



AI-REGULATION.COM

Upgrading Europol: Artificial Intelligence, Operational Integration, and the Forthcoming Revision of the Europol Regulation

By Evangelos Zarkadoulas





Evangelos Zarkadoulas is a Senior Officer of the Hellenic Police specializing in the investigation of serious and organized crime, having served, inter alia, in the Homicide Department of the Attica Security Directorate. In recent years, he has held the position of Justice and Home Affairs Counsellor at the Permanent Representation of Greece to the European Union, where he acts as a liaison between the Hellenic Police and the European institutions on matters of internal security, police cooperation, and information exchange. He represents Greece in working groups of the European Commission and the European Artificial Intelligence Board that address the use of artificial intelligence in law enforcement and its regulation within the EU institutional framework. Academically, he is a PhD candidate in Law and a researcher at the Cyber and Data Security Lab of the Vrije Universiteit Brussel (VUB), focusing on the proportionate and responsible use of artificial intelligence by law enforcement authorities in the European Union.

To cite this article: E. Zarkadoulas, *Upgrading Europol: Artificial Intelligence, Operational Integration, and the Forthcoming Revision of the Europol Regulation*, AI Regulation Papers 26-05-5, [AI-Regulation.com](https://www.ai-regulation.com), May 27th, 2026.

These statements are attributable only to the author, and their publication here does not necessarily reflect the view of the other members of the AI-Regulation Chair or any partner organizations.

Upgrading Europol: Artificial Intelligence, Operational Integration, and the Forthcoming Revision of the Europol Regulation

Debates concerning the forthcoming reform of Europol illustrate a broader transformation in the European Union's approach to internal security management. This article contends that Europol is evolving into an AI-enabled, infrastructure-oriented model for European law enforcement. Such a model prioritises interoperability, expansive ecosystems, and intelligence-driven information exchange. The analysis demonstrates Europol's transition from a support-oriented agency to an analytical infrastructure embedded within interconnected law enforcement ecosystems. Furthermore, the article explores the convergence of policing, judicial cooperation, electronic evidence, and AI analytics, as reflected in ongoing policy discussions regarding the simultaneous reforms of Europol and Eurojust. Finally, this article evaluates the constitutional challenges arising from these dynamics, particularly in relation to data governance and the constraints on supranational operational integration within the EU's decentralised framework.

Current discussions surrounding the forthcoming reform of Europol increasingly reflect a broader transformation in the architecture of European Union internal security governance, as law enforcement operates in data-intensive, technologically mediated environments. The European Commission is expected to introduce parallel reform proposals for Europol and Eurojust in late June 2026, in response to accelerating digitalisation, expanding cross-border criminal networks, encrypted communications, and increased reliance on large-scale data analysis.¹ Institutional programming documents, strategic policy papers, and intergovernmental discussions now frame artificial intelligence, interoperability, and operational analytics as structural prerequisites for contemporary European policing cooperation, rather than as peripheral technological enhancements.²

Within the Europol context, interoperability refers not merely to technical connectivity between databases and information systems, but also to the practical capacity to facilitate continuous analytical coordination, secure information exchange and integrated cross-border law enforcement cooperation across distributed European internal security infrastructures. As a consequence, the reform trajectory extends beyond the expansion of a Union agency's toolkit, signifying a broader institutional shift toward infrastructure-driven, intelligence-led models of European law enforcement governance.

Historically, Europol functioned primarily as a support-oriented agency, facilitating criminal intelligence exchange among Member States within a decentralised policing framework established by Article 88 TFEU.³ Its scope was constrained by the absence of autonomous coercive powers and the predominance of Member State control over investigations and law enforcement activities. Recent institutional developments, however, indicate a gradual yet significant transformation. The expansion of Europol's mandate to process large and complex datasets, including those requiring AI-supported filtering, correlation and analytical prioritisation mechanisms, together with the increased prominence of Operational Task Forces, real-time investigative support capabilities, and interoperable analytical environments, collectively signal a departure from a purely information-sharing model.⁴ Europol is now regarded as an analytical infrastructure that supports intelligence-led coordination across interoperable European policing ecosystems.

This transformation extends beyond Europol itself. The emerging internal security architecture integrates policing, judicial cooperation, digital evidence governance, interoperability frameworks, and platform-based information ecosystems within broader transnational structures. The evolving relationship between Europol and Eurojust, the growing significance of Joint Operational Platform initiatives, Operational Task Forces,⁵ and Joint Investigation Teams,⁶ the centrality of electronic

¹ European Commission, *Commission Work Programme 2026: Europe's Independence Moment* COM(2025) 870 final, Annex I, 21 October 2025; Preparatory institutional discussions concerning the forthcoming Europol and Eurojust reform packages.

