GUIDE PRATIQUE . MAI 2026 . VOLUME 2

Hashtag Avocats

PÔLE RÉGULATION FINANCIÈRE, INTELLIGENCE ARTIFICIELLE ET CONFORMITÉ

Intelligence artificielle et qualification *en LCB-FT*

Règlement (UE) 2024/1689 dit AI Act.

Guide pratique à destination des établissements financiers, de leurs équipes conformité et de leurs conseils.

AUTEUR PRINCIPAL

Arnaud Touati

Avocat Associé Fondateur

Barreaux de Paris et de Luxembourg

ÉDITION

SELARL Hashtag Avocats . Toque D1675 . Version 1 . Mai 2026

Avertissement

Le présent guide pratique a été rédigé par le pôle régulation financière, intelligence artificielle et conformité du cabinet Hashtag Avocats à des fins exclusivement informatives et pédagogiques. Il offre une présentation synthétique du régime issu du règlement (UE) 2024/1689 dit AI Act et de son articulation avec la qualification des systèmes d'intelligence artificielle utilisés en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme. Il ne constitue pas un conseil juridique et ne saurait engager la responsabilité du cabinet ou de son auteur au titre de situations particulières.

Toute application opérationnelle du dispositif requiert une analyse personnalisée tenant compte de la qualification précise du système concerné, des cas d'usage poursuivis, de l'architecture interne de l'établissement, des juridictions impliquées et de l'état du droit positif à la date de la décision.

La matière étant en évolution constante, notamment s'agissant des normes harmonisées en cours d'élaboration au sein du CEN-CENELEC, des futures lignes directrices du Bureau européen de l'IA, des bacs à sable nationaux opérationnels au plus tard le 2 août 2026 et des prises de position à venir de l'ACPR, de l'AMF et de la CNIL, le lecteur est invité à confirmer toute donnée opérationnelle auprès du cabinet.

Document achevé d'être rédigé le 20 mai 2026. Reproduction et diffusion soumises à autorisation préalable du cabinet.

TABLE DES MATIÈRES

Sommaire

PRÉAMBULE

Le déplacement silencieux *du métier de la conformité*

Ce que change l'entrée en application progressive du règlement (UE) 2024/1689 pour les équipes LCB-FT du secteur financier.

Pendant deux décennies, la conformité financière a appris à composer avec la donnée. La directive sur la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, dans ses versions successives jusqu'à la cinquième, ainsi que le règlement général sur la protection des données, ont structuré une discipline désormais mature. À cette discipline s'ajoutent les obligations sectorielles propres aux établissements de crédit, aux entreprises d'investissement, aux établissements de paiement et de monnaie électronique, et plus récemment aux prestataires de services sur crypto-actifs, qui ensemble forment un écosystème normatif dense et exigeant.

Avec l'entrée en vigueur, le 1er août 2024, du règlement (UE) 2024/1689 dit AI Act, le rapport entre la conformité financière et l'intelligence artificielle change de nature. Ce texte horizontal d'ampleur considérable, qui inaugure le premier instrument réglementaire mondial dédié à l'intelligence artificielle, ne se contente pas de surveiller la conformité externe des outils technologiques que les établissements déploient pour exécuter leurs obligations de vigilance, de filtrage ou de signalement. Il gouverne désormais leur conception même, leur gouvernance, leur documentation et la qualité du contrôle humain qui s'exerce sur eux. C'est, en substance, une grammaire nouvelle qui se superpose à la grammaire ancienne.

Le présent guide pratique a vocation à restituer la réalité du droit positif au 20 mai 2026, à dissiper les contresens les plus fréquemment observés dans les directions conformité, à éclairer les principales zones d'incertitude interprétative, et à formuler des recommandations opérationnelles concrètes à l'attention des établissements financiers et de leurs conseils. Il s'inscrit dans la collection éditoriale du pôle régulation financière, intelligence artificielle et conformité du cabinet Hashtag Avocats, dont il constitue le volume 2, le volume 1 ayant été consacré à l'échange automatique d'informations en matière de crypto-actifs.

Le contresens le plus structurant que nous avons souhaité dissiper tient à la qualification haut risque. Une partie significative de la communauté regtech a diffusé, au cours des derniers mois, l'idée selon laquelle tout outil d'intelligence artificielle déployé en LCB-FT entrerait, par défaut, dans la

catégorie haut risque de l'annexe III du règlement. Le texte dit exactement le contraire. L'annexe III, point 5 b), exclut expressément du périmètre haut risque *« les systèmes d'IA utilisés à des fins de détection de fraude financière »*, position confirmée par le considérant 58 du règlement, par la publication institutionnelle de l'ACPR « AI Act » et réaffirmée lors de la réunion de Place du 17 septembre 2025. Cette exclusion, juridiquement nette, ne libère cependant pas les établissements ; elle reconfigure leurs obligations autour d'un ensemble d'exigences qui demeurent.

Le guide qui suit décline ces enjeux selon une progression construite en six parties. La première rappelle le cadre juridique général de l'AI Act. La deuxième traite la qualification des systèmes d'IA en LCB-FT et la portée précise de l'exclusion. La troisième détaille les obligations résiduelles applicables au titre du règlement IA. La quatrième propose des qualifications pratiques sur quatre cas d'usage représentatifs. La cinquième aborde la gouvernance interne et la conformité IA by design. La sixième formule des recommandations opérationnelles différenciées selon les fonctions de l'organisation.

01. Le cadre juridique de l'AI Act

Architecture du texte, logique pyramidale par les risques, distinction fournisseur-déployeur, modèles d'IA à usage général, sanctions et calendrier.

