

Europol's horizons between European cooperation, procedural sovereignty and the risk of evidence without a territory

Sergio Bianchi, *Director of the Agenfor International Foundation*

Andrea Cumini, *former investigator with the Central Operations Service (SCO), Italian Ministry of the Interior*

Leonardo Lavarini, *Industrial Engineering Technician, System Engineer, AI Systems and Infrastructure Developer*

ABSTRACT

Europol's transformation from an information-exchange centre into a European infrastructure for analysis, cloud services and public-private cooperation accentuates a structural tension. The Union may organise police cooperation and the circulation of information, while the exercise of coercive powers and the safeguards governing the gathering of evidence remain entrusted to the Member States; the police function also remains distinct from the intelligence function. This article reconstructs the conflict that emerged from the EDPS's 2019 inquiry into large datasets, the 2022 reform, the litigation concerning EncroChat, Sky ECC, ANOM and Matrix, and proposal COM(2026) 580. It argues that the risk does not depend solely on the physical location of servers, but on the loss of functional control over investigative and pre-investigative data: legal basis, controllership, purpose, segregation, keys, logs, chain of custody and defence access. Two case studies, Seity and CIRA4PREV, are then used to assess possible alternative architectures, without attributing to technology the ability to cure deficiencies in authorisation, proportionality or adversarial process.

Parole chiave

Europol; digital evidence; interception; sovereign cloud; confidentiality of investigations; EncroChat; artificial intelligence; intelligence.

1. Security and investigations between national and European law

Internal security is an area of intertwined, but not undifferentiated, competences. The Union seeks to ensure a high level of security through prevention, coordination and police and judicial cooperation, and may regulate the collection, storage, processing, analysis and exchange of information. Responsibility for public order, however, remains with the States and national security remains their exclusive responsibility. Article 88(3) TFEU also reserves the application of coercive measures to national authorities: Europol supports and coordinates, but may not independently order searches, seizures or interceptions.^[1]

This allocation creates two legal frameworks. The Europol Regulation determines who may process data within the Agency's ecosystem, for which tasks and subject to which controls. The procedural law of the competent State instead determines the conditions, authorities, manner of execution and admissibility/use of the investigative measure. Directive 2014/41/EU on the European Investigation Order (EIO) links the two frameworks through mutual recognition, but does not turn Europol into a judicial authority or introduce a general European rule on the admissibility of evidence.^[2]

A methodological criterion follows: the lawfulness of processing at Europol does not cure an unlawful national acquisition; conversely, evidence usable under the *lex fori* may still raise issues of data protection, accountability and effective oversight. The critical point arises when technical infrastructure precedes legal qualification. Copying a server, indexing metadata, analysing large datasets or submitting raw data to an artificial-intelligence model already constitute processing, even when described as mere pre-analysis.

2. The «big data challenge»

Over the last five years Europol has been subject to numerous reviews that brought legal and technical issues to light. Those issues are now resurfacing in the context of the proposed reform currently under discussion.

In 2019 the EDPS opened an own-initiative inquiry after Europol itself had reported the difficulty of reconciling large national data contributions with the categories of data subjects then permitted by law. The decision of 17 September 2020 found that the processing of large datasets, including those collected through OSINT, breached the limitations in Regulation (EU) 2016/794 and the principle of data minimisation. To distinguish suspects, contacts, victims and witnesses from persons with no established link to an offence, Europol first processed the entire dataset in its forensic environment.^[3]

[1] Article 4(2) TEU; Articles 67(3), 72, 87, 88(3) and 89 TFEU.

[2] Directive 2014/41/EU, in particular Articles 1, 6 and 14.

[3] EDPS, Decision on the own initiative inquiry on Europol's big data challenge, 17 September 2020, paras 1.1, 4.11 and 5.3-5.8.