² Europol, *Europol Programming Document 2026–2028* (Management Board, December 2025); Exchange of views within the JHA Council and relevant working parties on operational cooperation, interoperability and AI-supported law enforcement coordination.

³ Treaty on the Functioning of the European Union (TFEU), Consolidated Version [2016] OJ C 202/1, art 88.

⁴ Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794 as regards Europol's cooperation with private parties, the processing of

personal data by Europol in support of criminal investigations, and Europol's role in research and innovation [2022] OJ L 169/1.

⁵ Operational Task Forces are coordinated cross-border investigative structures supported by Europol for specific operational priorities and complex investigations.

⁶ Unlike Europol-supported Operational Task Forces, which primarily function as continuous coordination and analytical support structures, Joint Investigation Teams are temporary case-specific investigative mechanisms coordinated with Eurojust's support.

evidence mechanisms such as SIRIUS,⁷ and the integration of criminal analytics into cross-border investigations collectively indicate the development of integrated operational-judicial governance environments at the Union level.⁸ Concurrently, collaboration with private technology platforms, financial intermediaries, and digital service providers has become an established component of European law enforcement governance.

In parallel, the operationalisation of AI-enabled policing infrastructures introduces significant constitutional and governance challenges. The increasing reliance on large-scale analytical ecosystems, exploratory data processing, and interoperable environments places pressure on traditional law enforcement data governance models, which are based on predefined relevance, identifiable data subject categories, and purpose-limited processing. Nevertheless, the reform trajectory does not pursue constitutional federalisation of policing powers within the Union. This article argues that the combined effect of recent legislative amendments to the Europol Regulation and emerging technologically driven law enforcement needs is progressively repositioning Europol towards an intelligence-led, AI-supported model of European law enforcement governance characterised by interoperable analytical infrastructures, large-scale data ecosystems and integrated cross-border information exchange.

I. From Information Exchange to AI-Enabled Operational Infrastructure

For most of its institutional history, Europol operated primarily as a coordination and criminal intelligence assistant agency facilitating information exchange between Member State law enforcement authorities within a decentralised policing framework. In practice, Europol's role historically focused on functions such as criminal intelligence analysis, support for cross-border investigations, coordination of information exchange through systems such as SIENA⁹ and analytical assistance to national authorities.

However, traditional coordination mechanisms were primarily designed to facilitate reactive exchanges of

information between national authorities in individual investigations, rather than to support continuous analytical processing, large-scale data correlation and real-time cooperation across interconnected cross-border law enforcement ecosystems. In contrast, contemporary investigations now frequently involve encrypted communications, large-scale digital evidence, AI-supported analytical processing, online criminal ecosystems and rapidly evolving datasets that cannot easily be managed through fragmented or reactive coordination mechanisms alone. Accordingly, Europol's role increasingly extends beyond facilitating information exchange toward supporting continuous analytical coordination through interoperable infrastructures capable of integrating AI-supported analysis, scalable data processing and real-time practical support throughout multiple jurisdictions.

The following institutional developments illustrate this evolution. In particular, the 2022 amendments to the Europol Regulation, the subsequent Joint Statement of the European Police Chiefs and the additional legislative amendments adopted in 2025 increasingly signal a broader transformation in the organisational logic of European law enforcement cooperation. Rather than focusing exclusively on information exchange, these turning points progressively reposition Europol within the operational architecture of European security governance.

Initially, Regulation (EU) 2022/991 was notably meaningful because it expanded Europol's ability to process large and complex datasets, strengthened its role in supporting innovation and research activities, facilitated cooperation with private parties and online service providers, and enabled broader forms of analytical support for Member States authorities.¹⁰ These modifications are especially important in increasingly data-intensive investigative environments involving encrypted communications, large-scale digital evidence and AI-supported analytical processing. Rather than merely

⁷ SIRIUS is an EU-funded project jointly implemented by Europol and Eurojust that supports law enforcement and judicial authorities in obtaining cross-border electronic evidence through cooperation with online service providers, including by facilitating coordination, guidance and information exchange concerning electronic evidence requests.

⁸ Europol and Eurojust, *Joint Europol-Eurojust Annual Report 2024 to the Council of the European Union, European Parliament and the European Commission* (2025).

