ISSUE
05
October
2025

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.

Europol's Internet Organised Crime Threat Assessment (IOCTA) Report 2025

The 2025 edition of Europol's Internet Organised Crime Threat Assessment (IOCTA), titled "Steal, Deal and Repeat: How Cybercriminals Trade and Exploit Your Data", presents a stark picture of the evolving cybercrime landscape.

Organised crime groups are adapting rapidly to new technologies, pushing their activities deeper into the digital realm and turning data into both a commodity and a target.

Over the past year, cybercriminals have continued to exploit vulnerabilities in digital infrastructure at scale. Data theft now ranks as a major threat, with compromised personal and institutional data becoming a valuable asset in criminal markets.

The IOCTA reveals how these illicit datasets are traded, reused, and monetised across criminal ecosystems—fueling identity theft, fraud, extortion, and more.

A wide range of methods are used to gain unlawful access to data, including the exploitation of technical flaws and, increasingly, human error. Social engineering remains a particularly powerful tool, allowing criminals to deceive individuals into handing over sensitive information

Crucially, the growing use of generative AI and large language models (LLMs) is enhancing the sophistication of these social engineering attacks. AI-driven tools can now personalise scams, generate convincing phishing messages, and even automate key steps in the criminal process, making it easier for offenders to reach more victims with greater efficiency.

As the IOCTA 2025 makes clear, protecting data in today's cybercrime landscape requires not only strong technical defences, but also increased awareness of how human and algorithmic factors are exploited by organised criminal actors.

Co-funded by the European Union

How the EU AI Act Impacts US-Based Companies

The EU AI Act, in force since August 2024, has global reach, affecting not only EU companies but also US-based businesses offering AI systems or services in the EU market.

From high-risk AI tools to general-purpose models, compliance obligations—such as transparency, data governance, and risk management—apply regardless of where the provider is located. US firms must adapt to EU standards, implement compliance frameworks, and monitor evolving guidance from the European AI Office.

Early preparation is key to mitigating legal, financial, and reputational risks while maintaining market access in the world's second-largest digital economy.

The New U.S. Action Plan for Artificial Intelligence

The Trump administration says the U.S. is in an "AI race" and intends to "win"

The White House has released "America's AI Action Plan," a 28-page roadmap detailing more than 90 federal policy actions to accelerate U.S. leadership in artificial intelligence. Framed around three pillars—accelerating innovation, building AI infrastructure, and leading in international diplomacy and security—the plan marks a sharp pivot from Biden-era guardrails toward deregulation and rapid deployment.

The administration says the U.S. is in an "AI race" and intends to "win," with AI and crypto czar David Sacks emphasizing speed and competitiveness. The plan promises faster permitting for data centers, expanded access to energy, and streamlined agency processes. It also encourages AI exports to allies and directs agencies (e.g., FTC, FCC) to identify and remove barriers to development.

A notable—and controversial—feature is its federalism stance: the White House recommends withholding certain federal AI funding from states it deems to have "burdensome" AI regulations, while asserting it will not interfere with "prudent" state laws. The document also signals revocations or revisions of prior oversight measures and urges uniform federal procurement rules to avoid "ideological bias" in AI systems used by government contractors.

Supporters in industry and some local leaders argue the blueprint will unlock private investment, speed infrastructure build-out, and bolster national security and export competitiveness vis-à-vis China. The focus on energy capacity aligns with data-center growth plans in AI hubs.

Critics, including advocacy groups and several state lawmakers, say the plan mirrors the tech sector's wish list, weakens environmental protections, raises electricity-cost and emissions risks, and sidelines safety and fairness frameworks. Media analyses also highlight provisions seen as targeting "woke" or "biased" AI, without defining standards, and warn of pre-emption pressure on state-level innovation policy.

New Rules for General-Purpose AI

As of 2 August 2025, the EU's obligations under the AI Act for providers of general-purpose AI (GPAI) models kick in across the bloc. These rules require clearer documentation of how models are trained, strong enforcement of copyright, and higher accountability in development.