The warning was followed by an action plan based on dataset labelling, access restrictions, periodic reviews and quality control. The EDPS considered it insufficient, particularly because no maximum time limit had been set; subsequent progress reports showed organisational improvements but did not resolve the problem of retaining uncategorised data.^[4] By decision of 21 December 2021, notified on 3 January 2022, the EDPS therefore ordered categorisation to be completed within six months for new contributions and within twelve months for legacy data, with deletion of data that remained non-compliant.^[5]

In the meantime, however, Regulation (EU) 2022/991 amended the applicable legal framework. It did not abolish the categorisation in Annex II, but added two exceptional regimes alongside the ordinary rule that could allow Europol not to comply with EDPS decisions. Article 18(6a) permits temporary processing of data received in order to establish whether they fall within the permitted categories, subject to functional separation and a maximum period of three years. Article 18a also permits the processing of investigative data that cannot be assigned to those categories where this is necessary and proportionate to support a specific criminal investigation requested by a Member State, the EPPO or Eurojust.^[6]

The ordinary rule retains two levels. For cross-checking under Article 18(2)(a), data concerning suspects or convicted persons and persons who, on the basis of factual indications, might commit criminal offences may be processed. For strategic or operational analysis and information exchange, witnesses, victims or potential victims, contacts and associates, and persons able to provide information may also be included.

The derogation in Article 18a remains linked to a specific investigation, must be documented and notified to the EDPS, and does not authorise indiscriminate reuse. The transitional provisions introduced in 2022, which allowed further processing of legacy holdings, were challenged by the EDPS on the ground that they retroactively neutralised the January 2022 order. At the preliminary stage, the General Court declared the action inadmissible without ruling on the substantive lawfulness of the new regime; appeal C-698/23 P is still pending and the Advocate General has nevertheless proposed that the order be set aside.^[7]

In parallel, journalistic investigations began into the so-called ‘parallel files’, describing the Computer Forensic Network as an environment with less robust safeguards than the ordinary information system and opening a new area of suspicion regarding Europol's activities. The verifiable

^[4] Europol, Action Plan following the EDPS Decision on Europol's big data challenge, 2020; EDPS, response to the action plan, D(2020) 2821; Europol, progress reports of March and October 2021.

^[5] EDPS, Decision on retention by Europol of datasets lacking Data Subject Categorisation, 21 December 2021, operative part, points 1-5; EDPS, The EDPS orders Europol to erase data concerning individuals with no established link to a criminal activity, 10 January 2022.

^[6] Regulation (EU) 2016/794, Article 18(5a) and (6a), and Article 18a, as amended by Regulation (EU) 2022/991; Annex II.

^[7] General Court of the European Union, order of 6 September 2023, EDPS v Parliament and Council, T-578/22; Opinion of Advocate General Campos Sánchez-Bordona, 8 May 2025, C-698/23 P. As at 25 August 2026, the case remains pending.

part of the criticism is, in fact, already contained in the EDPS records: multiple copies, prolonged retention, broad access and incomplete categorisation increased the risk that non-suspected persons would enter a European investigative memory that was difficult to know about and challenge. There is therefore no need to posit a clandestine database; it is enough to observe the gap between the declared purpose, the actual architecture and the capacity for reuse.^[8]

The external dimension broadens the problem. The 2018 working arrangement with Israel does not authorise the exchange of personal data, for which an international agreement is required. According to documents reconstructed by Statewatch in 2026, the subsequent negotiations prompted objections from the Council Legal Service concerning compatibility with international law and the negotiating mandate. Since this is a journalistic reconstruction, the attribution must remain explicit. The general legal issue is nonetheless clear: once sensitive data have been transferred, purpose, territorial limits, independent oversight and remedies must remain verifiable throughout the chain.^[9]

3. EncroChat, Sky ECC, ANOM and Matrix: transnational digital evidence

Data handling in police operations is also at the centre of a complex legal debate whose outcomes are not yet clearly defined.

Operations against major encrypted platforms have made visible the gap between technical acquisition and procedural control of evidence. In EncroChat, the French authorities, with Dutch assistance, deployed a tool within the service and obtained content, traffic data and location data; user data were then made available to national authorities through a Europol server. In M.N. (C-670/22), the Court of Justice held that a public prosecutor may issue an EIO for evidence already in the possession of the executing State if, in a comparable domestic case, that prosecutor is competent to request its transmission. The conditions governing the original interception need not be replicated in the issuing State, but subsequent judicial review of fundamental rights must be possible, something that becomes extremely complex, if not impossible, where such activities are carried out by intelligence agencies or by police forces that rely on secrecy concerning procedures and the systems used to access and exfiltrate data.^[10]

The Court also classified the infiltration of terminal devices aimed at collecting content, traffic and location data as an ‘interception of telecommunications’ for the purposes of the obligation to notify the State in whose territory the user is located, together with the necessary authorisation procedures. As regards the remedy, it did not impose a uniform European exclusionary rule: the

[8] EDPS, decisions of 17 September 2020 and 21 December 2021, cited above; G. Zandonini, Behind closed doors: Europol's opaque relations with tech companies, Statewatch, 30 October 2025.