⁹ SIENA (Secure Information Exchange Network Application) is Europol's secure platform for information exchange between Member State law enforcement authorities and partners.

¹⁰ Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation [2022] OJ L 169/1.

enabling information exchange, Europol is now regarded as an analytical infrastructure supporting intelligence-led coordination across interoperable European policing ecosystems. In this context, “operational infrastructure” increasingly refers not merely to institutional coordination mechanisms but also to interconnected analytical environments, support platforms, secure information-sharing systems, and AI-supported capabilities that facilitate continuous cross-border law enforcement cooperation.

Another milestone within this broader institutional trajectory was the Joint Statement of the European Police Chiefs on the Future Development of Europol, adopted in Krakow on 29 April 2025.¹¹ While Member States have historically supported Europol’s information analysis and exchange functions, the Krakow Statement is particularly pivotal because it explicitly endorsed Europol’s progressive technological evolution in AI-enabled, data-intensive policing environments. The Police Chiefs supported the constant evolution of Europol as the European central agency for information analysis and assistance in criminal matters, while simultaneously reaffirming that investigative and coercive powers must remain with the Member States.

The Statement also endorsed strengthening Operational Task Forces, the EMPACT platform,¹² interoperability frameworks, SIENA-enabled information exchange systems, and Europol’s role as an EU Information Hub capable of processing large and complex datasets. In practical terms, this increasingly implies the capacity to support cross-border analytical information exchange through scalable AI-assisted analytical environments capable of processing extensive datasets originating from multiple national authorities and digital ecosystems. The Statement also addressed the expansion of Europol’s technological capacities through artificial intelligence, machine learning, large language models, facial recognition technologies, drones and secure European police cloud infrastructures.

In parallel, the Statement advocated further development of the Europol Innovation Lab and the possible establishment of a future AI Lab.

Particularly significant was the support expressed for strengthening Europol’s role in facilitating operational cooperation and information exchange with private parties, including online service providers, financial institutions and cryptocurrency exchanges, especially in the context of cross-border digital investigations, access to electronic evidence and the detection of illicit financial and cryptocurrency transactions, while maintaining compliance with Union data protection standards. Collectively, these positions illustrate the extent to which Member States increasingly perceive Europol not merely as a coordination and assistance platform, but as a technologically enabled infrastructure supporting intelligence-led European police cooperation.

From a legislative perspective, Europol’s mandate was additionally reinforced by Regulation (EU) 2025/2611, which entered into force in January 2026 and introduced additional amendments to the Europol Regulation to strengthen Europol’s support capacities in the areas of migrant smuggling and trafficking in human beings.¹³ The Regulation, accommodating the Joint Statement of the European Police Chiefs on the Future Development of Europol, consolidates Europol’s role as the Union’s criminal information hub by bolstering the use of SIENA, strengthening assistance for Operational Task Forces and EMPACT activities, expanding Europol’s on-the-field deployments and enabling enhanced criminal intelligence exchange among Member States. Viewed collectively, these mechanisms increasingly contribute to advancing a more integrated infrastructure capable of supporting continuous cross-border analytical coordination across distributed European law enforcement environments.

In practice, the integration of interoperable information exchange systems, coordination structures, and AI-supported analytical environments progressively enables Europol to function not merely as an information-sharing platform but as a scalable infrastructure supporting intelligence-led police cooperation across the

¹¹ *Joint Statement by the European Police Chiefs on the Future Development of Europol*, Krakow, 29 April 2025.

¹² EMPACT (European Multidisciplinary Platform Against Criminal Threats) constitutes the EU’s operational cooperation framework for tackling serious and organised crime.

¹³ Regulation (EU) 2025/2611 of the European Parliament and of the Council of 16 December 2025 amending Regulation (EU) 2016/794 as regards the strengthening of Europol’s support and enhancing police cooperation, for preventing and combating migrant smuggling and trafficking in human beings [2025] OJ L 2025/2611.

European Union. The last reform¹⁴ also institutionalises the European Centre Against Migrant Smuggling as a permanent centre of specialised expertise within Europol, while strengthening Europol's analytical and support functions, including in relation to biometric data processing, cross-border coordination and large-scale criminal intelligence analysis. Reliance on AI-supported analytical tools intended to assist in identifying cross-border criminal networks, migrant smuggling routes, and high-risk criminal patterns further underscores the importance of these legal modifications.