1.1 Architecture et logique pyramidale par les risques

Le règlement (UE) 2024/1689 a été adopté par les institutions européennes le 13 juin 2024, publié au Journal officiel de l'Union européenne le 12 juillet 2024 et est entré en vigueur le 1er août 2024[1]. Avec 113 articles, 180 considérants et 13 annexes, il s'agit de l'un des textes les plus volumineux du droit dérivé européen. Il se présente comme le premier instrument horizontal au monde dédié à l'intelligence artificielle, structuré selon une logique de gestion proportionnée du risque inspirée de la législation européenne sur la sécurité des produits.

Le règlement décline quatre paliers d'intensité réglementaire, hiérarchisés selon le niveau de risque que le système d'intelligence artificielle est susceptible de présenter pour la santé, la sécurité et les droits fondamentaux des personnes. Au sommet, les pratiques interdites limitativement énumérées à l'article 5, dont la commercialisation et l'utilisation sont en principe prohibées. En dessous, les systèmes à haut risque encadrés par les articles 6 à 27, soumis à un véritable corpus d'exigences techniques et organisationnelles. Plus bas, les systèmes à risque limité soumis aux obligations de transparence des articles 50 et suivants. À la base, les systèmes à risque minimal, laissés à la libre concurrence et à des codes de conduite volontaires.

Cette logique pyramidale a une vertu cardinale : elle évite l'imposition d'obligations uniformes à des systèmes dont la criticité est, dans les faits, très inégale. Elle suppose en revanche un travail rigoureux de qualification au cas par cas, qui ne peut être délégué à des automatismes interprétatifs. Toute la difficulté pratique de la conformité IA se loge dans cette opération de qualification, qui détermine en cascade l'intensité des obligations applicables.

1.2 Les huit pratiques interdites de l'article 5

L'article 5 du règlement dresse la liste limitative des huit catégories de pratiques considérées comme contraires aux valeurs de l'Union et donc

[1] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, JOUE L du 12 juillet 2024. Sources concordantes : EUR-Lex, version FR ; Commission européenne, AI Act Explorer ; ACPR, publication institutionnelle « AI Act ».

absolument prohibées. Ces interdictions sont applicables depuis le 2 février 2025, par dérogation au calendrier général d'application du règlement.

Sont notamment prohibés les systèmes recourant à des techniques subliminales, manipulatrices ou trompeuses qui altèrent substantiellement le comportement d'une personne d'une manière susceptible de causer un préjudice ; les systèmes exploitant les vulnérabilités de groupes spécifiques liées à leur âge, à un handicap ou à une situation économique ou sociale ; les systèmes de notation sociale fondés sur le comportement social ou des caractéristiques personnelles, lorsque l'évaluation conduit à un traitement défavorable injustifié ; les systèmes d'évaluation prédictive du risque qu'une personne commette une infraction pénale, fondés exclusivement sur le profilage ou sur l'évaluation de traits de personnalité ; le moissonnage non ciblé d'images facialees provenant d'Internet ou de vidéosurveillance pour constituer des bases de reconnaissance faciale ; l'inférence des émotions sur le lieu de travail ou dans les établissements d'enseignement, sauf usages médicaux ou de sécurité ; la catégorisation biométrique inférant des caractéristiques sensibles ; et l'identification biométrique à distance en temps réel à des fins répressives, sous réserve d'exceptions strictement encadrées.

Le point d'attention spécifique pour la conformité financière tient à l'évaluation prédictive du risque d'infraction sur la seule base du profilage. Cette interdiction trace une frontière fine entre la détection algorithmique du risque, qui demeure parfaitement licite en LCB-FT, et l'anticipation algorithmique du comportement délictueux sur la seule base du profilage, qui est prohibée. La distinction conceptuelle est essentielle et conditionne, en aval, la légalité même de certains outils de scoring de risque dans le secteur financier.

Les manquements aux pratiques interdites de l'article 5 sont sanctionnés à hauteur de 35 millions d'euros ou 7 pour cent du chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu[2]. C'est le palier supérieur de l'article 99 du règlement, et son niveau de sévérité, plus élevé que celui du régime général du RGPD, dit la gravité que le législateur européen attache à ces interdictions.

1.3 Les systèmes à haut risque et l'annexe III

L'article 6 du règlement, lu avec l'annexe III, identifie huit domaines de qualification haut risque : biométrie, infrastructures critiques, éducation et

[2]Article 99, paragraphe 3, du règlement (UE) 2024/1689 : sanctions financières en cas de manquement aux interdictions de l'article 5. Le montant le plus élevé entre la valeur fixe et le pourcentage du chiffre d'affaires est retenu.

formation professionnelle, emploi et gestion des travailleurs, accès aux services privés essentiels et aux services et prestations publics essentiels, activités répressives, migration, asile et contrôle aux frontières, et administration de la justice et processus démocratiques[3]. Dans le secteur financier, deux familles de systèmes sont expressément qualifiées : les systèmes destinés à l'évaluation de la solvabilité des personnes physiques ou à l'établissement de leur note de crédit, et les systèmes d'évaluation des risques et de tarification en assurance-vie et santé.

La rédaction exacte de l'annexe III, point 5 b), comporte une exclusion lourde de conséquences dont nous traiterons en détail dans la partie 2 : *« à l'exception des systèmes d'IA utilisés à des fins de détection de fraude financière »* [4]. Cette exclusion expresse constitue la nuance la plus importante du règlement pour notre matière.

