Crypto &TradFi

Spécial IA × cybersécurité : La double face de l'IA dans la finance européenne

Décrypter la réglementation pour les investisseurs

Quand l'IA devient à la fois le risque et la défense

Les éditions précédentes du Regulatory Brief ont décrit la régulation européenne par couches successives : l'AI Act et son Omnibus (Seqlense Regulatory Brief 7), son articulation avec le RGPD (Seqlense Regulatory Brief 8), la transition vers la cryptographie post-quantique (Seqlense Regulatory Brief 9) et la cristallisation de la souveraineté technologique européenne (Seqlense Regulatory Brief 10). Cette onzième édition s'attaque à un sujet qui croise tous les précédents : la convergence opérationnelle entre l'intelligence artificielle et la cybersécurité dans le secteur financier.

Entre le 3 et le 12 juin 2026, six publications de référence ont marqué un tournant. Le 3 juin, l'AMF a publié une actualité appelant les acteurs financiers à renforcer leurs dispositifs face aux menaces liées à l'IA. Le même jour, les trois autorités européennes de supervision (EBA, EIOPA, ESMA) ont publié leur premier rapport annuel conjoint sur les incidents TIC majeurs au titre de DORA, relatant 3 383 incidents recensés en 2025 et une alerte explicite concernant les outils pilotés par l'IA. Le 8 juin, l'AMF a complété cette séquence par une édition spéciale de son Baromètre de l'épargne et de l'investissement, consacrée à l'usage de l'IA par les épargnants français. Et entre le 9 et le 12 juin, l'AFM néerlandaise a publié trois actualités complémentaires sur le même nexus IA-cyber-DORA, quasi simultanément à ses homologues.

Cette convergence n'est pas fortuite. Elle traduit une bascule institutionnelle : la cybersécurité IA cesse d'être une rubrique technique pour devenir un objet de gouvernance, et la convergence supervisorielle européenne se manifeste désormais en temps réel, sans attendre la formalisation de lignes directrices communes. Les vocabulaires utilisés par les régulateurs convergent également : « industrialisation des campagnes malveillantes » côté AMF, « highly capable AI-driven tools » côté ESAs, « snellere AI-aanvallen » côté AFM, autant d'expressions qui dessinent une grille d'analyse commune.

Pour les acteurs financiers régulés et les investisseurs, cette « double face » de l'IA, vecteur d'attaque et outil de défense, source d'information pour les épargnants et facteur d'opacité, appelle une lecture intégrée. Cette édition en propose les éléments principaux.

Le signal faible

La cybersécurité IA cesse d'être un sujet technique pour devenir une attente supervisorielle explicite, formalisée simultanément par plusieurs régulateurs européens.

Trois éléments lexicaux apparaissent dans la communication des autorités financières au printemps 2026 et marquent ce changement de statut. D'abord, le premier concerne l'expression « industrialisation des campagnes malveillantes » utilisée par l'AMF. Cette formulation sort le sujet du registre de l'attaque isolée pour l'inscrire dans une dynamique de masse. Ensuite, les termes « highly capable AI-driven tools » sont utilisés par les ESAs dans le rapport conjoint DORA et constituent une autre formulation qui caractérise, sans détour, des outils offensifs en cours de banalisation. Enfin, l'invitation explicite à « intégrer les risques liés à l'IA dans les scénarios de cybersécurité » figure explicitement parmi les recommandations de l'AMF adressées aux dirigeants des entités régulées.

Pour les directions générales et les comités des risques, ce déplacement lexical signifie que la cybersécurité IA cesse d'être une rubrique technique pour devenir un enjeu de gouvernance. Le 1er juillet 2026, l'AMF tiendra un webinaire pédagogique à l'intention des professionnels supervisés. À partir de cette même date, elle interrogera les sociétés de gestion de portefeuille, les prestataires de services de financement participatif et les prestataires de services sur crypto-actifs sur les mesures prises ou envisagées face aux risques liés aux modèles d'IA, dans le cadre d'une enquête dont les résultats seront publiés à l'automne.

Focus 1 : La convergence AMF / ESAs du 3 juin 2026

Le même jour, l'AMF et les trois autorités européennes de supervision ont publié deux documents qui se complètent. L'AMF, dans une actualité intitulée « Résilience cyber : l'AMF appelle les acteurs financiers à renforcer leurs dispositifs face à l'évolution rapide des menaces liées à l'intelligence artificielle », formule neuf recommandations opérationnelles, annonce un webinaire pédagogique le 1er juillet et le lancement d'une enquête sectorielle dès juillet. Les ESAs, dans leur premier rapport conjoint sur les incidents TIC majeurs DORA (référence JC 2026 16), recensent 3 383 incidents majeurs en 2025 et soulignent que des outils pilotés par l'IA hautement capables imposent aux entités financières de renforcer leurs mesures de cybersécurité.

