Crypto & TradFi

AI × Cybersecurity Special: The Two Sides of AI in European Finance

Unravelling the regulations for investors

When AI becomes both the risk and the defence

Previous editions of the Regulatory Brief have described European regulation in successive layers: the AI Act and its Omnibus (Seqlense Regulatory Brief 7), its relationship with the GDPR (Seqlense Regulatory Brief 8), the transition to post-quantum cryptography (Seqlense Regulatory Brief 9) and the crystallisation of European technological sovereignty (Seqlense Regulatory Brief 10). This eleventh edition tackles a subject that intersects with all the previous ones: the operational convergence between artificial intelligence and cybersecurity in the financial sector.

Between 3 and 12 June 2026, six landmark publications marked a turning point. On 3 June, the AMF published a news item calling on financial actors to strengthen their defences against AI-related threats. On the same day, the three European supervisory authorities (EBA, EIOPA, ESMA) published their first joint annual report on major ICT incidents under DORA, detailing 3,383 incidents recorded in 2025 and issuing an explicit warning regarding AI-driven tools. On 8 June, the AMF followed this up with a special edition of its Savings and Investment Barometer, dedicated to the use of AI by French savers. And between 9 and 12 June, the Dutch AFM published three additional news items on the same AI-cyber-DORA nexus, almost simultaneously with its counterparts.

This convergence is no coincidence. It reflects an institutional shift: AI cybersecurity is ceasing to be a technical issue and becoming a matter of governance, and European supervisory convergence is now manifesting itself in real time, without waiting for the formalisation of common guidelines. The terminology used by regulators is also converging: ‘industrialisation of malicious campaigns’ from the AMF, ‘highly capable AI-driven tools’ from the ESAs, and ‘snellere AI-aanvallen’ from the AFM – all expressions that form a common analytical framework.

For regulated financial institutions and investors, this ‘double-edged’ nature of AI, both a vector for attack and a tool for defence, a source of information for savers and a factor contributing to opacity, calls for a comprehensive understanding. This edition outlines the key points.

The weak signal

AI cybersecurity is ceasing to be a technical issue and is becoming an explicit supervisory requirement, formalised simultaneously by several European regulators.

Three key terms appear in the financial authorities’ communication in spring 2026, marking this change in status. Firstly, the first concerns the expression “industrialisation of malicious campaigns” used by the AMF. This phrasing removes the subject from the realm of isolated attacks and places it within a mass-scale dynamic. Secondly, the terms “highly capable AI-driven tools” are used by the ESAs in the joint DORA report and constitute another formulation that unambiguously characterises offensive tools that are becoming commonplace. Finally, the explicit call to “integrate AI-related risks into cybersecurity scenarios” features explicitly among the AMF’s recommendations addressed to the senior management of regulated entities.

For senior management and risk committees, this shift in terminology means that AI cybersecurity is no longer a technical issue but has become a governance concern. On 1 July 2026, the AMF will hold an educational webinar for supervised professionals. From that same date, it will survey portfolio management firms, crowdfunding service providers and crypto-asset service providers on the measures taken or planned to address risks associated with AI models, as part of a survey whose results will be published in the autumn.

Focus 1: AMF/ESAs Convergence of 3 June 2026

On the same day, the AMF and the three European supervisory authorities published two complementary documents. The AMF, in a news item entitled “Cyber resilience: the AMF calls on financial actors to strengthen their measures in the face of rapidly evolving threats linked to artificial intelligence”, sets out nine operational recommendations, announces an educational webinar on 1 July and the launch of a sector-specific survey from July onwards. The ESAs, in their first joint report on major DORA ICT incidents (reference JC 2026 16), identified 3,383 major incidents in 2025 and emphasised that highly capable AI-driven tools require financial entities to strengthen their cybersecurity measures.

This dual publication, combining the voice of a national authority with that of the three European authorities, outlines the expected supervisory stance: dynamic DORA compliance, an ‘all-in’ approach adapted to the pace of evolving threats, and the explicit integration of AI-driven attack scenarios into testing scenarios and crisis exercises.

What to watch out for:

- The AMF webinar on 1 **July 2026** aimed at asset management firms, pension fund managers and pension scheme administrators.
- The results of **the AMF survey** on measures to address risks associated with AI models, expected in autumn 2026.
- The **DORA review focusing on French entities** announced by the AMF following on from the ESAs report.

Focus 2: The Dutch perspective with the AFM in three publications

Between 9 and 12 June 2026, the AFM (Autoriteit Financiële Markten) published three news items that echoed, often word for word, the concerns expressed by the AMF and the ESAs. On 9 June, it warned of AI-driven attacks, whose chains are becoming faster and more sophisticated, and which particularly expose small and medium-sized players; it recommended strengthening basic measures (multi-factor authentication, access management, monitoring) and the defensive use of AI. On 11 June, it published a thematic review on ICT risk management for trading platforms under DORA, identifying overly broad gap analyses and several areas requiring improvement (security monitoring, access management, logging, emergency changes, continuity).

On 12 June, the AFM published its assessment of the Dutch law implementing the AI Act. Its Chair, Laura van Geest, considers the text to be "fundamentally workable" but in need of targeted adjustments. The AFM challenges the proposed division of responsibilities between itself and the DNB, and argues that both authorities should be designated, each in their respective roles (conduct and prudential), as supervisors of the prohibition provisions and high-risk standards of the AI Act. This debate foreshadows a key issue for all European jurisdictions.