One of the clearest indicators of this ongoing transformation lies in the centrality of operational analytics within Europol's institutional identity. The Europol Programming Document 2026–2028 explicitly places criminal analysis at the core of the Agency's mission and presents Europol as an “EU criminal information hub” capable of supporting agile and real-time collaboration across Member States.¹⁵

Operational reality increasingly intensifies the role of Europol National Units as distributed coordination and operational support nodes within the broader Europol ecosystem. In this context, Europol National Units could assume a more prominent function in areas such as analytical support, coordination, innovation governance, OSINT-related activities and the facilitation of information exchange between national authorities and Europol. Their importance is particularly significant in interoperable, AI-supported environments, where continuous analytical coordination, scalable information exchange and real-time assistance depend on integrated cooperation structures linking national law enforcement authorities with Europol's infrastructure. Future initiatives could also include enhanced support functions through the use of Europol tools and infrastructures, including mobile capabilities and technologically deployment environments operating under Europol's coordination.

The institutionalisation of research and innovation functions within Europol constitutes another critical dimension of this transformation. The expanding role of the Europol Innovation Lab, the

operationalisation of the EU Innovation Hub for Internal Security, and the development of controlled experimentation environments, such as the ODIN sandbox, demonstrate the emergence of institutionalised innovation governance structures within European law enforcement. Beyond technological experimentation, such environments also contribute to the testing, evaluation and future conformity assessment and certification procedures applicable to AI-supported tools intended for police use, particularly within interoperable environments where the deployment of AI-supported analytical systems depends on compliance, trustworthiness, reliability and cross-border governance compatibility under the evolving European AI framework.

Artificial intelligence occupies a vital position within this evolving technological model. Institutional documents increasingly frame AI not as a speculative potential capability, but as an essential response to the scale, complexity and operational velocity of contemporary policing environments.¹⁶ In practical terms, AI-supported analytical tools assist national authorities, for example, in identifying links between criminal networks, prioritising investigative leads, detecting suspicious financial or communication patterns and processing large volumes of digital evidence. Within this context, AI-enabled analytical support appears as an infrastructural enabler of coordination rather than as an isolated technological tool.

Importantly, however, this transformation should not be understood as the emergence of a federal European police authority. Despite the increasing operationalisation of Europol and the growing centrality of analytical infrastructures, the constitutional architecture of European policing remains formally decentralised. Member States continue to retain control over coercive powers, enforcement authority and core police competences. The evolving Europol model, therefore, appears characterised less by supranational federalisation than by the gradual construction of a federated analytical infrastructure designed to support intelligence-led information analysis and exchange across distributed European internal security ecosystems.

¹⁴ *ibid.*

¹⁵ Europol Programming Document 2026–2028.

¹⁶ Europol, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement* (Publications Office of the European Union 2024).

Europol's institutional evolution increasingly reflects a broader transition from reactive information exchange toward continuous AI-enabled coordination embedded within interoperable European internal security infrastructures. The integration of analytical platforms, AI-supported tools, interoperable information systems and real-time coordination mechanisms transforms Europol from a primarily support-oriented agency into a technologically enabled infrastructure supporting intelligence-led European law enforcement.

II. Interoperability, Large-Scale Data Ecosystems and AI Governance

The transformation of Europol cannot be considered solely through the expansion of its institutional mandate or the growing sophistication of its coordination and assistance mechanisms. At the centre of the emerging reform trajectory lies a deeper transformation concerning the role of data, interoperability and analytical infrastructures within European law enforcement governance.

One of the clearest manifestations of this shift is the growing institutional centrality of large and complex datasets within Europol's model. Recent evaluations, implementation appraisals, and strategic documents repeatedly emphasise the necessity of processing extensive, often initially unstructured datasets, particularly because contemporary cross-border investigations increasingly involve fragmented digital evidence, encrypted communications, platform-based criminal activity and large volumes of operational data whose relevance may not be immediately identifiable at the point of collection.¹⁷

Within this evolving governance architecture, artificial intelligence increasingly functions as a structural enabler of analytical scalability, interoperable information exchange and large-scale criminal intelligence processing. Debates concerning interoperability, large-scale data ecosystems and governance overlap with broader discussions on the deployment, governance and supervision of AI-

supported law enforcement infrastructures within the European Union.

