

ISSUE

08

July
2026

QUARTERLY NEWSLETTER
JEAN MONNET CENTRE OF EXCELLENCE
NEAPOLIS UNIVERSITY PAFOS

AI-2-TRACE-CRIME

Jean Monnet
Center of
Excellence

AI-2-TRACE-CRIME

The Jean Monnet Centre of Excellence AI-2-TRACE-CRIME, hosted by Neapolis University Pafos, is an interdisciplinary hub focused on advancing the responsible use of Artificial Intelligence (AI) in asset recovery, anti-money laundering (AML), and crime prevention. Led by Dr. Georgios Pavlidis, the Centre brings together experts from law, computer science, and international studies, supported by an Advisory Board of external experts.

This EU-funded initiative operates through three thematic streams. The first explores the development of legal frameworks for ethical and transparent AI use in AML and crime prevention, focusing on human rights, accountability, and data protection. The second investigates AI's technical dimensions, such as machine learning and natural language processing, to enhance tools for tracing illicit assets and detecting suspicious financial patterns. The third addresses AI's role in security, examining risks like AI-assisted cyberattacks and proposing strategies to counteract criminal misuse.



this issue

IOCTA 2026 Report **P.1**

Commission's guidelines **P.2**

TE-SAT 2026 Report **P.3**

Activities of our Center **P.4**

IOCTA 2026: AI, Anonymity and the Changing Economics of Cybercrime

Europol's Internet Organised Crime Threat Assessment (IOCTA) 2026 depicts a cybercrime landscape transformed not simply by new technologies, but by the speed, scalability and anonymity they provide. Its central warning is a widening "velocity gap": criminals are adopting technologies faster than law enforcement can adapt its investigative capabilities. AI, encryption, proxies and increasingly sophisticated criminal infrastructures are accelerating this shift.

Online fraud is identified as the fastest-growing area of organised crime. Investment fraud—particularly involving crypto-assets—business email compromise, romance fraud and attacks on payment systems increasingly operate through transnational, industrial-scale infrastructures. Generative AI is making social engineering more personalised and convincing, while Europol warns that agentic AI could increasingly automate elements of criminal workflows, allowing offenders to operate at greater scale with less direct human involvement.

The report also highlights how the financial infrastructure of cybercrime is evolving with cryptocurrencies remaining the preferred payment method for ransomware.

Ransomware remains a major threat, with Europol observing more than 120 active ransomware brands in 2025. At the same time, ransomware-as-a-service and the wider crime-as-a-service economy continue to lower barriers to entry. The boundaries between financially motivated cybercrime and hybrid threats are also becoming less distinct, as state-linked actors can draw upon criminal networks and services for disruptive operations.

Looking ahead, Europol anticipates increasingly autonomous forms of cybercrime in which agentic AI systems may execute entire criminal workflows with minimal human intervention. The response, it argues, requires law enforcement itself to harness innovative technologies, strengthen cross-border and private-sector cooperation, and secure lawful access to critical data.

For AI-2-TRACE-CRIME, the message is particularly significant: AI is simultaneously reshaping criminal capability and becoming essential to the investigative response. The challenge is not merely to regulate emerging technologies, but to ensure that enforcement, financial intelligence and asset-tracing capabilities can evolve at comparable speed.



Co-funded by
the European Union

Faster Financial Intelligence Across the EU

AMLA has finalised common standards to streamline cooperation between Financial Intelligence Units and reporting to the European Public Prosecutor's Office. The new machine-readable templates will standardise FIU and AMLA reporting, improve comparability and enable faster automated processing. A third set of templates will facilitate cross-border exchanges through FIU.net, including requests, spontaneous disclosures and feedback. The standards will apply progressively from July 2027, with full technical implementation by July 2028.



AI Act Transparency Rules Move from Principle to Practice

The European Commission has published new guidelines clarifying the transparency obligations that will apply to providers and deployers of certain AI systems from 2 August 2026.

As the EU AI Act enters a decisive phase of implementation, the European Commission has published new guidelines clarifying the transparency obligations that will apply to providers and deployers of certain AI systems from 2 August 2026. The objective is straightforward but increasingly important: people should be able to recognise when they are interacting with AI or encountering content that has been artificially generated or manipulated.

Under the new requirements, providers must design relevant AI systems—including interactive systems such as chatbots—to inform individuals when they are interacting with AI. Providers must also ensure that AI-generated or manipulated content can be identified through machine-readable marking.

Deployers face additional disclosure duties when using deepfakes, emotion-recognition or biometric-categorisation systems, as well as when publishing AI-generated content on matters of public interest without human review or editorial responsibility.

The guidelines translate these broad legal obligations into more practical terms. They clarify concepts such as “direct interaction”, synthetic content and deepfakes, while explaining relevant exceptions. Routine editing functions, such as spelling and grammar correction, for example, are distinguished from forms of AI-generated content that trigger transparency requirements.

The Commission has also linked the guidelines to the voluntary Code of Practice on Transparency of AI-generated Content, developed by independent experts with extensive stakeholder input.

Compliance with the Code can provide providers and deployers with a practical route for demonstrating conformity with the AI Act. Together with the AI Act Service Desk, these instruments form part of a broader effort to provide legal certainty as implementation accelerates.