La conséquence pratique de la qualification haut risque, lorsqu'elle s'applique, est lourde : application des articles 8 à 15 du règlement, qui imposent un système de gestion des risques continu, une gouvernance des données et des jeux d'entraînement, une documentation technique substantielle, un dispositif de journalisation, des exigences de transparence et d'information du déployeur, un contrôle humain effectif au sens de l'article 14, et des standards d'exactitude, de robustesse et de cybersécurité[5]. À cela s'ajoutent, pour le fournisseur, l'évaluation de conformité de l'article 43, le marquage CE de l'article 48 et l'enregistrement à la base de données européenne de l'article 49 ; pour le déployeur, les obligations spécifiques de l'article 26 et, dans certaines hypothèses, l'analyse d'impact sur les droits fondamentaux de l'article 27.

L'article 6, paragraphe 3, du règlement aménage une clause de dérogation permettant d'écarter la qualification haut risque pour les systèmes qui ne présentent pas de risque important de préjudice à la santé, la sécurité ou les droits fondamentaux, à condition qu'au moins une condition limitativement énumérée soit remplie. Cette dérogation est cependant

[3]Annexe III du règlement (UE) 2024/1689 : liste des systèmes d'IA à haut risque visés à l'article 6, paragraphe 2. La liste comprend huit domaines limitativement énumérés.

[4]Annexe III, point 5 b), du règlement (UE) 2024/1689, texte en vigueur : *« systèmes d'IA destinés à être utilisés pour évaluer la solvabilité de personnes physiques ou pour établir leur note de crédit, à l'exception des systèmes d'IA utilisés à des fins de détection de fraude financière »*. Considérant 58 du règlement, dans le même sens. Position confirmée par l'ACPR dans sa publication institutionnelle « AI Act » et lors de sa réunion de Place du 17 septembre 2025.

[5]Articles 8 à 15 du règlement (UE) 2024/1689 : exigences applicables aux systèmes à haut risque, soit un système de gestion des risques (article 9), une gouvernance des données et des jeux d'entraînement (article 10), une documentation technique (article 11), des enregistrements automatiques d'événements (article 12), une transparence et une information à l'égard des déployeurs (article 13), un contrôle humain effectif (article 14), et des exigences d'exactitude, de robustesse et de cybersécurité (article 15).

neutralisée dès lors que le système effectue un profilage de personnes physiques au sens du RGPD, hypothèse à laquelle les systèmes LCB-FT individualisés peuvent, selon leur architecture, se trouver confrontés.

1.4 Fournisseur, déployeur et chaîne de valeur

La répartition des obligations dans la chaîne de valeur de l'intelligence artificielle est conditionnée par la qualification d'opérateur retenue par l'article 3 du règlement. Deux qualifications principales doivent être distinguées : le fournisseur et le déployeur.

Le fournisseur, au sens de l'article 3 point 3, est la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui développe un système d'IA ou un modèle d'IA à usage général, ou qui fait développer un tel système ou un tel modèle, et qui le met sur le marché ou le met en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit. Cette qualification recouvre principalement les éditeurs de solutions d'IA, qu'il s'agisse de grands acteurs technologiques, de regtechs spécialisées ou, dans certaines hypothèses, d'établissements financiers ayant développé en interne une solution qu'ils diffusent ensuite à d'autres entités.

Le déployeur, au sens de l'article 3 point 4, est la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme utilisant un système d'IA sous sa propre autorité, sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle non professionnelle. La majorité des banques, des fintechs, des compagnies d'assurance et des prestataires de services sur crypto-actifs qui intègrent un outil tiers à leur dispositif de conformité se rangent dans cette catégorie.

Le cumul des deux qualifications est possible, et même fréquent en pratique. Un même établissement peut se trouver simultanément fournisseur, pour la part qu'il développe ou personnalise substantiellement, et déployeur, pour la part qu'il consomme tel quel. Chaque cas d'usage doit donc faire l'objet d'une qualification individualisée, fondée sur l'analyse fine de la production, de la mise sur le marché et de l'utilisation du système. Cette qualification conditionne en cascade l'ensemble des obligations applicables, et toute erreur d'aiguillage initial entraîne des conséquences en chaîne.

1.5 Le régime spécifique des modèles d'IA à usage général

Les articles 51 à 56 du règlement, applicables depuis le 2 août 2025, instaurent un régime dédié aux modèles d'intelligence artificielle à usage

général, communément désignés par l'acronyme GPAI pour General-Purpose AI. Le texte distingue les GPAI standards des GPAI à risque systémique.

La présomption de risque systémique s'attache, en application de l'article 51 paragraphe 2, aux modèles dont la quantité cumulée de calcul d'entraînement, mesurée en opérations en virgule flottante, dépasse 10^{25} FLOP. Ce seuil correspond actuellement à un petit nombre de modèles de pointe au niveau mondial, principalement développés par les acteurs technologiques majeurs.

Les fournisseurs de GPAI standards sont tenus, en application de l'article 53, de produire une documentation technique du modèle, d'informer les fournisseurs en aval qui intègrent leur modèle dans des systèmes d'IA, de mettre en place une politique de respect du droit d'auteur et de publier un résumé suffisamment détaillé des données utilisées pour l'entraînement. Les fournisseurs de GPAI à risque systémique sont, en application de l'article 55, soumis à des obligations renforcées d'évaluation des modèles selon des protocoles harmonisés, d'atténuation des risques systémiques, de notification au Bureau européen de l'IA des incidents graves et de cybersécurité du modèle et de son infrastructure.

