ISSUE
06
January
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

EU-wide survey on usage of digital tools at work

A landmark EU-wide survey conducted by the Joint Research Centre (JRC) and the European Commission's Directorate-General for Employment has revealed that digitalisation is now embedded in almost every aspect of European work life. According to the 2024–2025 AIM-WORK survey, which gathered data from more than 70,000 workers across the 27 EU Member States, nine in ten employees rely on digital tools such as computers, mobile devices, and office software, while 30% use AI applications—particularly chatbots powered by large language models.

AI is most commonly employed for writing (65%) and translation (59%), followed by data processing and idea generation (38%), transcription (28%), image creation (27%), planning and scheduling (24%), and customer advice (19%). Adoption is highest in Northern and Central Europe and among office-based professions. Digital monitoring has become a key feature of contemporary workplaces, with 37% of EU workers monitored for their working hours and 36% for entry and exit times. Monitoring practices differ by sector: physical location tracking is prevalent in transport, construction, and manufacturing, while digital activity monitoring is common in finance, ICT, and public administration. Central and Eastern European countries report higher use of CCTV, internet tracking, and call monitoring.

Algorithmic management—automated systems that allocate tasks or evaluate performance—is emerging more gradually but with growing significance. The survey shows that 24% of workers have their schedules set automatically, while 13% are subject to automated performance assessments. Such systems are reshaping supervision and human resource management across Europe.

The JRC study also categorises workers according to their degree of "platformisation"—the extent to which digital tools, monitoring, and algorithmic management shape their work. It finds that 6% of workers remain untouched by these trends, 33% use digital tools without being monitored, 42% experience partial platformisation, 9% are subject to informational platformisation (data-driven monitoring and evaluation, typical in finance and insurance), 7% to physical platformisation (notably in transport and logistics), and 2% are fully platformised.

The report links full and physical platformisation to more negative conditions, including higher stress and reduced autonomy, whereas informational platformisation tends to have milder effects and often accompanies remote work.

Biometric Vulnerabilities and Future Law Enforcement Preparedness

Europol's 2025 Innovation Lab report, 'Biometric Vulnerabilities: Ensuring Future Law Enforcement Preparedness', analyses the growing importance of biometric technologies in modern policing and border security, while highlighting critical vulnerabilities that could compromise their reliability and security. As biometric systems—such as facial recognition, fingerprint, iris, and voice identification—become central to law enforcement operations and EU-wide information systems, ensuring their integrity is a strategic necessity.

For more information, click here

How the Digital Services Act (DSA) impacts our life

The DSA regulates online services such as social media, marketplaces, app stores, and online travel and accommodation services, for example, Shein, Instagram, X, TikTok, LinkedIn and Booking.com.

The Digital Services Act (DSA) is the European Union's comprehensive framework regulating online services such as social media platforms, marketplaces, app stores, and travel or accommodation services — including well-known platforms like Shein, Instagram, X, TikTok, LinkedIn, and Booking.com. Its core objective is to create a safer and more transparent digital environment where users' fundamental rights are fully protected.