[9] G. Zandonini, EU Commission still seeking controversial police agreement with Israel despite warnings, Statewatch, 30 July 2026; Working Arrangement establishing cooperative relations between Europol and the Israel Police, 2018.

[10] Court of Justice of the European Union (Grand Chamber), 30 April 2024, M.N. (EncroChat), C-670/22, ECLI:EU:C:2024:372, in particular paras 84-99 and 118-130.

national court must disregard the evidence where the accused is unable to comment on it effectively and it is liable to have a preponderant influence on the findings. This is a European minimum of fairness, not full harmonisation of the chain of custody.

National responses to this characteristically legal issue remain divergent. The German Federal Court of Justice (*Bundesgerichtshof, BGH*) admitted EncroChat data for serious offences, relying on German domestic rules governing the use of evidence obtained abroad. In Italy, the Joint Sections (*Sezioni Unite*) of the Italian Supreme Court of Cassation, judgments Nos 23755 and 23756 of 2024, excluded the application of Article 234-bis of the Italian Code of Criminal Procedure (*codice di procedura penale, c.p.p.*), treated circulation of the evidence under Articles 270 and 238 c.p.p., and considered an EIO issued by the public prosecutor sufficient for evidence already gathered abroad. Lack of access to the decryption algorithm does not, by itself, make the evidence unusable; judgment No 44047/2024 applied the same approach to Sky ECC.^[11]

The disagreement concerns primarily the degree of verifiability rather than automatic inadmissibility. The presumption that a foreign measure was lawfully carried out speeds up cooperation, but may turn the technical secrecy invoked by the executing State into an evidential black box, which may be framed as an infringement of defence rights. The European Court of Human Rights declared the applications in *A.L. and E.J. v. France* inadmissible because French law provided a remedy against acquisition and transfer; it did not thereby generally certify the reliability of the technique.^[12]

ANOM adds a further element: the platform was designed and distributed as part of an FBI operation and copied messages to a server located in an undisclosed third State. In 2025 the German Federal Court of Justice (BGH) admitted the US data for serious offences, and the German Federal Constitutional Court (*Bundesverfassungsgericht, BVerfG*) subsequently rejected a constitutional complaint. The cases of *Raal* and *Reudolph*, pending before the European Court of Human Rights, now raise the issue of defence access to the authorisation, integrity safeguards and filters applied.^[13]

Matrix, dismantled in December 2024 in an operation coordinated by Europol, Eurojust, France and the Netherlands, has not yet produced comparable European case-law. It is nevertheless a test for the future: when Europol infrastructure participates in real-time acquisition or analysis, the national court must be able to distinguish the original data, algorithmic transformations and the contribution of each actor.^[14]

[11] Italy: Supreme Court of Cassation, Joint Sections, 29 February–14 June 2024, Nos 23755 and 23756; Supreme Court of Cassation, Third Criminal Section, 26 September–3 December 2024, No 44047. Germany: Federal Court of Justice (BGH), 2 March 2022, 5 StR 457/21.

[12] European Court of Human Rights, *A.L. v France* and *E.J. v France*, inadmissibility decisions made public on 17 October 2024.

[13] Germany: Federal Court of Justice (BGH), 9 January 2025, 1 StR 54/24; Federal Constitutional Court (BVerfG), 23 September 2025, 2 BvR 625/25. European Court of Human Rights, *Raal v Estonia* and *Reudolph v Estonia*, applications Nos 14711/25 and 14712/25, communicated on 12 February 2026.

[14] Europol, International operation takes down another encrypted messaging service used by criminals, press release of 3 December 2024.