La pertinence concrète de ce régime pour la conformité financière tient à la consommation croissante de modèles de fondation tiers à des fins de conformité : rédaction de notes typologiques, synthèse de dossiers de vigilance, copilotes pour les analystes, automatisation de revues de presse adverse. La frontière entre simple consommation d'un GPAI et reclassification de l'utilisateur en fournisseur, par exemple en cas de modification substantielle du modèle ou de mise à disposition à des tiers, doit être expertisée au cas par cas. Cette question est aussi celle de la dépendance technologique stratégique, dont la dimension géopolitique ne saurait être négligée à l'heure des grands modèles à dominante extra-européenne.

1.6 Sanctions, calendrier et littératie transversale

L'article 99 du règlement gradue les sanctions de manière proportionnée à la gravité des manquements. Les manquements aux pratiques interdites sont sanctionnés à hauteur de 35 millions d'euros ou 7 pour cent du chiffre d'affaires mondial. Les manquements aux obligations applicables aux systèmes à haut risque et aux modèles GPAI sont sanctionnés à hauteur de 15 millions ou 3 pour cent. La fourniture d'informations inexactes, incomplètes ou trompeuses aux autorités notifiées, aux autorités

compétentes nationales ou au Bureau européen de l'IA est sanctionnée à hauteur de 7,5 millions ou 1 pour cent. Dans tous les cas, le montant le plus élevé est retenu.

Le calendrier d'application, fixé par l'article 113, est strictement progressif. Les pratiques interdites et la littératie en IA s'appliquent depuis le 2 février 2025. Les obligations relatives aux modèles GPAI et la gouvernance sont applicables depuis le 2 août 2025. L'application générale, en particulier pour les systèmes à haut risque visés à l'annexe III, interviendra le 2 août 2026. L'extension aux systèmes à haut risque rattachés aux produits visés à l'annexe I est fixée au 2 août 2027. Ce calendrier ménage aux établissements un temps d'adaptation appréciable, à condition de l'utiliser pour structurer méthodiquement la conformité plutôt que de différer l'effort.

L'article 4 du règlement, en vigueur depuis le 2 février 2025, mérite une mention particulière. Il impose à tous les fournisseurs et déployeurs de systèmes d'intelligence artificielle de prendre les mesures nécessaires pour garantir un niveau suffisant de maîtrise de l'IA pour leur personnel et pour les personnes opérant les systèmes pour leur compte. Cette obligation transversale s'applique indépendamment de la qualification haut risque du système et concerne donc immédiatement les équipes de conformité financière, dès lors qu'elles utilisent ou supervisent un outil d'intelligence artificielle. Aucun établissement ne peut donc se prévaloir d'un temps d'attente sur ce point.

02. La qualification des systèmes d'IA en LCB-FT

L'exclusion centrale de l'annexe III point 5 b), ses quatre précisions, le sort des systèmes hybrides et la frontière à surveiller.

2.1 Le point central : l'exclusion de l'annexe III, point 5 b)

Le contresens le plus structurant que nous avons rencontré dans les directions conformité de plusieurs établissements consiste à supposer que tout outil d'intelligence artificielle déployé en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme entre, par défaut, dans la catégorie des systèmes à haut risque de l'AI Act. Cette lecture, qui circule dans certaines publications regtech et dans plusieurs notes internes auxquelles nous avons eu accès, est inexacte. Le texte du règlement dit exactement le contraire.

L'annexe III, point 5 b), du règlement (UE) 2024/1689 vise expressément les systèmes destinés à être utilisés pour évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit. Mais la rédaction ajoute immédiatement : *« à l'exception des systèmes d'IA utilisés à des fins de détection de fraude financière »*. Cette exclusion n'est pas une exception interprétative ni un tempérament jurisprudentiel : elle figure dans le texte même de l'annexe et a été insérée par le législateur européen en pleine conscience de la spécificité du secteur financier.

Le considérant 58 du règlement justifie cette non-qualification haut risque par la nécessité de ne pas entraver les outils servant à la détection de la fraude financière et les outils prudentiels utilisés notamment pour le calcul des exigences de fonds propres des établissements de crédit et des entreprises d'assurance contre le risque de crédit et le risque opérationnel. Le législateur européen a donc consciemment ménagé un espace de licéité, conscient que la dramatisation excessive de la qualification haut risque aurait pour effet contre-productif de freiner les outils dont la finalité même est de renforcer la conformité.

Cette lecture a été confirmée par l'Autorité de contrôle prudentiel et de résolution dans sa publication institutionnelle « AI Act », dans laquelle elle précise que la qualification haut risque vise l'évaluation de la solvabilité « *hors lutte contre la fraude* », position réaffirmée publiquement lors de la réunion de Place du 17 septembre 2025 devant l'ensemble des acteurs financiers de la place. À notre connaissance, aucune doctrine européenne contraire n'a été publiée à ce jour.

2.2 Les quatre précisions de bon aloi

Cette exclusion expresse appelle néanmoins quatre précisions, qui en délimitent strictement la portée.

Première précision, relative à l'exclusivité d'usage. L'exclusion ne couvre que les systèmes effectivement et exclusivement consacrés à la détection de la fraude et au dispositif LCB-FT. Un système qui mêlerait à cette finalité une fonction d'évaluation de solvabilité, ou qui influencerait directement la décision d'accès au crédit ou les conditions tarifaires, retomberait dans le périmètre haut risque pour la fonction concernée. L'architecture interne du système devient ici un sujet de qualification juridique au plus haut niveau, et la documentation technique doit pouvoir démontrer le cantonnement effectif de la finalité.