The timing is significant. Most AI Act provisions, together with the enforcement powers of the Commission and national market-surveillance authorities, begin applying on 2 August 2026. Certain AI systems already on the market will have until 2 December 2026 to comply with marking and detection requirements.

The real test will be whether technical marking and disclosure mechanisms remain effective as generative AI itself continues to evolve.



Europol TE-SAT 2026: A More Complex Terrorism

Europol's EU Terrorism Situation and Trend Report (TE-SAT) 2026 highlights an increasingly complex threat environment. In 2025, EU Member States reported 45 completed, failed or foiled terrorist attacks and 486 terrorism-related arrests. Jihadist terrorism accounted for 24 attacks and 347 arrests, while right-wing, left-wing and anarchist threats also persisted.

A particularly significant development is the growing importance of the digital environment.

Online platforms facilitate radicalisation, recruitment and operational coordination, while ideological boundaries are becoming increasingly fluid, particularly among younger individuals exposed to overlapping extremist narratives.

Artificial intelligence adds another dimension. Europol reports the use of generative AI to produce propaganda, deepfakes and extremist content, while AI-powered bots and chatbots can support recruitment and amplify engagement.

The report also identifies diverse terrorist-financing methods, combining traditional mechanisms such as cash and hawala with cryptocurrencies and emerging digital value-transfer channels. Occasional intersections between terrorist actors and organised crime—including money laundering, weapons and drug trafficking—further underline the increasingly interconnected nature of Europe's security challenges.

EYE ON TECH Digital Euro: A New Frontier for AML/CFT?

The digital euro could reshape Europe's payments landscape—but also raise important questions for AML/CFT. As central bank money moves into digital form, greater traceability and standardised payment infrastructure could strengthen the detection of suspicious transactions and facilitate financial investigations. Yet these benefits must be balanced against privacy, data protection and proportionality.

The challenge lies in designing a system that preserves the digital euro's cash-like characteristics without creating blind spots for illicit finance. Offline payments and enhanced privacy features may require carefully calibrated safeguards, while intermediaries will remain central to customer due diligence and transaction monitoring.

Q&A | Financial Intelligence vs Privacy: How Much Data Is Enough?

Q: Does more data necessarily mean better financial intelligence?

A: Not always. Effective AML/CFT increasingly depends on connecting information across financial institutions, FIUs and public authorities. AMLA could strengthen this process by improving cooperation and information sharing across the EU. Yet accumulating more data does not automatically generate better intelligence.

Poor-quality, irrelevant or excessive information may obscure meaningful risks, produce false positives and intensify privacy concerns. The challenge is therefore not simply to collect more, but to use data intelligently and proportionately. Effective financial intelligence requires high-quality information, safeguards, purpose limitation and accountable tools—balancing the fight against financial crime with EU data-protection standards and fundamental rights.



Building Europe's Sovereign AI Infrastructure

The EU's new

Competitiveness

Coordination Tool (CCT)

aims to accelerate

strategic investment by

bringing together EU

institutions, Member

States and industry. A

flagship initiative is the

planned deployment of AI

GigaFactories: large-scale

facilities designed to train

and deploy advanced AI

models. The initiative

aims to mobilise €20

billion, combining EU,

national and European

Investment Bank support.

Interest has already been

substantial, with 77

expressions of interest

covering 60 sites across

16 Member States.

Research Spotlight: Recent Publications:

Research Spotlight highlights recent publications produced within the framework of the Jean Monnet Centre of Excellence AI-2-TRACE-CRIME, showcasing research on artificial intelligence, fundamental rights, digital surveillance, transnational crime and emerging challenges in European and international law.

The Fog of Information: The EU AI Act and Legal Strategies Against AI-Fuelled Disinformation

Eleni Gavril & Georgios Pavlidis, *European Journal of Privacy Law & Technologies*, Vol. 2025/2, pp. 1-12

Generative AI has dramatically increased the speed, scale and sophistication with which disinformation can be produced and disseminated. This article examines how the EU AI Act may contribute to addressing AI-driven disinformation, even though the legislation does not regulate the phenomenon directly. Particular attention is given to transparency obligations, risk-based regulation and rules concerning synthetic content and general-purpose AI. Situating the AI Act alongside the Digital Services Act, the Code of Practice on Disinformation and EU fundamental-rights law, the authors argue for a more integrated regulatory approach capable of strengthening democratic resilience without disproportionately restricting freedom of expression.

Algorithmic Administration and the EU AI Act: Legal Principles for Public Sector Use of AI

Ioannis Kastanas & Georgios Pavlidis, *Journal of Ethics and Legal Technologies*, Vol. 7, 2025, pp. 59–79.

This article explores the increasing use of artificial intelligence by public authorities and the challenges this creates for the administrative rule of law. Focusing on areas such as welfare benefits, migration, education and law enforcement, the authors examine how the EU AI Act interacts with fundamental administrative-law principles, including legality, transparency, proportionality, accountability and the duty to provide reasons. The study assesses whether the Act's safeguards for high-risk systems are sufficient to ensure meaningful human oversight and reviewability, and proposes interpretative approaches aimed at ensuring that algorithmic public administration remains both innovative and compatible with fundamental rights and procedural fairness.