Finally, *BW v Europol and Eurojust* (T-1180/23), concerning *Sky ECC*, confirms the fragmentation of remedies. The General Court distinguished national processing operations from those attributable to the agencies and rejected automatic liability for the operation as a whole. The judgment has been appealed in Case C-399/26 P, which remains pending.^[15]

4. COM(2026) 580: public-private platform and Europol cloud

The European Union clearly needs greater transnational investigative capacity, albeit within the framework of Article 88(3) TFEU. The law currently governing Europol's activities remains Regulation (EU) 2016/794, as amended in 2022 and 2025. In June 2026, however, in response to the underlying need for greater investigative effectiveness, proposal COM(2026) 580 was tabled. It is not yet in force and aims to recast that framework and configure Europol as an information hub, operational hub and technology and innovation hub. It provides for a Europol Analytical Environment, a shared space for Joint Operational Analysis Cases and common cloud infrastructure. The terminology itself indicates that this new Europol profile moves more towards an intelligence-led model than traditional policing.^[16]

Article 47 codifies a permanent exchange mechanism also involving private parties, Europol and the Member States, comprising central infrastructure, web interfaces, interoperable APIs and secure channels. Article 96 governs the receipt, processing and forwarding of personal data. Europol could directly receive information that a private party states it is lawfully entitled to transmit and process it within the limits of Europol's mandate. In domestic exchanges concerning offences outside that mandate, Europol should remain a purely technical operator without access to the content.^[17]

Codification makes an already essential public-private relationship visible and identifies the channel, roles and reporting obligations. It does not, however, solve the upstream problem: a private party's declaration is not equivalent to verification of the relevant national legal basis and does not confer coercive powers on Europol. An efficient API can turn into routine an exchange that, in an individual proceeding, would have required an order from a judicial authority, time limits or a prohibition on bulk acquisition.

Article 50 establishes the Europol cloud as a platform for storage, processing, analysis and exchange, open in the cases provided for also to Union bodies and third countries. The proposal

[15] [1] General Court of the European Union, 25 February 2026, *BW v Europol and Eurojust* (*Sky ECC I*), T-1180/23, ECLI:EU:T:2026:149; appeal C-399/26 P, lodged on 24 April 2026 and pending as at 25 August 2026.

[16] European Commission, COM(2026) 580 final, 24 June 2026, in particular Articles 12, 40-42 and 50; Regulation (EU) 2016/794, as amended by Regulations (EU) 2022/991 and 2025/2611.

[17] COM(2026) 580, Articles 47, 91 and 96. The technical mechanism in Article 47 must be distinguished from the general basis for relations with private parties in Article 91 and from the conditions for exchange of personal data in Article 96.

requires access control, compartmentalisation, a law-enforcement digital identity and logging of operations, but leaves architecture, security and system-migration requirements to implementing acts. That referral is sensitive: choices capable of affecting confidentiality, jurisdiction and defence access risk being treated as merely technical specifications. The EDPS, which increasingly appears as a bulwark of legality in the balance between security requirements and rights, has also called for more predictable criteria of ‘relevance and necessity’, strict purpose and retention limits, clear rules on access and queries, and specific safeguards for data received from private parties and for cloud security.^[18]

5. ‘Hot’ data and cloud computing under Italian law: functional control

The first risk arising from Europol's expansion, which is not yet clearly defined, concerns data not linked to specific investigations; the second concerns the transnational processing of ‘hot data’, such as ongoing interceptions, streams from remote-access interception tools, operational logs and forensic copies that have not yet been stabilised. Finally, there is the issue of the compatibility of the intelligence-led model with different national legal systems.

Under the Italian legal system, intercepting communications is not the same as acquiring an already existing document. Article 268(3) of the Italian Code of Criminal Procedure (*codice di procedura penale*, c.p.p.) lays down, as a rule, the use of equipment installed at the public prosecutor's office, while allowing other solutions in the cases provided by law; for computer or telematic communications, paragraph 3-bis also permits privately owned equipment. Article 89 of the Implementing Provisions to the Italian Code of Criminal Procedure (*disposizioni di attuazione del c.p.p.*) nevertheless requires intercepted communications to be transferred to the equipment of the public prosecutor's office under constant integrity checks. Article 269 c.p.p. and Article 89-bis of those Implementing Provisions then establish the Digital Interception Archive under the direction and supervision of the public prosecutor.^[19]

Italian Decree-Law No 105/2023 provided for inter-district digital infrastructures, governed by the Italian Ministerial Decrees of 6 October 2023 and 5 January 2024. The centralised model does not, however, remove control from the public prosecutor's offices: it requires logical segregation by office, encryption, keys unavailable to system operators, strong authentication and tamper-proof logs. The arrangement shows that the decisive requirement is not the physical coincidence of server and courthouse, but the continued legal and technical control of the competent authority.^[20]

[18] COM(2026) 580, Articles 50 and 51; EDPS, Opinion 18/2026 on the proposal for a Regulation on Europol, 11 August 2026, in particular the observations concerning data of persons with no established link to criminal offences, access and queries, private parties and the security of the tools.