Deuxième précision, relative à la neutralisation par le profilage. La dérogation de l'article 6, paragraphe 3, qui permet d'écarter la qualification haut risque pour les systèmes ne présentant pas de risque important, ne s'applique pas lorsque le système effectue un profilage de personnes physiques au sens du RGPD. Dès lors que la finalité LCB-FT comporte un profilage individualisé, la prudence interprétative commande un alignement volontaire sur les exigences haut risque, ou à tout le moins une vigilance renforcée sur la documentation, le contrôle humain et la transparence.

Troisième précision, relative au périmètre strictement limité à l'AI Act. L'exclusion vaut uniquement pour la qualification au sens du règlement IA. Elle ne dispense ni du RGPD, ni des obligations sectorielles propres à la lutte contre le blanchiment, ni du régime de résilience opérationnelle numérique de DORA. Autrement dit, l'exclusion ne libère pas, elle reconfigure : la grammaire de la conformité change, mais le volume des obligations à respecter ne diminue pas significativement.

Quatrième précision, relative à la frontière entre fraude financière et fraude au paiement. La rédaction du règlement se borne à exclure la détection de fraude financière sans définir ce qu'elle recouvre exactement. La frontière avec la fraude transactionnelle commerciale, avec la fraude au paiement entendue au sens de la directive sur les services de paiement, ou encore avec certaines hypothèses de fraude documentaire, est susceptible d'évoluer au gré de la doctrine européenne et des premières lignes directrices du Bureau européen de l'IA. La vigilance des établissements doit donc rester active sur cette zone interprétative.

2.3 Les systèmes hybrides et le risque de requalification

Les systèmes hybrides constituent, en pratique, la principale source de difficulté qualificative. Nombre d'outils déployés dans le secteur financier combinent plusieurs finalités : détection de fraude et scoring de solvabilité, vigilance LCB-FT et appétence commerciale, screening transactionnel et tarification dynamique. Ces combinaisons sont souvent justifiées par des considérations d'efficience opérationnelle ou de mutualisation des coûts de développement, mais elles posent un problème de qualification au regard de l'AI Act.

La méthode que nous recommandons consiste à procéder à une qualification fonctionnelle différenciée. Pour chaque fonction du système, l'établissement doit déterminer si elle relève d'une catégorie haut risque (notamment la fonction crédit ou tarification assurantielle), d'une fonction exclue (notamment la détection de fraude au sens strict), ou d'une fonction relevant d'un autre régime (transparence ou risque minimal). Cette qualification différenciée appelle une architecture technique qui permette de cloisonner les flux et de documenter le périmètre de chaque finalité, afin de justifier auprès du superviseur ou, le cas échéant, du juge, la qualification retenue.

À défaut de cloisonnement effectif, la prudence interprétative commande de traiter l'ensemble du système comme relevant du régime haut risque pour la part qui influe sur les décisions sensibles (crédit, tarification, exclusion). Cette approche conservatrice évite tout risque de requalification a posteriori par le superviseur, mais elle suppose une acceptation des contraintes documentaires et organisationnelles correspondantes.

2.4 La frontière à surveiller entre fraude financière et fraude au paiement

La rédaction de l'exclusion de l'annexe III, point 5 b), utilise les termes de *détection de fraude financière »*, sans définition complémentaire ni renvoi à un autre instrument réglementaire qui en préciserait le champ. Cette absence de définition expresse soulève une question d'interprétation que la doctrine européenne sera amenée à trancher dans les prochains mois.

La position que nous défendons consiste à retenir une lecture large de la fraude financière, englobant non seulement les schémas de blanchiment des capitaux et de financement du terrorisme au sens du paquet AML/CFT et du droit français LCB-FT, mais également la fraude au paiement au sens de la deuxième directive sur les services de paiement, certaines hypothèses de fraude documentaire et de fraude à l'identité, et la lutte contre les abus

de marché au sens du règlement (UE) 596/2014. Cette lecture large a pour mérite de couvrir l'ensemble des outils d'IA utilisés à des fins de protection du système financier contre les comportements illicites, sans introduire de distinctions artificielles entre des fraudes connexes.

Une lecture restrictive est cependant envisageable, qui limiterait l'exclusion aux seules hypothèses de blanchiment et de financement du terrorisme stricto sensu, à l'exclusion des autres formes de fraude. Cette interprétation, qui résulterait d'une lecture littérale combinée du considérant 58 et de l'annexe III, aurait pour effet de faire retomber dans le périmètre haut risque les outils de détection de fraude au paiement, ce qui paraît contraire à l'esprit du texte. Nous estimons donc que la lecture large doit prévaloir, mais nous recommandons aux établissements de documenter avec soin leur choix interprétatif, dans l'attente d'une clarification doctrinale formelle.

03. Les obligations qui demeurent au titre de l'AI Act

Littératie, transparence, obligations du déployeur et articulation avec l'article 22 du RGPD à la lumière de l'arrêt SCHUFA Holding.

3.1 La littératie effective des équipes (article 4)

L'article 4 du règlement (UE) 2024/1689 impose à tous les fournisseurs et déployeurs de systèmes d'intelligence artificielle de prendre les mesures nécessaires pour garantir un niveau suffisant de maîtrise de l'IA pour leur personnel et pour les personnes opérant les systèmes pour leur compte. Cette obligation transversale, en vigueur depuis le 2 février 2025, s'applique indépendamment de la qualification haut risque du système et concerne donc immédiatement les équipes de conformité financière.