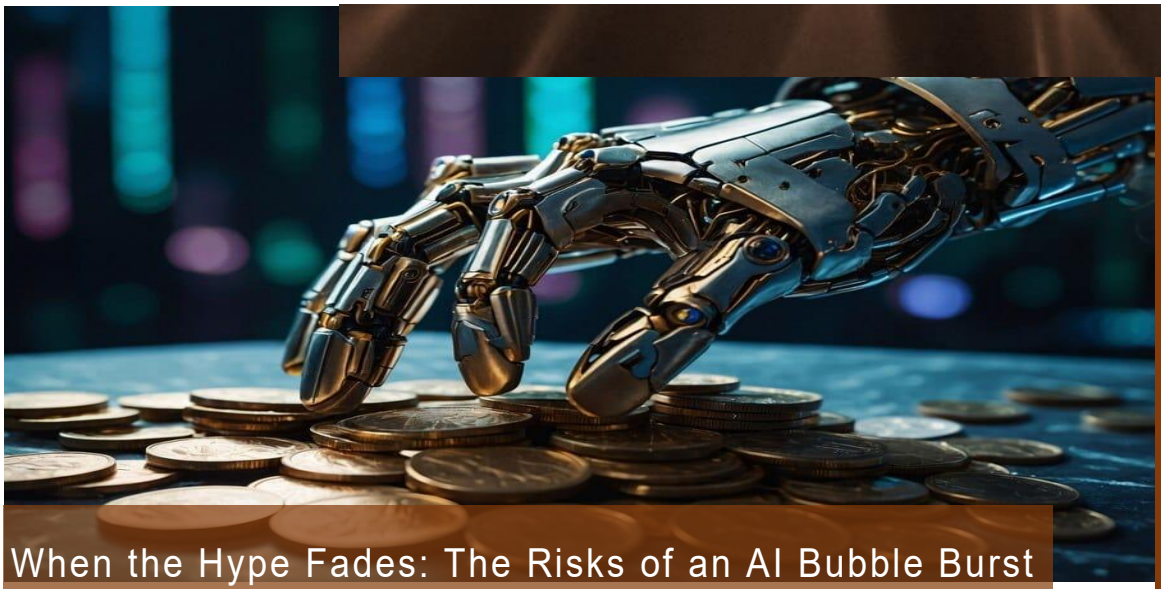
The DSA strengthens user control over online experiences. Platforms must clearly explain any removal or suspension of content or accounts and cannot restrict visibility without justification. Users who disagree with such actions have the right to appeal through the platform's internal system or independent out-of-court dispute settlement bodies.

Users can also flag illegal content, goods, or services through user-friendly mechanisms directly on platforms. Providers are obliged to inform users about the outcome of their reports and explain available appeal options. Furthermore, users of large online platforms with over 45 million EU users can now choose non-personalised feeds, allowing them to view content chronologically or by preference rather than algorithmic profiling. This enhances user autonomy and helps reduce exposure to manipulative or addictive content.

The DSA introduces strong advertising transparency obligations: all ads must be clearly labelled and include information on who placed them and why they are shown. Importantly, platforms are prohibited from using sensitive personal data—such as religion, race, or sexual orientation—for targeted advertising and completely banned from showing targeted ads to minors.

The Act outlaws dark patterns—deceptive design techniques that pressure users into unwanted decisions, such as making a large "accept" button more prominent than "decline." Platforms must ensure fair, visible, and accessible choices. Additionally, marketplaces must verify and display seller identities, ensuring users know exactly who they are buying from.

Enforcement of the DSA is shared between national authorities and the European Commission. It entered into force for very large online platforms (VLOPs) and search engines (VLOSEs) in August 2023 and has applied to all other platforms since February 2024, except micro and small enterprises. Each Member State has a Digital Services Coordinator responsible for local supervision and handling user complaints. The European Commission directly oversees large platforms, with powers to investigate suspected infringements, request information, conduct interviews, and inspect company premises.



When the Hype Fades: The Risks of an AI Bubble Burst

The rapid expansion of artificial intelligence has fuelled extraordinary optimism and investment, but it also carries the risk of an AI bubble—an unsustainable surge driven by speculation, exaggerated promises, and short-term returns. If this bubble bursts, the consequences could be severe for the global economy, innovation ecosystems, and public trust in technology.

Financially, overvalued AI startups and inflated market expectations could collapse once profitability proves elusive, echoing the dot-com crash. Venture capital might retreat abruptly, leaving genuine innovators without funding and resulting in widespread layoffs across the tech industry. Policymakers, who have tied digital strategies and public investments to AI growth, could face setbacks in national and EU digital agendas.

Beyond economics, a burst would damage confidence in AI itself. Public perception could shift from excitement to scepticism, slowing adoption even in high-value domains such as healthcare, environmental protection, and education. Universities and research institutions could experience cuts in funding, curtailing long-term exploration of ethical and trustworthy AI.

Q&A Quantum Tecnology and Law Enforrcement

Q: What are the implications of emerging quantum technologies for law enforcement and security?

Quantum computers will eventually be capable of breaking widely used public-key cryptographic algorithms This creates a long-term risk of “store-now, decrypt-later” attacks, where adversaries collect encrypted data today to decrypt it once quantum capability becomes available. Quantum computing may enhance complex pattern recognition, password recovery, and data decryption tasks in criminal investigations.

However, it may also enable adversaries to conceal traces or manipulate digital evidence more effectively Quantum sensors can detect minute environmental changes, improving forensic analysis (e.g., trace detection, imaging) and enhancing situational awareness during field operations.