[19] Italian law: Articles 268(3) and (3-bis) and 269 of the Code of Criminal Procedure (*codice di procedura penale*, c.p.p.); Articles 89 and 89-bis of the Implementing Provisions to the c.p.p.; Ministerial Decree of 20 April 2018 on software used for interception by means of a remote-access interception tool (*captatore informatico*).

[20] Italian law: Decree-Law of 10 August 2023, No 105, converted with amendments by Law of 9 October 2023, No 137; Ministerial Decree of 6 October 2023; Ministerial Decree of 5 January 2024; Italian Data Protection Authority (Garante per la protezione dei dati personali), Opinion of 22 February 2024, web doc. No 9995724.

Three consequences follow. First, a generic commercial cloud service with telemetry, uncontrolled replication, subcontractors, reuse for training, or administrative access to data in clear text is incompatible with the regime governing raw interception data. Second, remote infrastructure may be used only if it is authorised, segregated and subject to the authority's functional control. Third, transferring a copy to Europol for analysis constitutes further processing distinct from the primary acquisition and requires a separate legal basis, specified purposes, necessity, marking of restrictions, chain of custody and the possibility of verification in judicial proceedings.

The relevant territoriality is therefore legal and functional. It must be possible to determine who is responsible for the investigation and controls keys and identities, who can order deletion and blocking, which court exercises oversight, which legal systems govern the provider, where backups and logs reside, and whether the defence can reproduce the transformation of the data. A general clause requiring compliance with national law is insufficient if the architecture makes it impossible in practice to exercise those safeguards.

6. Analytical tools, artificial intelligence and confidentiality of investigations

One of the major components in which the Europol reform invests is the Innovation Lab, that is, a 'service laboratory' available to national police forces. Public sources do not permit a complete inventory of the products used by the Europol Innovation Lab, but describe four families of capabilities: OSINT/SOCMINT automation; analysis of large datasets through scalable and cloud infrastructures; computer vision and biometrics; and experimental environments for artificial-intelligence models and systems. Those sources illustrate use cases and risks; they do not establish that every technology discussed is operational on real data. In fact, practical use of this 'laboratory' requires careful consideration of its legal consequences. For an Italian investigator, for example, who is bound by Italian criminal procedure and Italian rules on the confidentiality of investigations, handling interception data in a Europol cloud could present a challenge that is very difficult to overcome.^[21]

For investigative confidentiality, metadata as well as content are far from innocuous residues. The operator's account, the time and frequency of queries, case-file identifiers, IP addresses, target names, prompts, relationship graphs, errors and support tickets may reveal the subject, pace, sources and techniques of an investigation. In a cloud environment these traces propagate into logs, backups, observability systems and anti-fraud tools, often subject to retention and access rules different from those applying to the main content.

Article 329 of the Italian Code of Criminal Procedure (c.p.p.) protects investigative acts within the time limits laid down by Italian law; Articles 326 and 379-bis of the Italian Criminal Code (*codice*

[21] Europol Innovation Lab, AI and policing: the benefits and challenges of artificial intelligence for law enforcement, 2024, in particular pp. 12-22, 29-36 and 48-51; Europol, AI bias in law enforcement: a practical guide, 2024. The sources describe families of capabilities and risks, not a complete inventory of operational deployments.

penale, c.p.) protect, under different personal-scope requirements, official secrecy and secrecy relating to criminal proceedings. Italian Legislative Decree No 51/2018 requires specified purposes, minimisation, security and logging of operations for law-enforcement processing. Entrusting data to an authorised and necessary provider does not automatically constitute a breach; secondary use, unauthorised access or covert export may, however, amount to unlawful processing, a personal-data breach and, where the legal elements are met, criminally punishable disclosure.^[22]

Artificial intelligence adds three risks to this already problematic framework. The first is confidentiality: remote models and SaaS architectures can expose content and operational metadata. The second is epistemic: probabilistic systems can produce errors, spurious correlations or summaries that cannot be traced precisely to the source. The third is procedural: opacity in the model, prompt and transformations may prevent the defence from reproducing or challenging the result. Various Europol documents and the INTERPOL-UNICRI Toolkit therefore emphasise risk assessment, human oversight, traceability, audit, data protection and separation between fact, inference and confidence level, thereby raising a characteristic intelligence problem concerning the grading of sources and information.^[23]

There is no need to require every component to be deterministic; what is required is that the process by which it is used be sufficiently determinate to make the input, model version, configuration, output and human intervention reconstructable. Where Europol acts merely as a technical intermediary, it should not be able to reconstruct content or metadata beyond the minimum necessary. Where it receives a copy for its own tasks, it becomes controller of a further processing operation and must make the legal basis, purpose, retention, recipients and restrictions imposed by the State verifiable. Separation must be cryptographic and organisational, not merely declared in the interface.