The importance of exploratory and inferential analytical processing is particularly clear in this transformation. Europol's evolving model depends on the ability to identify patterns and correlations within datasets whose relevance may not initially be apparent at the point of collection. Debates surrounding data subject categorisation, unspecified data and pre-analysis mechanisms demonstrate the extent to which the logic of contemporary policing is shifting away from narrowly targeted investigative processing toward broader analytical environments capable of supporting intelligence-led coordination.¹⁸

Interoperability constitutes a core component of this evolving governance architecture. Within Europol, interoperability refers not merely to technical connectivity between databases and information systems, but also to the capacity to enable continuous analytical coordination, secure information exchange, and integrated cross-border law enforcement cooperation across distributed European internal security infrastructures, connecting systems such as SIENA, analytical platforms, and cross-border criminal intelligence environments. Institutional discussions, therefore, present interoperability not simply as a technical enhancement that facilitates more efficient data exchange, but as the organisational principle that enables continuity across fragmented European police environments.¹⁹

The growing emphasis on interoperability, large-scale analytical coordination, and AI-supported environments intensifies the strategic importance of setting up secure European police cloud infrastructures within the Europol ecosystem. Such infrastructures are increasingly relevant within the broader framework of the Union's strategic autonomy objectives. Given Europol's mandate and the sensitive nature of the data processed within European law enforcement cooperation environments, the establishment of secure Union-

¹⁷ Europol, *Consolidated Annual Activity Report 2024* (Publications Office of the European Union 2025); Europol, *European Union Serious and Organised Crime Threat Assessment 2025: The Changing DNA of Serious and Organised Crime* (Publications Office of the European Union 2025); Europol, *The Evolving Threat Landscape: How Encryption, Proxies and AI are Expanding Cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026* (Publications Office of the European Union 2026).

¹⁸ European Data Protection Supervisor (EDPS), *Decision on the Retention by Europol of Datasets Lacking Data Subject Categorisation (Cases 2019-0370 & 2021-0699)* (21 December 2021); Exchange of views within JHA working parties on operational cooperation and internal security.

¹⁹ Exchange of views within the JHA Council and relevant working parties on operational cooperation, law enforcement and interoperability.

based analytical and cloud infrastructures has become a prominent governance priority.

From an operational perspective, such infrastructures could facilitate scalable analytical processing, real-time cross-border coordination, secure information exchange, and the development of AI-supported analytical tools across interoperable European law enforcement environments. They also contribute to reducing dependence on external technological infrastructures, particularly non-EU clouds and digital service providers, while strengthening cybersecurity, data resilience and technological sovereignty within the broader European internal security architecture. This objective is especially significant given the sensitive nature of law enforcement data, the strategic importance of secure infrastructures and broader Union concerns regarding technological dependence in critical domains.

Simultaneously, the rising reliance on interoperable analytical ecosystems increases the importance of standardisation within European law enforcement cooperation. In this context, standardisation is becoming relevant not only for technical interoperability and secure information exchange, but also for the governance and lifecycle oversight of AI-supported systems. This could include, for example, the evolution of common standards concerning AI system documentation, audit logs, interoperability protocols, secure data-sharing procedures and conformity assessment requirements applicable to AI-supported law enforcement tools operating across multiple jurisdictions. The development of common operational and governance standards could accelerate greater compatibility among national law enforcement infrastructures, ensure compliance with evolving Union regulatory requirements, and contribute to a more coherent deployment of AI-enabled police capabilities in the European law enforcement ecosystem.

Artificial intelligence is progressively embedded within this emerging environment as an infrastructural enabler of analytical scalability and coordination. Institutional references to AI-assisted filtering, analytical prioritisation, real-time

assistance and scalable analytical processing all point toward a governance model in which AI operates as a structural enabler of continuity across distributed security infrastructures.²⁰

The establishment of internal governance structures designed to align AI experimentation with European AI governance requirements illustrates this evolution. The creation of the AI Alignment Committee and repeated references to compliance with the AI Act demonstrate that Europol considers AI governance not merely a technical or operational issue, but an institutional challenge requiring dedicated oversight, accountability and compliance mechanisms.²¹

Beyond coordination and analytical support, the future institutional evolution of Europol may also justify consideration of a more integrated innovation and technology governance structure within the Agency itself. The progressive expansion of the Europol Innovation Lab, combined with the growing importance of artificial intelligence and technological experimentation, is accelerating the potential establishment of a broader Europol Innovation and Technology Foresight Centre that integrates existing innovation structures with AI Lab and Technology Foresight components.²²

From a forward-looking institutional perspective, such a structure could amplify the research, development, testing and governance of technological tools relevant to European law enforcement authorities, including AI-supported capabilities, analytical instruments, digital forensic technologies, decryption tools and secure interoperability solutions. An integrated innovation and technology governance structure could also bolster the dissemination of investigative tools and technological solutions to Member States law enforcement authorities through mechanisms similar to the Europol Tools Repository, in conjunction with strengthening capacities to identify and mitigate malicious uses of emerging technologies.