Technologies based on quantum entanglement offer secure information transfer resistant to interception. Quantum networks could revolutionise cross-border data sharing and evidence transmission by ensuring authenticity and integrity.

EYE ON AML/CFT

Outcomes of the FATF 2025 Plenary

The fourth Plenary under the Mexican Presidency, held in Paris from 22 to 24 October 2025, reaffirmed the Financial Action Task Force’s (FATF) mission to deprive criminals of their illicit gains through stronger global coordination, asset recovery, and technological vigilance. Delegates from the FATF’s Global Network—representing over 200 jurisdictions—approved a series of significant measures that collectively reinforce the architecture of global AML/CFT.

Key outcomes included: the adoption of new asset recovery guidance strengthening confiscation and international cooperation; the mutual evaluation reports of Belgium and Malaysia, the first under the FATF’s new risk-based and time-bound methodology; the removal of Burkina Faso, Mozambique, Nigeria, and South Africa from increased monitoring following successful reforms; the endorsement of a Horizon Scan on Artificial Intelligence (AI) and deepfakes; and renewed emphasis on global cohesion through the FATF Guest Initiative.

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.

Data Governance, Quality, and Accountability: Unpacking Article 10 of the EU AI Act

Nikoletta Constantinou & Georgios Pavlidis, *Cyprus Law Review (KYNE)*, Vol. 3/2025, pp. 128–133.

This article examines Article 10 of the EU Artificial Intelligence Act and its requirements concerning data quality, governance and traceability for high-risk AI systems. The authors show that seemingly technical rules governing training, validation and testing data have a fundamentally rights-based dimension: biased, incomplete or poorly documented data can generate discriminatory and opaque outcomes. Situating Article 10 within the broader framework of the EU Charter of Fundamental Rights and the GDPR, the study highlights both its potential to strengthen responsible AI governance and the challenges surrounding interpretation, implementation and regulatory enforcement.

The Cost of Decryption: The ECHR's Warning Against Mass Surveillance in *Podchasov v. Russia*

Eirini Tsagkaraki & Georgios Pavlidis, *Cyprus Law Review (KYNE)*, Vol. 1–2/2025, pp. 47–53.

Focusing on the European Court of Human Rights' landmark 2024 judgment in *Podchasov v. Russia*, this article explores the tension between law-enforcement access to digital communications and the protection of privacy. The ECtHR addressed, for the first time directly, mandatory decryption of end-to-end encrypted communications, finding that indiscriminate decryption requirements disproportionately interfere with Article 8 ECHR. The authors place the judgment within the Court's wider surveillance jurisprudence and examine its broader significance for encryption, digital privacy and the limits that democratic societies must place on state surveillance.

Automated Decisions under Scrutiny: Lessons from C-203/22 for Europe's Digital Rule of Law

Georgios Pavlidis, Ioannis Kastanas & Nikoletta Constantinou, *Cyprus Law Review (KYNE)*, Vol. 3/2025, pp. 161–166.

Examining the CJEU's judgment in Case C-203/22, *CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria)*, this article considers the growing legal demands for transparency and accountability in automated decision-making. The judgment clarifies what the GDPR requires when individuals seek meaningful information about the logic behind automated profiling and scoring systems, while addressing the competing protection of trade secrets. The authors argue that the ruling advances a more substantive model of algorithmic transparency based not merely on disclosure, but on intelligibility and practical contestability, strengthening the emerging foundations of Europe's digital rule of law.

Other Initiatives

The AI Continent Action Plan of the European Union

The plan will bring the necessary elements together to help European businesses excel in AI by setting up at least 19 AI factories across Europe, using a world-leading supercomputing network. These factories will support startups, industry, and researchers to develop cutting-edge AI models and applications. The plan will also establish up to 5 AI gigafactories, large-scale facilities with massive computing power and data centres. They will enable the training of complex AI models at an unprecedented scale. This initiative requires both public and private investment and will secure EU leadership in frontier AI. The InvestAI facility also aims to mobilise €20 billion, to drive private investment in gigafactories. Finally, the EU Proposes the cloud and AI development act that will boost private investment in cloud and data centres. The goal is to at least triple the EU's data centre capacity within the next five to seven years, prioritising sustainable data centres.

For more information, click **here**

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