7. The boundary between police cooperation and intelligence

The expansion of Europol's mandate is not merely a quantitative issue. The 2022 reform permits preliminary processing of large datasets, but links the derogation in Article 18a to a specific criminal investigation. COM(2026) 580, by contrast, accentuates the Agency's earlier intervention, integration with national systems and direct receipt of data, including from private parties. The question is when criminal analysis, although aimed at prevention, materially takes on the characteristics of intelligence, and when it instead remains within the sphere of criminal procedure.

Articles 87 and 88 TFEU include within police cooperation the collection, storage, analysis and circulation of information also needed for crime prevention. The shift towards intelligence appears, however, when autonomous initiative by the supranational body is combined with the

[22] Italian law: Article 329 of the Code of Criminal Procedure (c.p.p.); Articles 326 and 379-bis of the Criminal Code (codice penale, c.p.); Legislative Decree of 18 May 2018, No 51, with particular regard to purpose limitation, minimisation, security, logging of operations and the rules governing processors.

[23] Europol Innovation Lab, AI and policing, cited above, pp. 33-36 and 47-51; INTERPOL-UNICRI, Toolkit for Responsible AI Innovation in Law Enforcement: README File, revised edition, 2024, sections devoted to principles, risk assessment and the system life cycle.

absence of a specific offence or operational need, generalised collection of data on non-suspected persons, and the production of threat scenarios or operational priorities unrelated to an identified proceeding. These are all activities that private analysts or an intelligence agency may perform, but that do not fit easily within the Agency's mission.^[24]

This transformation encounters limits in EU primary law. Article 88 TFEU defines Europol as a supporting body and reserves coercive measures to the States; Article 4(2) TEU assigns national security to the sole responsibility of the Member States, while Article 72 TFEU preserves their responsibilities for public order and internal security. Europol's competence regarding hybrid threats is therefore lawful only insofar as it remains linked to criminal offences falling within the Agency's mandate.

National legal systems confirm that police and intelligence are not interchangeable functions. In Italy, the judicial police operate under Articles 55 et seq. of the Italian Code of Criminal Procedure (c.p.p.) and Article 109 of the Italian Constitution, while the DIS-AISE-AISI intelligence system operates under the direction of the President of the Council of Ministers; Article 23 of Italian Law No 124/2007 generally excludes judicial-police status for intelligence-service personnel. In France, the distinction is primarily functional, between the police judiciaire and services governed by the French Code de la sécurité intérieure. In Germany, the Trennungsgebot (separation principle) excludes police powers for the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz) and requires qualified statutory bases for data exchange. In Spain, the Policía Judicial is functionally dependent on judges and the public prosecutor, while the CNI operates for the Government and its intrusive measures are subject to special prior judicial control. In Greece, finally, the EYP performs national-security functions distinct from criminal investigation.^[25]

These barriers are not insurmountable in terms of communication: all legal systems provide for exchange and coordination. They remain binding, however, in terms of allocation of powers and safeguards. Exchange does not confer judicial-police powers on an intelligence service, nor does it allow the police to use intelligence methods outside the conditions governing them. Europol's intermediation cannot cure the original unlawfulness of data collection or automatically transform classified information into admissible evidence.

The Union already has intelligence capabilities, but not a single secret service. EU INTCEN, within the European External Action Service, produces strategic analysis on the basis of contributions from States, delegations and open or institutional sources. EUMS INT performs military analysis; the two structures cooperate within the Single Intelligence Analysis Capacity (SIAC). SatCen provides

[24] Articles 4(2) TEU and 72, 87 and 88 TFEU; Regulation (EU) 2016/794, Articles 4 and 18; COM(2026) 580, Articles 12 and 96.