Building upon the progressive institutionalisation of innovation governance, AI experimentation environments, interoperability frameworks and analytical infrastructures within Europol, such

²⁰ Europol, *AI and Policing*.

²¹ Europol, *Programming Document 2026–2028*.

²² Council of the European Union, 'Justice and Home Affairs Council, 7–8 October 2019' (Council of the European Union, 8 October 2019)

<https://www.consilium.europa.eu/en/meetings/jha/2019/10/07-08/>

("Ministers expressed their overall support for the creation of an innovation lab at Europol which could act as a monitor of new technological developments and drive innovation").

future-oriented developments no longer appear entirely speculative within the broader trajectory of European internal security governance transformation. Concurrently, a dedicated technology foresight function could monitor new and emerging technologies, such as generative AI systems, autonomous drone technologies, and advanced biometric analytical tools; the evolution of existing technological ecosystems; and assess their implications for European law enforcement. This could include identifying potential opportunities, technological benefits and innovation pathways, while simultaneously assessing emerging risks, vulnerabilities and forms of malicious technological use associated with evolving criminal ecosystems. Europol's future role, therefore, progressively extends beyond operational assistance toward becoming a central infrastructure for technological coordination, innovation governance and technology foresight within the broader European internal security architecture. Notably, this trajectory would remain compatible with the decentralised constitutional structure of European policing, insofar as technological development and support would continue to be distinguished from autonomous coercive authority. The operational integration of AI within Europol's activities also requires significant reinforcement of specialised human resources dedicated not only to the technical development and deployment of AI systems, but also to ensuring compliance with the evolving European regulatory framework throughout the entire lifecycle of AI systems. In this respect, effective compliance with the AI Act depends on the availability of specialised personnel capable of combining operational understanding, technological literacy, and legal and regulatory expertise. Particularly meaningful is the recruitment or secondment of personnel originating from the law enforcement community itself, as such expertise will enable a more informed understanding of both the capabilities and the practical implications of AI-supported tools within policing environments. The future governance of AI within Europol therefore relies not only on technological infrastructures and analytical capabilities, but also on institutional compliance capacities and specialised human oversight structures capable of supporting legally compliant and operationally responsible AI deployment.

An additional issue that warrants future consideration is the possible inclusion of AI-enabled crimes in the catalogue of criminal offences within Europol's competence. The increasing use of AI in organised crime, cybercrime, fraud, identity manipulation, and the automated facilitation of criminal activities challenges traditional offence classifications that are based primarily on the underlying criminal conduct rather than the enabling technological infrastructure. Although AI-enabled criminality does not presently constitute an autonomous category within the Europol mandate, the expanding role of AI-supported criminal ecosystems justifies reflection at the Union level regarding whether certain forms of AI-enabled crime should eventually receive more explicit recognition within the Agency's competence field. Such an initiative would nevertheless require careful legal delimitation to avoid excessively broad or technologically indeterminate expansion of competence, particularly given the rapid evolution and heterogeneous nature of AI-supported criminal practices.

III. Europol, Eurojust and the Emergence of Integrated European Security Governance

The transformation of Europol progressively extends beyond the narrow sphere of police cooperation. This institutional evolution is particularly visible in environments that depend on AI-supported analytical coordination, large-scale digital evidence management, and interoperable cross-border investigative ecosystems. As operational analytics, interoperability frameworks, and large-scale data ecosystems become embedded within European internal security governance, the traditional institutional separation between policing and judicial cooperation becomes difficult to maintain in practice.

Recent institutional documents and intergovernmental discussions describe Europol and Eurojust as complementary components of a broader internal security ecosystem rather than as isolated cooperation bodies operating within

parallel institutional structures.²³ The Joint Europol–Eurojust Annual Report 2024 is far-reaching because it outlines how synergies between Europol and Eurojust are gradually extending beyond traditional collaboration mechanisms toward more integrated ecosystems combining analytical support, judicial cooperation, digital evidence, and interoperable cross-border investigative environments. The fact that the Commission is expected to present parallel reform proposals for both Europol and Eurojust illustrates the extent to which police and judicial cooperation are increasingly conceived as interconnected dimensions of European law enforcement governance.

