. The variety, velocity, and volume of personal data in criminal investigations require careful attention to purpose limitation and data minimization principles [32,33].

Recent scholarship has highlighted the challenges of implementing these interoperable systems across EU agencies. Faggiani's analysis of EU-LISA's role in coordinating digitalisation across Eurojust, Europol, and other institutions notes that while the technical infrastructure offers "extraordinary potential," implementation has been marked by "persistent opacity" in governance structures and decision-making processes [48]. Similarly, Kot's examination of interoperability as a tool for combating terrorism and serious cross-border crime identifies both the benefits of integrated information systems and the persistent challenges of ensuring proportionate access controls [49].

The European Commission's 2024-2025 guidance on lawful access to data emphasizes that access must be necessary, proportionate, based on clear legal rules, subject to independent oversight, and accompanied by effective remedies [34]. The lessons from anti-money laundering regulation are instructive here: well-intentioned frameworks can produce unintended consequences when implementation outpaces safeguards, potentially driving legitimate activities into less regulated channels while failing to disrupt sophisticated criminal operations [19].

5. External Cooperation: Quality Over Quantity

The SPD anticipates deepening cooperation with third countries and international organizations, increasing the number of liaison prosecutors (LPs), and enabling structured exchanges of personal data [1]. It also positions

Eurojust to implement Council conclusions on strengthening judicial cooperation with third countries in the fight against organized crime [34]. Expanded reach is vital, but it raises differentiated risks tied to legal standards, governance practices, and data protection regimes outside the EU.

Eurojust's role in the external dimension of EU judicial cooperation has expanded considerably since its establishment [51]. As Škrlec notes, Eurojust's engagement with third countries and international organizations extends its influence but also raises questions about the consistency of safeguards and the transparency of cooperation arrangements [51,52].

Past experiences on trans-governmental enforcement networks have highlighted both the potential and the pitfalls of cross-border cooperation arrangements [35,36]. The success of external cooperation hinges on quality, not volume: agreements should embed transparent safeguards, purpose limitation, independent redress, and auditability [1,34]. Without these, data-sharing and operational collaboration can generate rights risks and evidentiary challenges, undercutting both prosecution efficacy and public trust [1].

The Second Additional Protocol to the Budapest Convention on Cybercrime, adopted in 2021, represents an important step toward enhanced international cooperation, but its effectiveness depends on adequate implementation capacity [37,27]. The European Data Protection Supervisor has emphasized that international agreements for crime fighting must explicitly protect fundamental rights and provide for data subject remedies [38].

The expansion of Eurojust's external network must also account for the heterogeneity of legal systems and enforcement capacities among partner jurisdictions. The criminogenic asymmetries that characterize the international system, including divergent legal frameworks, variable enforcement capacity, and differential transparency regimes, can be exploited by criminal actors seeking jurisdictional arbitrage [3]. Effective external cooperation requires not merely formal agreements but sustained attention to capacity-building, mutual legal assistance procedures, and the alignment of evidentiary standards.

The UNODC has emphasized that multilateral responses to transnational organized crime remain fragmented and often ineffective, with powerful states sometimes preferring informal, unilateral solutions that pose challenges to rule of law and human rights [39,40]. Eurojust's external cooperation must navigate these tensions while maintaining fidelity to EU fundamental rights standards, a task that requires both diplomatic sophistication and adequate institutional capacity.

6. Policy Recommendations

1. **Treat the SPD as an Investment-Grade Business Case.** The SPD offers clear workload drivers, risk registers, and programmatic milestones. It should be leveraged to justify urgent reinvestment, beyond incremental adjustments, commensurate with Eurojust's strategic role in the internal security ecosystem [1]. The framing should emphasize that under-investment in judicial cooperation capacity effectively subsidizes transnational criminal enterprise by preserving the jurisdictional fragmentation and coordination latency that criminal networks exploit. The European Commission's evaluation of Eurojust's performance under Regulation 2018/1727 should inform a realistic assessment of resource needs [41].
2. **Set a Realistic Resource Baseline in the Eurojust Regulation Revision.** The forthcoming EJR revision should anchor a sustainable staffing and budgetary framework that reflects the true scope of Eurojust's mandate and the complexity of the transnational criminal environment it confronts. This should include dedicated resourcing for cryptocurrency and blockchain-related investigations, reflecting the growing prominence of these technologies in criminal finance [24].
3. **Fund Cybersecurity to the Level of Systemic Risk.** Given the sensitivity of judicial cooperation data and the demonstrated willingness of criminal actors to exploit digital vulnerabilities, cybersecurity investment should be treated as a core operational requirement rather than a discretionary enhancement. The increasing sophistication of crypto-enabled crime demands particular attention to the security of systems handling financial intelligence [25,7].