[25] Italy: Articles 55 et seq. of the Code of Criminal Procedure (c.p.p.), Article 109 of the Italian Constitution, and Law of 3 August 2007, No 124, Article 23. France: Code de procédure pénale, Articles 12 et seq., and Code de la sécurité intérieure, Book VIII. Germany: Bundesverfassungsschutzgesetz, Section 8(3), and Federal Constitutional Court (BVerfG), 24 April 2013, 1 BvR 1215/07. Spain: Article 126 of the Spanish Constitution, Ley 11/2002 and Ley Orgánica 2/2002. Greece: Law 3649/2008 on the EYP and Greek rules on criminal investigation.

geospatial analysis, while Europol, Frontex and ENISA produce sector-specific analysis within their respective mandates. None of these structures is equivalent to a European agency endowed with the general collection powers of national intelligence services.^[26]

The 2024 Niinistö report highlighted the urgent need to better connect intelligence analysis and European decision-making and proposed developing, with the Member States, arrangements for a fully-fledged intelligence cooperation service at Union level, without duplicating the tasks of national services. That legitimate and important need does not, however, justify a surreptitious transformation of Europol. A genuine European service would require an appropriate legal basis, a definition of its relationship with Article 4(2) TEU, rules on intrusive powers, parliamentary and judicial oversight, data protection and democratic accountability.^[27]

8. Two case studies for technological continuity of safeguards

The following two cases are not presented as definitive products or already validated models. They are used to test in concrete terms whether alternative architectures can reduce some of the risk surfaces identified in the analysis: exfiltration and telemetry, loss of provenance, bulk collection and confusion between a pre-investigative indicator and evidence. The assessment concerns technical and organisational design; it does not replace empirical validation of effectiveness or the legal basis for processing.

8.1 Seity case study: local analysis and verifiability of output

In the project documentation cited by the authors, Seity is described as a prototype developed within the European PHYGITAL project for analysing investigative material using local models. The relevant element for this study is not computing power, but the choice to bring processing to where the data reside: an isolated environment, or one without connections to external providers, segregated document repositories and no telemetry to cloud services. This ‘localisation’ nevertheless permits interaction, through agentic architectures, with the rest of the investigative systems without transmitting or transferring data, except through ordinary police and judicial cooperation procedures.

The proposed architecture breaks the workflow into specialised components: audio transcription and diarisation, entity extraction, georeferencing on offline maps, timeline reconstruction, relationship graphs and RAG-assisted document search. Each output should refer back to its source document, paragraph or time marker. In procedural terms, the value of the design lies in the possibility of preserving a verifiable relationship between source, transformation and result, while keeping the operator as the decision-maker.^[28]

[26] European External Action Service, ‘Single Intelligence Analysis Capacity (SIAC) and its role in supporting EU decision making’, Impetus, Issue No 28, 2019, pp. 10–11; Council Decision 2014/401/CFSP of 26 June 2014 on the European Union Satellite Centre; Regulation (EU) 2016/794 on Europol; Regulation (EU) 2019/1896 on the European Border and Coast Guard; Regulation (EU) 2019/881 on ENISA.

[27] S. Niinistö, Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness, report presented to the President of the European Commission, 30 October 2024, pp. 22–23.

[28] The reconstruction of Seity is based on the project description provided by the authors in the manuscript. The assessment criteria are drawn from Europol Innovation Lab, AI and policing, cited above, and INTERPOL-UNICRI, Toolkit for Responsible AI Innovation in Law Enforcement, cited above. In the absence of an attached independent evaluation, the prototype’s performance is not treated as proven.

The case nevertheless has limitations that must be stated. Network isolation reduces the risk of exfiltration, but does not demonstrate accuracy, absence of bias or reproducibility. ‘Zero temperature’ does not make a generative model deterministic in an absolute sense; model versions, libraries, parameters and hardware must be fixed and recorded. Before evidential use, independent testing, task-specific error measurements, access management, append-only logs, output signatures and procedures distinguishing the analytical result from the original source are required. The prototype is therefore a case of security by architecture, not a presumption of reliability.