The European Commission has issued Guidelines clarifying who is considered a "provider," what constitutes placement on the market, and how open-source models may be exempt.

Also released were a public summary template for training data and a voluntary Code of Practice offering firms a structured path to compliance—with benefits like reduced enforcement risk

For GPAI models already on the market before 2 August 2025, firms have a transition period until 2 August 2027 to comply.

Specifically, the Act introduces a compute threshold—models trained above ~10^{23} FLOPs capable of generating language or multimedia are classified as GPAI

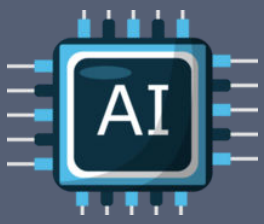
Those that surpass around 10^{25} FLOPs and pose systemic risks face stricter obligations, such as notifying the Commission and ensuring rigorous safety and security measures

Q&A Regulatory Tips

Q: What is Agentic AI, and how can organizations ensure compliance?

Agentic AI refers to systems capable of autonomous decision-making, executing complex tasks with minimal human oversight. To ensure compliance, organizations should start by mapping all use cases where such systems interact with users or critical operations. A thorough risk assessment is essential to evaluate safety, bias, and accountability, especially under the EU AI Act (Articles 6, 9, and 10).

Maintaining meaningful human oversight, alongside clear audit trails and updated documentation of technical files, decision logs, and risk mitigation strategies, helps build trust and ensures that innovation develops within a robust regulatory framework.



EYE ON AI

Current Industry Trends

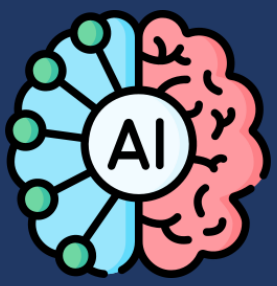
Analysts forecast that Amazon, Meta, Google, and Microsoft will collectively invest $400 billion in AI infrastructure by 2026, up from $350 billion in 2025.

Despite the buzz, many organizations struggle with actualizing AI. Challenges include data privacy, high infrastructure costs, hallucinations and bias in models, and fragmented leadership understanding. Strategic business adoption, grounded in governance and measurable outcomes, is now prioritized over flashy deployment.

AI Developments

Nvidia's Predictions for a Multi-Trillion Dollar AI Future

Nvidia President and CEO Jensen Huang has shared his vision for the rapid expansion of agentic AI, robotics, and supporting infrastructure. He foresees a dramatic surge in AI agents, positioning them as indispensable components of future technology ecosystems. (Source: Reuters)



Other Initiatives

Australia: Ongoing Review and Gap Analysis

Australia's federal government, led by Prime Minister Albanese, broadly agrees that AI regulation is necessary—but there's still no consensus on the specifics. Industry Minister Tim Ayres is overseeing a national AI capability plan, which emphasizes economic opportunity, fair benefit sharing, and safety. As part of the preparatory work, a "gap analysis" has been announced to assess existing frameworks in sectors like health, privacy, copyright, and online safety. The analysis will help determine whether a new, overarching AI law is required or if current regulations can suffice.

Activities of our Center

- **Participation in Training Activities**
  Final Training Event of the EU-funded program ChecMate (Empowering Europeans towards a Media-Savvy Citizenry), 10 July 2025; presenation by Georgios Pavlidis on the 'Legal Aspects of Disinformation and Misinformation in the Era of AI'
- **Participation in Training Activities**
  Webinar organized by the University of Lausanne in the context of COST Action "Globalization, Illicit Trade, Sustainability and Security" (GLITSS), Case Study Webinar Series: Responses to Illicit Trade; 28 August 2025; presenation by Georgios Pavlidis on "The New European Anti-Money Laundering Authority"
- **Participation in EU public consultation**
  Participation of our Center to the Multi-stakeholder Open Public EU consultation on the proposal for a Cloud and AI Development Act in July 2025