ISSUE
07
April
2026

QUARTERLY NEWSLETTER
JEAN MONNET CENTRE OF EXCELLENCE
NEAPOLIS UNIVERSITY PAFOS

AI-2-TRACE-CRIME

this issue

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.

Co-funded by the European Union

FATF Sharpens Its Focus on Digital Finance and Cyber-Enabled Fraud

At its February 2026 Plenary in Mexico City, the Financial Action Task Force (FATF) signalled an intensified focus on technology-driven financial crime and the rapidly changing landscape of illicit finance. Delegates from the FATF Global Network, encompassing more than 200 jurisdictions, discussed emerging threats.

Cyber-enabled fraud emerged as a major priority. The FATF approved new work examining how criminals exploit digital technologies to increase the scale, speed and sophistication of fraud. Importantly, the response is not framed solely in terms of tighter regulation: authorities and private-sector actors are also encouraged to harness technological innovation to detect suspicious activity, prevent fraud, recover victims' funds and identify perpetrators. The FATF has indicated that fraud will remain a key area of focus over the coming years.

The Plenary approved reports examining the risks posed by offshore virtual asset service providers (VASPs), particularly where regulatory and supervisory gaps can be exploited across borders, as well as emerging risks associated with stablecoins and unhosted wallets. The latter raises increasingly important questions about peer-to-peer transactions that may occur beyond traditional financial intermediaries.

The Plenary also adopted new-round mutual evaluation reports for Austria, Italy and Singapore. The revised methodology places greater emphasis on whether national AML/CFT systems actually deliver effective results, rather than focusing predominantly on formal compliance. Countries will also receive time-bound roadmaps identifying key actions to strengthen their defences against illicit finance.

Meanwhile, Kuwait and Papua New Guinea were added to the list of jurisdictions under increased monitoring, and the FATF advanced its strategic priorities for 2026–2028. The meeting also appointed Giles Thomson of the United Kingdom as the next FATF President, succeeding Elisa de Anda Madrazo in July 2026.

Together, these developments point to an AML/CFT agenda increasingly shaped by technological change—and by the challenge of ensuring that regulation and enforcement evolve as quickly as the financial ecosystem itself.

One AML Rulebook, but One AML System?

The EU’s new anti-money laundering framework marks a major step towards harmonisation through a single rulebook and the creation of AMLA. Yet common rules do not automatically produce uniform outcomes. Differences in national supervision, enforcement capacity, Financial Intelligence Units and institutional practices may continue to shape effectiveness. The real test will therefore be whether regulatory harmonisation can generate a genuinely integrated European AML system in practice.

ProtectEU

Europe Updates Its Counterterrorism Playbook for the Digital Age

In February 2026, the European Commission presented a new EU agenda to prevent and counter terrorism, a flagship initiative under the ProtectEU European Internal Security Strategy. The agenda responds to a threat environment increasingly shaped by digital technologies, online radicalisation and geopolitical instability, proposing action across six pillars: anticipating threats, preventing radicalisation, protecting people online and offline, responding to attacks, and strengthening international cooperation.

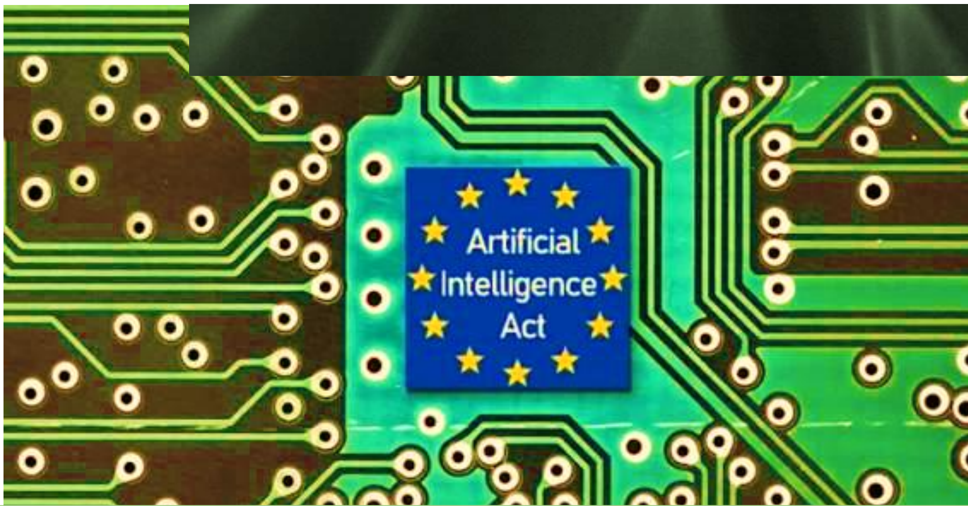
Technology is central to both the emerging risks and the proposed response. The Commission highlights the growing misuse of social media, artificial intelligence, crypto-assets, drones and 3D-printed weapons by terrorist and violent extremist actors. Particular concern surrounds the online targeting and radicalisation of minors. To improve early detection, the agenda proposes stronger EU-level intelligence analysis.

The online environment is another priority. The Commission will evaluate the Terrorist Content Online Regulation with a view to possible revision, strengthen enforcement of the Digital Services Act, and deepen cooperation with online platforms through the EU Internet Forum. It also plans to transform the existing EU Crisis Protocol into a broader Online Crisis Response Framework.