8.2 CIRA4PREV case study: cooperation without indiscriminate concentration of data

CIRA4PREV is used here as a design model for pre-investigative public-private cooperation. The starting problem is that platforms, banks, protection organisations, local authorities and OSINT analysts may observe weak signals before an investigation is opened, but bulk transfer of data to a central hub risks creating a repository concerning non-suspected persons. The model therefore proposes separating the indicator from the underlying data and, as far as possible, retaining controllership and responsibility with the entity that holds the data.^[29]

The workflow can be organised into five steps: lawful production of a structured indicator; recording provenance, the basis for collection, the category of data subject and the reliability level; minimisation or pseudonymisation before transmission; assessment by a public triage unit; and access to the full data only once the thresholds laid down by the applicable law are met. Indicators therefore trigger a check; they do not constitute a finding of guilt and do not automatically authorise a coercive measure.

The model's compatibility with Articles 47 and 96 of COM(2026) 580 depends on how it is implemented. A federated system, in which Europol receives minimised metadata or queries the data at the holder's premises, may reduce concentration. It can, however, also turn into distributed surveillance if queries are opaque, criteria are too broad, or private parties are in practice tasked with police activities. Protocols are therefore needed on authorised actors, lawful sources, data categories, retention, deletion, audit, independent oversight, victim protection and the transition from the pre-investigative level to the criminal case file.^[30]

Comparison of the two cases reveals two complementary strategies. Seity seeks to prevent investigative data from leaving the controlled environment; CIRA4PREV seeks to prevent pre-investigative data from being transferred before this is necessary. Neither architecture alone resolves issues of competence or admissibility. Both, however, make it possible to translate continuity of safeguards into verifiable design requirements, while leaving data handling and transfer to traditional models of police cooperation.

[29] S. Bianchi and N. Cea, Reframing European Common Operational Partnerships against THB and Migrant Smuggling. A public-private pre-investigative model inspired by FIU/AML cooperation, accountable OSINT and THB risk indicators, 2026, DOI 10.5281/zenodo.20376595, in particular paras 2, 3, 7, 9 and 11. CIRA4PREV is analysed here as a design model, not as an already validated system.

[30] Ibid., paras 7, 9 and 11; Eurojust, Genocide Network and Office of the Prosecutor of the International Criminal Court, Documenting International Crimes and Human Rights Violations for Criminal Accountability Purposes: Guidelines for Civil Society Organisations, 2022.

9. Conclusions

Proposal COM(2026) 580 has the merit of seeking to strengthen European security, make public-private cooperation visible and governable, and provide common infrastructure for European authorities. Its limitation, however, is the risk of equating the platform's technical security with the lawfulness of the exchange. The EDPS cases and the encrypted-phone cases show that infrastructure may be effective and produce evidential information while remaining weak in terms of categorisation, remedies, transparency and compliance with the *lex loci*.

The future rules should lay down in the Regulation itself, rather than referring them entirely to technical acts, at least the following: a prohibition on reuse and training on operational data; encryption with keys controlled by the contributing authority; segregation by proceeding and purpose; logs accessible to supervisory authorities and, within procedural limits, to the defence; a map of subcontractors and jurisdictions; differentiated retention of content and metadata; binding marking of national restrictions; export of a verifiable evidential package; the State's right to suspend or delete a workspace; and independent oversight of transfers to private parties and third countries.

The solution is not to set national sovereignty against European cooperation, but to build a verifiable continuity of safeguards. That continuity requires the legal territory of the evidence, the responsible authority, the purpose of processing and the competent court to remain identifiable throughout the chain. Only under those conditions can Europol become common infrastructure without becoming the place where evidence loses its author, control and capacity to be challenged.

Essential references

- European Commission, Proposal for a Regulation on the European Union Agency for Law Enforcement Cooperation (Europol), COM(2026) 580 final, 24 June 2026, CELEX 52026PC0580.
- EDPS, Decision on the own initiative inquiry on Europol's big data challenge, 17 September 2020.
- EDPS, Decision on retention by Europol of datasets lacking Data Subject Categorisation, 21 December 2021.
- EDPS, Opinion 18/2026 on the proposal for a Regulation on Europol, 11 August 2026.
- Europol Innovation Lab, AI and policing: the benefits and challenges of artificial intelligence for law enforcement, 2024.
- Europol, AI bias in law enforcement: a practical guide, 2024.
- INTERPOL-UNICRI, Toolkit for Responsible AI Innovation in Law Enforcement: README File, revised edition, 2024.
- S. Bianchi and N. Cea, Reframing European Common Operational Partnerships against THB and Migrant Smuggling, 2026, DOI 10.5281/zenodo.20376595.
- S. Niinistö, Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness, 2024.