



## Strengthening Governance, Ethics, and Reuse of Research AI Solutions for Investigations of Cyber-Enabled Crime

### KEY POINTS

- EU-funded AI tools for investigations of cyber-enabled crime face **not only technical limitations but also structural gaps in governance and coordination**.
- **Ethical and privacy trade-offs** (data minimisation vs data quality; bias vs operational effectiveness) are systemic and require explicit governance, not ad-hoc mitigation.
- A lack of **continuity, reuse, and accessibility of project results** significantly reduces policy and operational impact.
- Policy action is needed to shift from tool-centric innovation to **process-centric, accountable, and interoperable AI governance**.
- Strengthening governance frameworks can improve both **the protection of fundamental rights and investigative effectiveness**.

### CONTEXT AND POLICY RELEVANCE

Artificial intelligence (AI) is increasingly deployed to support **investigations into cyber-enabled and cyber-dependent crime**, including Malware-as-a-Service (MaaS), financial fraud, or the proliferation of child sexual abuse material (CSAM) and other illicit content. Over the last decade, EU-funded research and innovation programmes have developed a wide range of AI-based tools and proof-of-concept systems, operating under strict legal and ethical constraints, to assist law enforcement authorities (LEAs).

At the same time, the EU policy and regulatory landscape is undergoing **rapid transformations**, such as the entry into force of the e-Evidence Regulation (EU 2023/1543) in August 2026, or the mandatory reporting of actively exploited vulnerabilities on September 11, 2026. Other instruments, such as the AI Act, the GDPR, and the Law Enforcement Directive (LED), place **renewed emphasis on accountability, proportionality, transparency, and respect for fundamental rights in the use of AI for public-sector purposes**.

In this context, **policymakers** are increasingly confronted not with the question of *whether* AI should be used in law enforcement, but with **how to govern its use in practice** in ways that are accountable, interoperable, and aligned with fundamental rights.



These developments create both an opportunity and a challenge: while AI capabilities continue to evolve, institutional frameworks for their responsible and effective deployment often lag behind.

Insights emerging from recent multi-stakeholder exchanges between EU-funded projects in Madrid<sup>1</sup> in 2025 reveal a recurring pattern: **technical innovation is advancing faster than the procedural, organisational, and governance arrangements** needed to integrate AI systems into everyday investigative practice. Even when EU-funded tools demonstrate technical effectiveness, **their integration into real-world investigative environments** may require additional validation and formal authorisation processes. As a result, many promising tools remain confined to pilot phases, while **practitioners continue to rely on fragmented workflows or external commercial solutions**, which are considered “High-Risk” according to the AI Act and should undergo a formal **conformity assessment** and obtain CE Marking before operational deployment. As perpetrators' rapidly evolving modus operandi can render certain tools partially obsolete, **this policy brief highlights the need for adaptive governance frameworks** rather than one-off technological solutions to overcome the fragmentation of legal requirements and the need to integrate procedures, which have already been recognised in the Digital Omnibus<sup>2</sup> and in the BlueOLEx 2025<sup>3</sup>.

#### Policy focus:

How can EU policy better support the responsible, effective, and sustainable use of AI in digital investigations of cyber-enabled/dependent crime by strengthening governance, coordination, and the reuse of publicly funded results?

## KEY POLICY CHALLENGES

### Ethical trade-offs as structural conditions

AI-assisted investigations routinely involve tensions between competing normative and operational requirements. Examples include the balance between data minimisation obligations and the need for sufficiently rich datasets to ensure evidentiary quality, or between bias mitigation strategies and investigative effectiveness. These tensions are often treated as case-specific problems, rather than as structural features requiring systematic governance.

### Fragmentation of procedures and standards

Differences in legal interpretation, investigative workflows, documentation practices, and technical standards across Member States hinder interoperability and cross-border cooperation. This fragmentation limits the scalability of AI solutions developed within EU research initiatives and complicates their integration into operational environments.

### Dependence on non-EU tools and infrastructures

Despite sustained EU investment, LEAs frequently rely on commercial or non-EU tools for critical investigative functions. This raises concerns regarding digital sovereignty, long-term sustainability, auditability, and alignment with EU values and regulatory requirements.

### Limited reuse and institutional memory

EU-funded research initiatives generate extensive deliverables, datasets, methodologies, and lessons learned. However, these outputs are often difficult to discover, access, or reuse once projects end. The absence of systematic mechanisms for continuity leads to duplication of effort and underutilisation of publicly funded knowledge. In

<sup>1</sup> <https://preserveproject.eu/events/joint-international-stakeholder-workshop-what-an-inspiring-day-in-madrid/>

<sup>2</sup> <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>

<sup>3</sup> <https://www.enisa.europa.eu/news/blueolex-2025-testing-the-capabilities-of-eu-crisis-management-executives>

addition, operational constraints, staff turnover, and limited dedicated time for project activities may reduce sustained engagement of law enforcement partners, further weakening institutional memory and long-term reuse.