Operational Task Forces function as infrastructures for continuous analytical coordination across multiple jurisdictions and institutional actors. Unlike traditional case-based operational mechanisms, these structures facilitate continuous cooperation and the exchange of criminal intelligence across multiple jurisdictions in real time. Likewise, the growing integration of operational analytics, electronic evidence, and real-time information exchange introduces another mechanism: Joint Investigation Teams within broader analytical ecosystems supported by interoperable infrastructures.²⁴

Electronic evidence governance assumes particular relevance within this evolving architecture. Mechanisms such as SIRIUS increasingly facilitate cross-border access to electronic evidence, including subscriber information, communication metadata and digital account information held by online service providers and digital communication platforms.²⁵ In practice, such mechanisms assist national law enforcement and judicial authorities in identifying applicable legal procedures, coordinating requests for electronic evidence and navigating the complex environment surrounding digital investigations involving multiple jurisdictions and private technology actors. Their magnitude demonstrates that contemporary European security governance relies on integrated digital cooperation infrastructures that connect policing, prosecutorial cooperation, and platform-based information access across transnational environments.

The evolving relationship between Europol and Eurojust also accelerates broader transformations in the role of criminal analytics within European law enforcement. Criminal intelligence meaningfully functions not merely as an investigative resource supporting individual criminal cases, but as the organisational logic through which interoperable coordination infrastructures are structured and maintained.

IV. Hybrid Threats, Drones and the Constitutional Boundaries of Europol

The transformation of Europol and the gradual emergence of integrated AI-enabled security ecosystems simultaneously generate prominent constitutional and governance challenges within the European Union’s decentralised law enforcement architecture. The reliance on interoperability frameworks, large-scale analytical processing, AI-supported coordination and technologically mediated security infrastructures creates tensions concerning data governance, proportionality, institutional accountability and competence boundaries in domains such as hybrid threats, drones and counter-drone technologies. In this respect, the evolving Europol architecture reveals the structural difficulties associated with reconciling operational integration and scalable analytical governance with the decentralised structure of European policing authority.

Therefore, the resulting equilibrium is characterised by centralisation without constitutional federalisation. An emerging Europol model does not appear designed to establish a supranational police authority exercising autonomous enforcement powers across the Union. Instead, it resembles a federated analytical infrastructure intended to support intelligence-led information analysis and exchange across distributed national law enforcement systems.

Data governance and analytical processing are the most far-reaching governance tensions generated by this transformation. Contemporary environments depend on the large-scale processing of

²³ Europol and Eurojust, *Joint Europol–Eurojust Annual Report 2024*; Exchange of views within relevant preparatory bodies of the EU Council.

²⁴ JIJs Network, *Joint Investigation Teams: Practical Guide* (Publications Office of the European Union 2021).

²⁵ Europol, Eurojust and the European Judicial Network, *SIRIUS EU Electronic Evidence Situation Report 2024* (Publications Office of the European Union 2024).

heterogeneous datasets, often initially unstructured, originating from multiple national authorities, digital platforms, and cross-border information ecosystems.

Dedicated AI governance structures within Europol are particularly pivotal in this respect, as they present how AI governance is evolving from a purely technical or operational issue into a broader institutional and constitutional dimension of European internal security governance.²⁶

The integration of AI-supported analytical ecosystems and emerging technologies also expands Europol's relevance within a broader European internal and external security nexus, including those linking to hybrid threats, critical infrastructure protection and technologically enabled security risks. Growing concern about hybrid threats in European security discussions, driven by the current geopolitical landscape, has raised questions about the extent to which Europol should engage in countering hybrid activities. Nevertheless, hybrid threats remain conceptually and legally difficult to incorporate into the existing Europol mandate. No common Union definition of hybrid threats currently exists, while the phenomenon itself encompasses highly heterogeneous forms of conduct ranging from cyber operations and disinformation campaigns to espionage, sabotage, foreign interference and critical infrastructure disruption. In addition, Member States often diverge in the criminal law qualification and operational treatment of such activities. Hybrid threats are also closely associated with national security, an area which remains within the exclusive responsibility of Member States under Article 4(2) TEU.²⁷

Against this background, the explicit inclusion of "hybrid threats" as an autonomous category within the list of criminal offences falling under Europol's competence does not presently appear legally or institutionally advisable.²⁸ Existing legal bases already permit involvement where hybrid activities materialise through criminal offences currently falling within Europol's mission, including terrorism-related offences or participation in criminal networks. A more institutionally coherent approach, therefore, consists of strengthening Europol's role

from a strategic rather than operational perspective. Notably, Europol could contribute through strategic threat assessments, intelligence support and analytical reporting concerning hybrid activities involving criminal elements, while avoiding direct involvement in areas closely connected to national security competences.