Cette double publication, conjuguant la voix d'une autorité nationale et celle des trois autorités européennes, dessine la posture supervisorielle attendue : une conformité DORA dynamique,

ajustée au rythme de l'évolution des menaces, et l'intégration explicite des hypothèses d'attaque pilotées par IA dans les scénarios de tests et les exercices de crise.

Ce qu'il faut surveiller:

- Le webinaire AMF du **1er juillet 2026** à destination des SGP, PSFP et PSCA.
- Les résultats de l'**enquête AMF** sur les mesures face aux risques liés aux modèles d'IA, attendus à l'automne 2026.
- Le **bilan DORA centré sur les entités françaises** annoncé par l'AMF dans le prolongement du rapport ESAs.

Focus 2 : Le miroir néerlandais avec l'AFM en trois publications

Entre le 9 et le 12 juin 2026, l'AFM (Autoriteit Financiële Markten) a publié trois actualités qui font écho, souvent terme à terme, aux préoccupations exprimées par l'AMF et les ESAs. Le 9 juin, elle alerte sur les attaques pilotées par l'IA, dont les chaînes deviennent plus rapides et plus sophistiquées, et qui exposent particulièrement les acteurs de taille moyenne et petite ; elle recommande un renforcement des mesures de base (authentification multifacteurs, gestion des accès, monitoring) et un usage défensif de l'IA. Le 11 juin, elle publie une exploration thématique sur la gestion des risques TIC des plateformes de négociation au titre de DORA, identifiant des analyses d'écart trop globales et plusieurs domaines à renforcer (security monitoring, gestion des accès, logging, changements d'urgence, continuité).

Le 12 juin, l'AFM rend publique son évaluation de la loi néerlandaise de mise en œuvre de l'AI Act. Sa présidente, Laura van Geest, estime que le texte est « fondamentalement exécutable » mais nécessite des ajustements ciblés. L'AFM conteste la répartition proposée des compétences entre elle-même et la DNB, et plaide pour que les deux autorités soient désignées, chacune dans son rôle (conduite et prudentiel), comme superviseurs des dispositions d'interdiction et des normes haut risque de l'AI Act. Ce débat préfigure un sujet structurant pour l'ensemble des juridictions européennes.

Ce qu'il faut surveiller:

- L'**issue du débat AFM / DNB** sur la répartition des compétences AI Act, et son potentiel d'influence sur la France (AMF / ACPR / CNIL).
- L'évolution des **attentes supervisorielles sur les plateformes de négociation** (marchés réglementés, MTF, OTF) au titre de DORA.
- La **convergence en temps réel** des communications supervisorielles européennes (AMF, AFM, ESAs, à venir BaFin et CONSOB).

Focus 3 : Les investisseurs face à l'IA avec le Baromètre AMF du 8 juin 2026

Le 8 juin 2026, l'AMF a publié une édition spéciale de son Baromètre consacrée à l'usage de l'IA par les Français dans leurs pratiques d'investissement, à partir d'une enquête menée auprès de 2 120 personnes représentatives. Les résultats sont mesurés : 11 % des Français déclarent utiliser l'IA comme source d'information avant un placement, contre 42 % qui se tournent vers leur conseiller bancaire ou financier. Mais cette moyenne masque une fracture nette.

Les moins de 35 ans sont près de cinq fois plus nombreux que les plus de 55 ans à utiliser l'IA (19 % contre 4 %). L'usage progresse avec le niveau de diplôme et la position socioprofessionnelle, mais surtout avec l'appétence au risque : 33 % des investisseurs en crypto-actifs déclarent recourir à l'IA, 24 % des investisseurs en crowdfunding, 19 % des investisseurs en Bourse. La perception des Français est ambivalente : 54 % identifient un potentiel de conseils plus adaptés et 52 % une amélioration de la performance ou une baisse des frais, mais 67 % redoutent des erreurs ou de mauvaises décisions et 75 % une moindre transparence des placements.

Ce qu'il faut surveiller:

- L'évolution de l'usage de l'IA chez les **investisseurs en crypto-actifs** (33 %), particulièrement pour les CASPs MiCA.
- L'**érosion progressive de la part du conseiller bancaire** comme source d'information principale (48 % en 2024, 42 % en 2025).
- Les **attentes de transparence** des Français vis-à-vis de l'usage de l'IA par les professionnels.