La notion de maîtrise de l'IA, telle qu'elle ressort du considérant 20 du règlement, vise les compétences techniques, l'expérience, l'éducation et la formation, ainsi que le contexte dans lequel les systèmes d'IA doivent être utilisés. Il s'agit donc d'une notion plurielle, qui ne se réduit pas à une formation théorique sur l'AI Act mais englobe la compréhension fonctionnelle des systèmes effectivement déployés, de leurs limites, de leurs biais potentiels et des mesures correctives applicables.

La mise en œuvre concrète de l'article 4 suppose, dans un établissement financier, plusieurs actions cumulatives. Premièrement, une cartographie des fonctions et des rôles susceptibles d'interagir avec un système d'IA en LCB-FT (analystes de premier niveau, superviseurs, contrôle interne, responsables conformité, direction). Deuxièmement, un programme de formation différencié selon les rôles, qui ne se contente pas d'une session générique mais aborde les cas d'usage spécifiques à l'établissement. Troisièmement, une documentation interne accessible, qui décrit le fonctionnement des outils déployés et les modalités de leur supervision. Quatrièmement, une gouvernance pérenne, qui prévoit la mise à jour régulière des compétences à mesure que les systèmes évoluent.

3.2 La transparence des systèmes d'IA générative (articles 50 et suivants)

Les articles 50 et suivants du règlement organisent un régime de transparence pour les systèmes d'intelligence artificielle interagissant avec des personnes physiques ou générant des contenus synthétiques. Ce régime s'applique indépendamment de la qualification haut risque et

concerne donc, en pratique, la plupart des copilotes d'IA générative déployés en LCB-FT.

L'article 50 paragraphe 1 impose au fournisseur d'un système destiné à interagir directement avec des personnes physiques de concevoir et de développer ce système de manière à ce que les personnes concernées soient informées qu'elles interagissent avec un système d'IA, sauf lorsque cela est évident pour une personne raisonnablement attentive. L'article 50 paragraphe 2 impose aux fournisseurs de systèmes d'IA générative produisant des contenus synthétiques (texte, image, audio, vidéo) de marquer ces contenus de manière lisible et détectable par machine. L'article 50 paragraphe 4 impose aux déployeurs de systèmes générateurs ou manipulateurs de texte publié dans l'intérêt public sur des questions d'intérêt général de divulguer le caractère artificiellement généré ou manipulé du texte.

En LCB-FT, l'application de ces obligations vise principalement les copilotes utilisés pour la rédaction de notes typologiques, la synthèse de dossiers de vigilance ou la préparation de projets de déclaration de soupçon. Les utilisateurs internes (analystes, superviseurs) qui interagissent avec ces copilotes doivent savoir qu'ils dialoguent avec un système d'IA, et les contenus générés doivent être identifiables comme tels dans la documentation interne. Cette exigence n'interdit en aucune manière l'usage de ces outils, mais elle structure leur intégration dans les processus de conformité.

3.3 Les obligations du déployeur (articles 26 et 27)

L'article 26 du règlement fixe les obligations générales du déployeur d'un système d'IA à haut risque, lesquelles sont susceptibles de s'appliquer aux établissements financiers dès lors qu'une fonction de leur système y est rattachée. Ces obligations recouvrent l'utilisation conforme aux instructions du fournisseur, l'organisation d'une supervision humaine par des personnes physiques disposant des compétences, de la formation et de l'autorité nécessaires, la pertinence et la représentativité des données d'entrée que le déployeur contrôle, la journalisation automatique pendant la durée du fonctionnement du système, l'information du personnel exposé, et la notification des risques sérieux.

L'article 27 impose, dans certaines hypothèses limitativement énumérées, une analyse d'impact sur les droits fondamentaux préalable à la mise en service d'un système haut risque. Cette analyse, distincte de l'analyse d'impact relative à la protection des données prévue à l'article 35 du RGPD,

doit couvrir la description des procédures dans lesquelles le système est utilisé, la durée et la fréquence d'utilisation, les catégories de personnes physiques susceptibles d'être affectées, les risques spécifiques de préjudice et les mesures d'atténuation prévues, ainsi que les mesures à prendre en cas de matérialisation d'un risque.

Pour les systèmes d'IA en LCB-FT bénéficiant de l'exclusion de l'annexe III, point 5 b), les articles 26 et 27 ne s'appliquent pas directement. En revanche, si une fonction du système retombe par exception en haut risque (par exemple en cas d'hybridation avec une fonction crédit), ces obligations se réveillent et doivent être appliquées pour la part concernée. La frontière qualitative est ici essentielle, et elle conditionne le périmètre des diligences à conduire.

3.4 L'articulation avec l'article 22 du RGPD à la lumière de SCHUFA

L'article 22 du règlement général sur la protection des données interdit en principe les décisions exclusivement automatisées, y compris le profilage, produisant des effets juridiques significatifs sur la personne concernée ou l'affectant de manière similaire. Cette interdiction connaît trois exceptions : la nécessité à l'exécution ou à la conclusion d'un contrat, l'autorisation par le droit de l'Union ou par le droit national de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, ou le consentement explicite de la personne concernée.

La portée de l'article 22 a été clarifiée par la Cour de justice de l'Union européenne dans son arrêt SCHUFA Holding du 7 décembre 2023, affaire C-634/21[6]. La Cour a qualifié l'établissement d'un score de crédit automatisé de décision individuelle automatisée au sens de l'article 22, dès lors qu'il joue un rôle déterminant dans la décision finale, même lorsqu'une personne physique valide formellement le résultat. Cette lecture extensive a des conséquences directes pour la conformité financière : tout score algorithmique dont la formulation a vocation à emporter de facto la décision (clôture, refus d'entrée en relation, gel d'opération) entre dans le périmètre de l'article 22, indépendamment de la qualification haut risque ou non au sens de l'AI Act.