4. **Embed Robust Safeguards for Data Protection, Fundamental Rights, and Accountability.** As interoperability expands and external partnerships deepen, proactive investment in oversight mechanisms, redress procedures, and transparency reporting is essential to maintain public trust and legal integrity. The CJEU's jurisprudence on data retention and fundamental rights must inform system design from the outset [32,12].
5. **Develop Proactive Analytical Capacity.** Moving beyond reactive, demand-driven coordination requires investment in the analytical tools and specialist expertise necessary for early detection, link analysis, and strategic case prioritization—the capabilities that can convert Eurojust from a coordination facilitator into a genuine hub for judicial intelligence. Investment in blockchain analytics capabilities should be prioritized given the growing role of cryptocurrencies in transnational crime [24,26].
6. **Strengthen Public-Private Partnerships for Financial Intelligence.** The complexity of modern financial crime, including cryptocurrency-enabled offenses, requires enhanced cooperation between judicial authorities and private sector actors including financial institutions and blockchain analytics providers. Such partnerships should be structured to ensure appropriate safeguards while leveraging private sector expertise [7,25].

Conflict of Interest

The author declares that he has no conflicts of interest related to this research/study.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] Eurojust. Single Programming Document 2026–2028. European Union Agency for Criminal Justice Cooperation, 2025.

[2] European Commission. Digitalization of Justice Communication. Brussels: European Commission; 2020.

[3] Passas N. Structural analysis of corruption: The role of criminogenic asymmetries. Transnational Organized Crime. 1998;4(1):42–55.

[4] Passas N. Globalization and transnational crime: Effects of criminogenic asymmetries. In: Williams P, Vlassis D, editors. Combating transnational crime: Concepts, activities and responses. London: Frank Cass; 2001. p. 22–56.

[5] Passas N. Informal value transfer systems and criminal organizations: A study into so-called underground banking networks. The Hague: Ministry of Justice, The Netherlands; 1999.

[6] Europol. EU Serious and Organised Crime Threat Assessment (SOCTA) 2021. The Hague: Europol; 2021.

[7] Europol. Decoding the EU's Most Threatening Criminal Networks. The Hague: Europol; 2024.

[8] Regulation (EU) 2018/1727 of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust). Off J Eur Union. 2018.

[9] European Commission. Interoperability frameworks for EU information systems. Brussels: European Commission; 2021b.

[10] Passas N. Cross-border crime and the interface between legal and illegal actors. Security Journal. 2003;16(1):19–37.

[11] van Duyne P, von Lampe K, Passas N, editors. Upperworld and underworld in cross-border crime. Nijmegen: Wolf Legal Publishers; 2002.

[12] Mitsilegas V. The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence. Maastricht Journal of European and Comparative Law. 2018;25(3):263–265.

[13] Mitsilegas V. The European model of judicial cooperation in criminal matters: Towards effectiveness based on earned trust. Revista Brasileira de Direito Processual Penal. 2019;5(2):565–595.

[14] Weyembergh A. The principle of ne bis in idem in Europe's Area of Freedom, Security and Justice. In: Bergström M, Mitsilegas V, Quintel T, editors. Research Handbook on EU Criminal Law. 2nd ed. Cheltenham: Edward Elgar; 2024. p. 161–182.

[15] Brière C. Eurojust @ 20: A successful modernization of the agency? In: Bergström M, Mitsilegas V, Quintel T, editors. Research Handbook on EU Criminal Law. 2nd ed. Cheltenham: Edward Elgar; 2024. p. 407–426.

[16] Passas N. Global anomie, dysnomie, and economic crime: Hidden consequences of neoliberalism and globalization in Russia and around the world. Social Justice. 2000;27(2):16–44.

[17] Regulation (EU) 2023/2841 on measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. Off J Eur Union. 2023.

[18] Regulation (EU) 2019/816 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN). Off J Eur Union. 2019.

[19] Passas N. Hawala and other informal value transfer systems: How to regulate them? Risk Management. 2003;5(2):49–59.

[20] Passas N. Informal value transfer systems, terrorism and money laundering. Report to the National Institute of Justice. Boston: Northeastern University; 2003c.

[21] Council of Europe. White Paper on Transnational Organised Crime. Strasbourg: Council of Europe; 2014.

[22] European Parliament. Judicial cooperation in criminal matters: Fact Sheet. Brussels: European Parliament; 2024.

[23] Passas N, editor. Transnational financial crime. London: Routledge; 2016.

[24] Passas N. Cryptocurrencies, blockchain, and financial crimes. International Journal of Criminology and Sociology. 2025;14:76–89.

[25] Chainalysis. The 2024 Crypto Crime Report. New York: Chainalysis; 2024.

[26] OSCE. Decoding Crypto Crime: A Guide for Law Enforcement. Vienna: Organization for Security and Co-operation in Europe; 2024.