Focus 4 : La double face offensive/défensive de l'IA

La lecture combinée des publications de juin 2026 met en évidence un trait structurel de l'IA dans la finance : une symétrie offensive/défensive qui interdit toute lecture univoque. Côté offensif, les modèles d'IA accélèrent l'identification des vulnérabilités, facilitent leur exploitation et permettent l'industrialisation des campagnes malveillantes, des deepfakes audio ou vidéo pour des fraudes au président, de l'ingénierie sociale personnalisée à grande échelle et du malware adaptatif. Côté défensif, l'IA renforce la détection comportementale des anomalies, automatise la veille sur les vulnérabilités, soutient le triage des alertes du SOC et accélère la mise en œuvre de correctifs.

Cette symétrie impose une double contrainte. D'une part, la course à la maturité IA défensive : un acteur dont les outils de défense ne suivent pas le rythme d'évolution des outils offensifs voit son exposition relative s'aggraver à chaque cycle. D'autre part, la gouvernance des outils d'IA défensifs eux-mêmes : ils sont susceptibles d'erreurs, de biais et d'attaques adverses, et doivent donc être gouvernés selon les standards de l'AI Act tout en répondant aux exigences DORA. Cette double

exigence avec AI Act et DORA converge avec les articulations RGPD (Édition #8) et post-quantique (Édition #9) déjà documentées.

Ce qu'il faut surveiller:

- L'évolution des **capacités cyber des modèles d'IA frontière** et les évaluations associées publiées par leurs fournisseurs.
- L'intégration de l'**IA défensive dans les dispositifs réglementaires** (TLPT DORA, exercices de crise, audits PASSI, red teaming).
- La **gouvernance des outils d'IA défensifs** eux-mêmes, à la croisée de l'AI Act et de DORA.

À retenir

Cinq transformations structurantes sont actuellement à l'œuvre :

- Passage d'une **conformité DORA statique à une conformité DORA dynamique**, ajustée au rythme des menaces.
- Émergence d'une **vision intégrée IA-cyber**, avec l'inscription explicite de l'IA dans les scénarios cyber, les exercices de crise et les audits.
- Élévation du sujet au niveau du **comité des risques et du COMEX**, au-delà des seules DSI et RSSI.
- Reconnaissance de l'IA comme **couche fondamentale du parcours client**, notamment chez les jeunes investisseurs et les profils appétents au risque.
- Émergence d'une **convergence supervisorielle européenne en temps réel**, visible dans la quasi-synchronie des publications de l'AMF, des ESAs et de l'AFM.

Conclusion

L'IA n'est plus pour les régulateurs financiers européens un sujet d'anticipation, mais un objet de gouvernance à instruire avec les outils familiers du superviseur : cartographies, contrôles, exercices, déclarations d'incidents. La double face offensive/défensive interdit toute lecture univoque, et le calendrier opérationnel se précise avec, entre autres, le webinaire AMF du 1er juillet, l'enquête sectorielle dès l'été, et le bilan DORA français à l'automne. Pour les acteurs régulés, le temps n'est plus à la prise de conscience, mais à l'intégration concrète des risques IA dans le dispositif global de cybersécurité et de résilience opérationnelle.

Sources principales

- AMF, *« Résilience cyber : l'AMF appelle les acteurs financiers à renforcer leurs dispositifs face à l'évolution rapide des menaces liées à l'intelligence artificielle »*, actualité publiée le 3 juin 2026 (amf-france.org).
- Joint Committee of the ESAs (EBA, EIOPA, ESMA), *Report on Major ICT-related Incidents 2025*, référence JC 2026 16, publié le 3 juin 2026.
- AMF, *« Édition spéciale du Baromètre AMF : encore peu utilisée dans les pratiques d'investissement, l'intelligence artificielle séduit davantage les jeunes investisseurs »*, publication du 8 juin 2026.
- AMF, *Baromètre AMF de l'épargne et de l'investissement — 2025*, terrain 19 septembre — 3 octobre 2025, échantillon de 2 120 personnes.
- AFM (Pays-Bas), *« Snellere AI-aanvallen vragen om sterkere weerbaarheid »*, actualité du 9 juin 2026 ; rapport « Geavanceerde AI-modellen vergroten cyberrisico's voor ondernemingen » (afm.nl).
- AFM, *« Handelssystemen vragen om scherpere ICT-risicobeheersing onder DORA »*, exploration thématique du 11 juin 2026.
- AFM, *« Uitvoeringswet AI-verordening uitvoerbaar, maar aanpassingen nodig voor effectief toezicht »*, communiqué et uitvoeringstoets du 12 juin 2026.
- Règlement (UE) 2022/2554 du 14 décembre 2022 (DORA), applicable depuis le 17 janvier 2025.
- ENISA, *ENISA Threat Landscape: Finance Sector*, février 2025 ; MoU multilatéral ENISA-ESAs, juin 2024.
- ANSSI, *Guide d'hygiène informatique* — référence pour les bonnes pratiques de cybersécurité citée par l'AMF.
- AMF, *Priorités d'action et de supervision de l'AMF pour 2026*, document institutionnel.

****

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