[6]CJUE, 7 décembre 2023, SCHUFA Holding AG, aff. C-634/21, ECLI:EU:C:2023:957. La Cour qualifie de décision individuelle automatisée au sens de l'article 22 du RGPD l'établissement d'un score automatisé dès lors qu'il joue un rôle déterminant dans la décision finale, même en présence d'une validation humaine formelle.

Cette articulation appelle, dans la pratique opérationnelle, une vigilance particulière. Le déployeur doit, au titre du RGPD, fournir à la personne concernée des informations significatives sur la logique du traitement automatisé, l'importance des conséquences prévues et les modalités de recours. Mais l'article L. 561-19 du code monétaire et financier protège la confidentialité de la déclaration de soupçon adressée à TRACFIN, et interdit en principe d'informer la personne concernée du fait qu'une telle déclaration a été effectuée ou est envisagée. La conciliation de ces deux exigences constitue l'un des points les plus délicats de la pratique opérationnelle actuelle, et appelle une rédaction très soignée des mentions d'information et des protocoles de réponse aux demandes d'accès des personnes concernées.

04. Cas d'usage et qualifications pratiques

Application de la grille théorique à quatre cas d'usage représentatifs : copilote génératif, filtrage transactionnel, scoring LCB-FT, KYC perpétuel.

4.1 Le copilote d'IA générative pour la rédaction des déclarations de soupçon

Le copilote d'IA générative déployé en LCB-FT a vocation à assister les analystes dans la rédaction des notes typologiques, des projets de déclaration de soupçon et des synthèses de dossiers de vigilance. Il s'appuie généralement sur un modèle de fondation tiers, intégré à l'environnement de travail de l'analyste, qui produit des contenus à partir des éléments du dossier et de typologies préchargées.

Sur le plan qualificatif, ce copilote relève principalement du régime applicable aux modèles d'IA à usage général, sous la qualité de déployeur de l'établissement utilisateur. Il ne relève pas, par défaut, du régime haut risque, dès lors qu'il ne procède à aucune évaluation de solvabilité ni à aucune décision automatisée affectant directement la personne concernée. L'établissement reste néanmoins soumis aux obligations de l'article 4 sur la littératie, de l'article 50 sur la transparence à l'égard des destinataires internes qui doivent savoir qu'ils interagissent avec un système d'IA générative, et aux exigences du RGPD pour le transfert des données personnelles à un éventuel sous-traitant extra-européen.

Le rappel essentiel à intégrer dans la gouvernance interne est que la responsabilité de la déclaration de soupçon, en application de l'article L. 561-15 du code monétaire et financier, demeure exclusivement humaine. Aucun système d'IA, aussi performant soit-il, ne peut produire une déclaration en lieu et place de l'analyste humain qui en porte la responsabilité finale. Le copilote est un outil d'aide à la rédaction et à la synthèse, non un substitut au jugement professionnel.

4.2 Les outils de filtrage des transactions et de screening

Les outils de filtrage des transactions et de screening visent à identifier, en temps réel ou en différé, les opérations qui présentent des caractéristiques atypiques au regard du profil du client, des règles de seuil applicables, des listes de sanctions internationales et des typologies de blanchiment connues. Ils sont au cœur du dispositif LCB-FT des établissements financiers et constituent le cas d'usage IA le plus répandu dans le secteur.

Sur le plan qualificatif, ces outils bénéficient pleinement de l'exclusion de l'annexe III, point 5 b), dès lors qu'ils sont exclusivement consacrés à la détection de la fraude financière et au dispositif LCB-FT. Le bénéfice de l'exclusion suppose une consécration effective et exclusive : un outil qui mêlerait au filtrage transactionnel des fonctions de scoring commercial ou d'évaluation de l'appétence à un crédit retomberait dans le périmètre haut risque pour la part concernée.

Le régime applicable est donc principalement celui des obligations résiduelles : littératie de l'article 4, transparence à l'égard des analystes internes, articulation avec l'article 22 du RGPD pour les décisions emportant de facto la conséquence d'une mesure (gel, retenue, retard de traitement). À ces obligations s'ajoutent évidemment les obligations sectorielles propres à la LCB-FT, qui ne sont pas affectées par la qualification au regard de l'AI Act.

4.3 Les outils de scoring de risque LCB-FT

Les outils de scoring de risque LCB-FT attribuent à chaque client, sur la base d'un ensemble de variables, une note de risque qui conditionne l'intensité des mesures de vigilance applicables. Ils permettent d'optimiser l'allocation des ressources d'analyse en concentrant l'attention sur les profils les plus exposés.

Sur le plan qualificatif, ces outils bénéficient de l'exclusion de l'annexe III, point 5 b), à condition qu'ils soient effectivement et exclusivement consacrés à la finalité LCB-FT. Une attention particulière doit être portée à la dérogation de l'article 6, paragraphe 3, qui ne s'applique pas en cas de profilage individualisé au sens du RGPD. Or, par nature, le scoring de risque LCB-FT comporte un profilage individualisé : la prudence interprétative commande donc, à tout le moins, une vigilance renforcée sur la documentation, le contrôle humain et la traçabilité des décisions.