What to watch out for:

- **The outcome of the AFM/DNB debate** on the division of responsibilities under the AI Act, and its potential impact on France (AMF/ACPR/CNIL).
- The evolution of **supervisory expectations regarding trading platforms** (regulated markets, MTFs, OTFs) under DORA.
- The **real-time convergence** of European supervisory communications (AMF, AFM, ESAs, and soon BaFin and CONSOB).

Focus 3: Investors and AI: the AMF Barometer of 8 June 2026

On 8 June 2026, the AMF published a special edition of its Barometer dedicated to the use of AI by French people in their investment practices, based on a survey of 2,120 representative respondents. The results are mixed: 11% of French people say they use AI as a source of

information before making an investment, compared with 42% who turn to their bank or financial adviser. But this average masks a clear divide.

Those under 35 are nearly five times more likely than those over 55 to use AI (19% versus 4%). Usage increases with educational attainment and socio-professional status, but above all with risk appetite: 33% of crypto-asset investors say they use AI, 24% of crowdfunding investors, and 19% of stock market investors. The French public's perception is mixed: 54% see the potential for more tailored advice and 52% for improved performance or lower fees, but 67% fear errors or poor decisions and 75% worry about reduced transparency in investments.

What to watch out for:

- The evolution of AI usage among **crypto-asset investors** (33%), particularly for MiCA CASPs.
- **The gradual decline in the role of the bank advisor** as the main source of information (48% in 2024, 42% in 2025).
- French consumers' **expectations** regarding **transparency** in the use of AI by professionals.

Focus 4: The dual offensive/defensive nature of AI

A combined reading of the June 2026 publications highlights a structural feature of AI in finance: an offensive/defensive symmetry that precludes any unambiguous interpretation. On the offensive side, AI models accelerate the identification of vulnerabilities, facilitate their exploitation and enable the industrialisation of malicious campaigns, audio or video deepfakes for CEO fraud, large-scale personalised social engineering and adaptive malware. On the defensive side, AI enhances behavioural anomaly detection, automates vulnerability monitoring, supports the triage of SOC alerts and accelerates the deployment of patches.

This symmetry imposes a dual constraint. On the one hand, the race towards defensive AI maturity: an actor whose defensive tools fail to keep pace with the evolution of offensive tools sees their relative exposure worsen with each cycle. On the other hand, the governance of the defensive AI tools themselves: they are susceptible to errors, bias and adversarial attacks, and must therefore be governed in accordance with AI Act standards whilst meeting DORA requirements. This dual requirement for compliance with the AI Act and DORA converges with the GDPR (Issue #8) and post-quantum (Issue #9) aspects already documented.

What to watch out for:

- Developments in **the cyber capabilities of edge AI models** and the associated assessments published by their suppliers.
- The integration of **defensive AI into regulatory frameworks** (TLPT DORA, crisis exercises, PASSI audits, red teaming).

- The **governance of defensive AI tools** themselves, at the intersection of the AI Act and DORA.

Key takeaways

Five fundamental transformations are currently underway:

- A shift from **static DORA compliance to dynamic DORA compliance**, adjusted in line with the pace of threats.
- The emergence of an **integrated AI-cyber vision**, with AI explicitly incorporated into cyber scenarios, crisis exercises and audits.
- Elevation of the issue to the level **of the risk committee and the executive committee**, beyond just the CIO and CISO.
- Recognition of AI as **a fundamental layer of the customer journey**, particularly among young investors and risk-seeking profiles.
- The emergence of **real-time European supervisory convergence**, evident in the near-synchronisation of publications by the AMF, the ESAs and the AFM.

Conclusion

For European financial regulators, AI is no longer a matter of anticipation, but a governance issue to be addressed using the supervisor's familiar tools: risk mapping, controls, exercises and incident reporting. The dual offensive/defensive nature of the issue precludes any single interpretation, and the operational timetable is taking shape with, among other things, the AMF webinar on 1 July, the sectoral survey starting this summer, and the French DORA review in the autumn. For regulated entities, the time for raising awareness is over; it is now time for the practical integration of AI risks into the overall cybersecurity and operational resilience framework.

Main sources

- AMF, *"Cyber resilience: the AMF calls on financial firms to strengthen their defences in the face of rapidly evolving threats linked to artificial intelligence"*, news item published on 3 June 2026 (amf-france.org).
- Joint Committee of the ESAs (EBA, EIOPA, ESMA), *Report on Major ICT-related Incidents 2025*, reference JC 2026 16, published on 3 June 2026.
- AMF, *"Special edition of the AMF Barometer: still little used in investment practices, artificial intelligence is proving more appealing to young investors"*, published on 8 June 2026.
- AMF, *AMF Savings and Investment Barometer — 2025*, fieldwork 19 September — 3 October 2025, sample of 2,120 people.
- AFM (Netherlands), *"Faster AI attacks require stronger resilience"*, news item dated 9 June 2026; report "Advanced AI models increase cyber risks for businesses" (afm.nl).
- AFM, *"Trading systems require stricter ICT risk management under DORA"*, thematic review of 11 June 2026.
- AFM, *'Implementing Act for the AI Regulation is enforceable, but adjustments are needed for effective supervision'*, press release and implementation assessment of 12 June 2026.
- Regulation (EU) 2022/2554 of 14 December 2022 (DORA), applicable since 17 January 2025.
- ENISA, *ENISA Threat Landscape: Finance Sector*, February 2025; ENISA-ESAs multilateral MoU, June 2024.
- ANSSI, *IT Security Guide* — reference for cybersecurity best practices cited by the AMF.
- AMF, *AMF Action and Supervision Priorities for 2026*, institutional document.

***

The Seqlense Regulatory Brief — Crypto & TradFi · Issue #11