### Tool-centric evaluation of innovation

Innovation is frequently assessed primarily on technical performance. Less attention is paid to organisational uptake, training needs, documentation, human oversight arrangements, and accountability structures, even though these factors largely determine real-world impact.

## POLICY RECOMMENDATIONS

### Recommendation 1

#### Institutionalise governance of ethical trade-offs

EU policy should encourage the explicit identification, documentation, and governance of ethical and privacy trade-offs inherent in AI-assisted investigations. This includes integrating such trade-offs into operational guidelines, audit trails, and oversight mechanisms, rather than addressing them informally or retrospectively.

Particular attention should be paid to the legal frameworks governing the operations of law enforcement authorities. Even when EU-funded tools demonstrate technical effectiveness, their deployment may require additional certification, validation, and evidentiary safeguards before integration into operational environments. These constraints should be treated as structural conditions to be proactively managed, not as obstacles that emerge later.

**Expected impact:** Greater transparency, legal certainty, and smoother transition from research outputs to operational deployment, while preserving investigative effectiveness.

### Recommendation 2

#### Rebalance funding and evaluation criteria

Research and innovation funding schemes should place stronger emphasis on governance readiness, including documentation practices, accountability mechanisms, human-in-the-loop arrangements, and organisational integration. Technical performance should be assessed alongside these dimensions.

**Expected impact:** Improved deployability of AI solutions and stronger alignment with EU regulatory frameworks.

### Recommendation 3

#### Enable systematic reuse of EU-funded research results

The Commission should support mechanisms that facilitate the discoverability and reuse of EU-funded project outputs, such as shared repositories, standardised metadata, and AI-assisted search tools accessible to policymakers and practitioners.

Funding schemes should also incentivise sustained and meaningful participation by law enforcement partners throughout the project lifecycle, including dedicated time, clearly defined roles, and structured follow-up mechanisms beyond the formal project duration.

**Expected impact:** Increased return on public investment and faster uptake of evidence-based practices.

### Recommendation 4

#### Promote convergence of operational standards

Policy initiatives should support the gradual convergence of investigative workflows, documentation standards, and interoperability requirements across Member States, particularly for cross-border investigations of cyber-enabled crime. Harmonised validation and evidentiary standards would facilitate the lawful operational deployment of EU-funded AI tools and reduce

fragmentation that currently limits their scalability.

Given the rapidly evolving modus operandi of perpetrators, these standards should also include mechanisms for periodic review and adaptive validation to ensure that AI systems remain compliant, effective, and operationally relevant over time.

**Expected impact:** Strengthened EU-wide cooperation and reduced procedural friction.

### Recommendation 5

#### Support capacity building beyond technology

Capacity building measures should address not only technical skills but also ethical reasoning, governance literacy, and organisational change management related to AI deployment in law enforcement.

**Expected impact:** More resilient and responsible institutional adoption of AI systems.

#### Cross-cutting requirement: Lifecycle governance of AI systems

Across all recommendations, particular attention should be paid to lifecycle governance of AI systems. This includes ensuring the maintainability and retrainability of models, clear documentation of data provenance, reproducibility of results, and baseline standards of explainability. These elements are essential not only for compliance with emerging EU regulatory frameworks but also for evidentiary reliability, auditability, and long-term operational trust.

## EVIDENCE BASE AND LIMITATIONS

The analysis and recommendations presented in this brief draw on qualitative evidence from EU-funded research activities and structured exchanges among researchers, practitioners, and policy actors working on AI-supported investigations of cyber-enabled crime. Although the evidence base is not statistically representative, the convergence of findings across domains suggests that the identified challenges are systemic rather than sector-specific.

Further empirical research is needed to quantify impacts and assess national differences in implementation. Nevertheless, the consistency of the issues identified provides a sufficiently robust basis for policy-relevant recommendations.

## CONCLUDING REMARKS

EU-funded research has significantly advanced the technical capabilities available for AI-supported investigations of cyber-enabled crime. To translate these advances into durable policy and operational impact, greater attention must be paid to governance, coordination, and institutional integration.

A shift from a predominantly tool-centric perspective to a process- and governance-oriented approach can strengthen both the protection of fundamental rights and investigative effectiveness, aligning with evolving EU policy priorities.

#### Contact:

Dr Antonio Carnevale: [antonio.carnevale@uniba.it](mailto:antonio.carnevale@uniba.it)  
 Dr Sara Degli Esposti: [sara.degli.esposti@csic.es](mailto:sara.degli.esposti@csic.es)

#### Authors:

Dr Antonio Carnevale, UNIBA (PRESERVE); Dr Sara Degli-Esposti, CSIC (SAFEHORIZON); Susanne Siebald, Global Forum (PRESERVE); Ingrid Andersson, Global Forum (PRESERVE); Dr Carlos Cilleruelo Rodríguez, Byron Labs (ENSEMBLE); Claudia Calabrese, UNIBA (PRESERVE); Dr Santiago Macho González, Tree Technology (PRESERVE).