A partially different governance challenge concerns the growing relevance of drones and counter-drone technologies within the broader European security architecture. Drone-related security risks are linked with the protection of critical infrastructure, public spaces and the external borders of the European Union.²⁹ However, these trends also demonstrate the fragmentation and functional overlap characterising the governance of emerging security technologies across the justice and home affairs area. Within this landscape, Europol's role appears more limited than that of Frontex. Unlike Europol, Frontex possesses field-operational capabilities enabling it to support Member State authorities directly in the testing, deployment and on-the-ground use of drones and counter-drone technologies at the external borders and in critical operational environments. The evolving governance framework concerning drones, therefore, indicates how emerging security technologies progressively blur traditional institutional boundaries between border management and law enforcement, while simultaneously intensifying differentiated roles among Justice and Home Affairs agencies.

This broader institutional trajectory was reflected in the political guidance provided by the Justice and Home Affairs Council on 5 March 2026 concerning the future reform of Europol. Ministers supported strengthening Europol's role as a central hub for the exchange and analysis of information, including through the use of new technologies, while also reinforcing interoperability and synergies with other Union agencies and bodies. At the same time, many Member States expressed reservations about expanding Europol's mandate into additional crime areas and favoured maintaining the Agency's current competence scope. The Council additionally emphasised that Europol's governance model could be amplified without the creation of new

²⁶ Such as the AI Alignment Committee.

²⁷ Consolidated Version of the Treaty on European Union [2016] OJ C 202/13, art 4(2).

²⁸ As reflected in the debates during the preparatory phase of the revision of the Europol Regulation.

²⁹ European Commission, *Communication from the Commission to the European Parliament and the Council: Action Plan on Drone and Counter Drone Security* COM(2026) 81 final, 11 February 2026.

institutional structures.³⁰ These guidelines are particularly outstanding because they confirm the broader institutional direction of the reform process: strengthening operational integration, analytical coordination and technological capabilities while simultaneously preserving the decentralised constitutional structure of European law enforcement.

Conclusion

Recent discussions surrounding the forthcoming reform of Europol reflect a broader transformation of the European Union's internal security governance. The evolving Europol architecture demonstrates that the future of Europol lies not in the creation of a supranational police authority exercising autonomous coercive powers in the European Union, but in the gradual institutionalisation of integrated analytical and cross-border ecosystems designed to support intelligence-led information analysis and exchange across distributed national law enforcement systems.

Within this emerging architecture, artificial intelligence occupies a structural rather than merely technological role. AI is progressively embedded within operational reality, enabling analytical scalability, real-time information exchange, and interoperable governance in data-intensive security environments.

In parallel, the Europol reform process indicates that the operational integration of European policing continues to unfold within a constitutionally decentralised legal order. The emerging Europol model, therefore, is characterised by centralisation and analytical integration without a corresponding constitutional federalisation of policing powers within the Union.

Perhaps most significantly, the future Europol architecture would highlight the emergence of integrated operational-judicial governance ecosystems linking criminal intelligence analysis, electronic evidence, cross-border prosecutorial cooperation and interoperable platform-based infrastructures. The growing convergence among Europol, Eurojust, and broader European internal

security mechanisms suggests that contemporary law enforcement governance cannot be considered solely through rigid distinctions between criminal intelligence, policing, and judicial cooperation.

The Europol reform process illustrates how the European Union is attempting to reconcile AI-enabled operational integration with constitutional pluralism and decentralised sovereignty that continue to define the area of freedom, security and justice. What is ultimately at stake, therefore, is not merely the future mandate of Europol, but the constitutional form through which AI-enabled European internal security governance will evolve within the European Union. Against this background, the dynamics of Europol appear linked not only to coordination and assistance capacities, but also to the Union's ability to invest in interoperable, trustworthy and legally governable AI-enabled law enforcement infrastructures.

³⁰ Council of the European Union, 'Justice and Home Affairs Council, 5 March 2026' (Council of the European Union, 5 March 2026) <https://www.consilium.europa.eu/en/meetings/jha/2026/03/05/>