Financial dimensions feature prominently. The agenda calls for improved detection of terrorist financing involving cryptocurrencies and online payments, including through a future EU Financial Data Retrieval System. This reflects a wider shift toward connecting financial intelligence, digital evidence and cross-border law enforcement more effectively.

Other measures include €30 million to strengthen the security of public spaces, enhanced information-sharing through the Schengen Information System, possible expansion of travel-information frameworks beyond commercial aviation, and planned revisions of the mandates of Europol and Eurojust. International cooperation will also be reinforced.

The new agenda illustrates a broader transformation in EU policy: emerging technologies are increasingly understood not simply as tools exploited by threat actors, but also as essential instruments for prevention, intelligence and investigation. The challenge will be to translate this technology-driven approach into effective security measures while maintaining fundamental-rights safeguards and appropriate oversight.



From Rules to Reality: The AI Act Takes Shape

The seventh meeting of the EU AI Board, held on 20 March 2026 under the Cypriot Presidency of the Council, focused on the next phase of Europe's AI governance framework: turning regulatory ambitions into practice.

Discussions covered implementation of the AI Continent Action Plan and the Apply AI Strategy, including efforts to align national AI strategies and encourage sector-specific adoption of AI.

A key development was the presentation of the second draft of the Code of Practice on the labelling and marking of AI-generated content, revised following extensive input from industry, academia, civil society, Member States and the European Parliament.

The Board also reviewed progress on the implementation of the AI Act, including negotiations on the Digital Omnibus on AI, for which the Council had agreed its mandate on 13 March.

Members further exchanged good practices on national AI regulatory sandboxes.

The meeting illustrates how EU AI governance is moving from legislative design towards implementation, coordination and practical experimentation across Member States.

Q&A | Can AI Help Us Follow the Money?

Q: How can AI support the tracing of criminal assets?

A: AI can help investigators identify patterns that may be difficult to detect across large and fragmented datasets. Network analysis can reveal hidden relationships between individuals, companies and transactions; anomaly detection can flag unusual financial behaviour; and automated data matching can connect information across financial, corporate and property records.

Yet AI-assisted tracing also carries risks. Poor-quality data can produce misleading results, while opaque models and false positives may affect individuals unfairly or divert investigative resources. Effective use therefore requires human oversight, explainability, robust data governance and respect for fundamental rights. AI can strengthen asset tracing—but it should support, rather than replace, accountable investigative judgment.

EYE ON AI

One Year of Europe's AI Continent Ambition

One year after launching the AI Continent Action Plan, the European Commission reported progress across its five pillars: computing infrastructure, data, skills, AI adoption and regulatory simplification. Developments include 19 operational AI Factories, initiatives to attract AI talent, and up to €1 billion in calls supporting AI uptake across strategic sectors.

To mark the anniversary, the Commission published two reports examining AI adoption in public administration and the evolution of EU AI policymaking since 2018. The first proposes a framework for embedding AI within public-sector policies, capabilities and high-impact applications. The second traces Europe's broader effort to reconcile technological innovation and competitiveness with fundamental rights and public trust.

Together, the initiatives reflect the EU's growing emphasis on moving beyond AI regulation towards building the infrastructure, institutional capacity and conditions necessary for widespread and responsible AI adoption.

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.

From the AI Act to a European AI Agency: Completing the Union's Regulatory Architecture

Georgios Pavlidis, *Croatian Yearbook of European Law and Policy*, Vol. 21, 2025, pp. 125–143.

This article examines whether the EU's emerging artificial intelligence governance framework should evolve beyond the recently established AI Office towards a stronger, dedicated European AI Agency. While recognising the AI Act as a major step towards harmonised, risk-based regulation, the study argues that significant challenges remain in supervision, enforcement, standard-setting and cross-border coordination. A specialised supranational agency could strengthen regulatory coherence, enhance technical and risk-assessment capacity and provide the EU with a stronger institutional voice in global AI governance, while also supporting Europe's broader ambition to achieve greater digital and technological sovereignty.

Targeted Financial Sanctions and the Evolving European Union AML/CFT Framework: What's Changing and Why It Matters

Georgios Pavlidis, *Bratislava Law Review*, Vol. 9, No. 2, 2025, pp. 193–210.

This article analyses the growing integration of targeted financial sanctions into the EU's reformed anti-money laundering and counter-terrorist financing framework, particularly under AMLD6 and the new AML Regulation. It argues that this development represents more than a technical regulatory adjustment: sanctions are increasingly being transformed from predominantly foreign-policy instruments into structural preventive and compliance obligations for public authorities, financial institutions and other obliged entities. The study examines new risk-assessment, monitoring and enforcement mechanisms while highlighting continuing challenges involving sanctions evasion, institutional coordination, proportionality, legal certainty, resource disparities and the protection of fundamental rights.

Digital Markets Act Passes Its First Test

The European Commission's first review of the Digital Markets Act (DMA) concludes that, after two years of application, the framework remains fit for purpose and is helping make digital markets fairer and more contestable. The review points to greater user choice over browsers, search engines and personal-data use, alongside new opportunities for alternative app stores, messaging services and connected-device providers.

DISCLAIMER: *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.*

Co-funded by the European Union