[27] Franssen V. Cross-border gathering of electronic evidence in the EU: Toward more direct cooperation under the e-Evidence Regulation. In: Bergström M, Mitsilegas V, Quintel T, editors. Research Handbook on EU Criminal Law. 2nd ed. Cheltenham: Edward Elgar; 2024. p. 183–210.

[28] Tosza S. The e-Evidence Package is adopted: End of a saga or beginning of a new one? European Data Protection Law Review. 2023;9(2):163–172.

[29] Carrera S, Stefan M, Mitsilegas V. Cross-border data access in criminal proceedings and the future of digital justice. CEPS Task Force Report. Brussels: Centre for European Policy Studies; 2020.

[30] European Commission. Communication on a European Approach to Cybersecurity. Brussels: European Commission; 2024.

[31] Porcedda MG. Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In: Porcedda MG, editor. Cybersecurity Regulation in the European Union. Berlin: Springer; 2019. p. 1–30.

[32] De Hert P, Sajfert J. Variety, velocity, and volume of personal data in criminal investigations and proceedings. In: Bergström M, Mitsilegas V, Quintel T, editors. Research Handbook on EU Criminal Law. 2nd ed. Cheltenham: Edward Elgar; 2024. p. 211–237.

[33] Vavoula N. The criminalisation of irregular migration under EU law: An evolving human-rights centred legal framework? In: Bergström M, Mitsilegas V, Quintel T, editors. Research Handbook on EU Criminal Law. 2nd ed. Cheltenham: Edward Elgar; 2024. p. 294–319.

[34] European Commission. Roadmap for lawful and effective access to data for law enforcement. Brussels: European Commission; 2025. COM(2025) 349 final.

[35] Council of the European Union. Council conclusions on strengthening judicial cooperation with third countries in the fight against organised crime. Brussels: Council of the European Union; 2024.

[36] Passas N. Fighting Terror with Error: The Counter-productive Regulation of Informal Value Transfers. Crime, Law and Social Change. 2006b;45(4–5):315–336.

[37] Slaughter A-M. A New World Order. Princeton: Princeton University Press; 2004.

[38] Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Strasbourg: Council of Europe; 2021.

[39] European Data Protection Supervisor. International cooperation to fight crime should respect EU fundamental rights guarantees. Brussels: EDPS; 2025.

[40] UNODC. The Globalization of Crime: A Transnational Organized Crime Threat Assessment. Vienna: United Nations Office on Drugs and Crime; 2010.

[41] SIPRI. Transnational organized crime: A threat to global public goods. Stockholm: Stockholm International Peace Research Institute; 2022.

[42] European Commission. Evaluation of Eurojust under Regulation (EU) 2018/1727 [Internet]. Brussels: European Commission; 2025 [cited 2025 Jan]. Available from: https://commission.europa.eu/publications/evaluation-eurojust_en

[43] European Commission. Regulation (EU) 2023/2844 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters. Off J Eur Union. 2023. Regulation 2023/2844.

[44] European Commission. European e-Justice Strategy 2024–2028. Off J Eur Union. 2025. C/2025/437.

[45] Pingen A, Wahl T. New Legal Framework on Digitalisation of Judicial Cooperation. eucrim: European Criminal Law Review. 2024;4:331–332.

[46] Eurojust. Digital Criminal Justice Programme [Internet]. The Hague: Eurojust; 2025 [cited 2025 Jan]. Available from: https://www.eurojust.europa.eu/judicial-cooperation/instruments/digital-criminal-justice-programme

[47] European Data Protection Supervisor. International agreements to fight crime require strong data protection safeguards. Brussels: EDPS; 2023.

[48] De Hert P. Cybersecurity as a Fundamental Right: Towards a Digital Safety Charter for Europe. Computer Law & Security Review. 2024;51:105904.

[49] Faggiani V. Digitalisation of criminal justice in the EU through EU-LISA cooperation with Eurojust and Europol: between extraordinary potential and persistent opacity. Unio - Eu Law Journal. 2024;10(2):40–56. https://doi.org/10.21814/unio.10.2.6051

[50] Kot E. Interoperability of EU information systems – a tool to fight terrorism and serious cross-border crime (part I). Problemy Kryminalistyki. 2022;(315):5–12. https://doi.org/10.34836/pk.2022.315.1

[51] Mandayam R. The intersection of criminal justice and cybersecurity: legal implications. International Journal of Scientific Research in Engineering and Management. 2024;9(2):1–7. https://doi.org/10.55041/ijsrem41544

[52] Škrlec B. Eurojust and external dimension of EU judicial cooperation. Eucrim - The European Criminal Law Associations Forum. 2019;14(3):188–193. https://doi.org/10.30709/eucrim-2019-018