L'articulation avec l'article 22 du RGPD est ici particulièrement aiguë. Lorsque le score conditionne mécaniquement l'application d'une mesure (par exemple le passage en vigilance renforcée, la clôture, ou le gel d'opération), il joue un rôle déterminant dans la décision finale au sens de l'arrêt SCHUFA Holding, et active donc l'article 22 du RGPD avec ses exigences propres (information, droit de contester, intervention humaine). La conciliation avec la confidentialité de la déclaration de soupçon protégée par l'article L. 561-19 du code monétaire et financier doit faire l'objet d'une rédaction soignée des mentions d'information et des protocoles de réponse aux demandes d'accès.

4.4 Les outils de KYC perpétuel ou pKYC

Le KYC perpétuel, communément désigné par l'acronyme pKYC pour perpetual know your customer, consiste à substituer à la vigilance par événement (révision périodique du dossier client à dates fixes ou en cas de modification connue) une vigilance par flux continu, alimentée en temps réel par des signaux issus du système d'information de l'établissement et appréciée par un dispositif algorithmique de scoring dynamique.

Cette pratique professionnelle, encore non normée à ce jour mais déjà largement déployée dans le secteur, s'inscrit dans la trajectoire ouverte par le règlement AMLR pour les standards futurs et par la doctrine européenne sur l'efficacité du dispositif LCB-FT. Sa qualification au regard de l'AI Act suit la même logique que celle des outils de scoring de risque LCB-FT : exclusion de l'annexe III, point 5 b), sous réserve d'une finalité exclusive ; vigilance sur la dérogation de l'article 6, paragraphe 3, en présence d'un profilage individualisé ; articulation rigoureuse avec l'article 22 du RGPD.

La spécificité du pKYC tient à la temporalité de la décision. Là où le scoring statique produit une note à un instant donné, le pKYC produit des notes en flux continu, ce qui multiplie les hypothèses dans lesquelles une décision automatisée peut être réputée déterminante. La gouvernance interne doit donc prévoir des seuils de déclenchement précis, des protocoles de revue humaine systématique pour les décisions sensibles, et une journalisation exhaustive permettant la reconstitution des chaînes décisionnelles.

05. Gouvernance interne et conformité IA by design

Cartographie des systèmes déployés, gouvernance des données et documentation des choix, contrôle humain effectif et traçabilité décisionnelle.

5.1 La cartographie des systèmes d'IA déployés

La première étape de la conformité IA opérationnelle consiste à dresser une cartographie exhaustive des systèmes d'intelligence artificielle déployés dans l'établissement, qu'ils soient développés en interne ou consommés auprès de tiers. Cette cartographie doit recenser, pour chaque système, sa finalité fonctionnelle, son rattachement à une catégorie de qualification AI Act, la qualité de l'établissement à son égard (fournisseur ou déployeur), le ou les modèles d'IA sous-jacents, les flux de données qui l'alimentent, et le périmètre des décisions qu'il influence ou qu'il prend.

La cartographie n'est pas un livrable ponctuel mais un outil de gouvernance vivant. Elle doit être tenue à jour à chaque déploiement, à chaque mise à jour substantielle d'un système existant et à chaque évolution de la doctrine réglementaire. Elle constitue le fondement de la documentation à produire au superviseur en cas de contrôle, et elle alimente le dispositif de contrôle interne et la cellule conformité.

5.2 La gouvernance des données et la documentation des choix

La gouvernance des données utilisées pour entraîner, valider et tester un système d'IA est au cœur de l'AI Act et fait l'objet, pour les systèmes haut risque, des exigences détaillées de l'article 10. Mais, indépendamment de la qualification, la qualité des données conditionne l'efficacité opérationnelle, la pertinence statistique et la défense juridique du système.

Cette gouvernance suppose plusieurs actions structurantes. Premièrement, la documentation de la provenance des données, de leur licéité d'usage au regard du RGPD et des éventuels accords contractuels avec les sources externes. Deuxièmement, l'analyse de la représentativité statistique des jeux d'entraînement, et la documentation des biais potentiels ainsi que des mesures correctives apportées. Troisièmement, la traçabilité des versions des données utilisées à chaque étape, ce qui suppose un dispositif de versionning rigoureux. Quatrièmement, la documentation des choix méthodologiques retenus pour le développement et le paramétrage du modèle, qui doit être accessible aux équipes conformité et au contrôle interne.

5.3 Le contrôle humain effectif et la traçabilité décisionnelle

Le contrôle humain effectif, principe consacré par l'article 14 du règlement pour les systèmes haut risque, irrigue plus largement la doctrine européenne, y compris pour les systèmes qui n'entrent pas formellement dans cette qualification. La jurisprudence SCHUFA Holding a confirmé que ce contrôle ne se réduisait pas à une validation formelle a posteriori, mais devait inclure la possibilité effective pour la personne physique de comprendre les capacités et limites du système, de surveiller son fonctionnement, de déceler et de corriger les biais, et le cas échéant d'interrompre son utilisation.

La mise en œuvre opérationnelle de ce contrôle suppose des actions concrètes. Désignation d'une personne physique référente pour chaque système d'IA en LCB-FT déployé, disposant des compétences, de la formation et de l'autorité nécessaires. Documentation des seuils et des règles de déclenchement d'une revue humaine systématique. Journalisation exhaustive des décisions automatisées, avec horodatage, identifiant du système, version du modèle, données d'entrée et résultats produits. Protocole de revue périodique des performances du système, de ses biais éventuels et de l'adéquation de ses paramètres aux objectifs de conformité.

06. Recommandations opérationnelles

Actions différenciées à conduire dans les douze prochains mois selon les fonctions de l'organisation.

6.1 Pour les directions conformité

Pour les directions conformité des établissements financiers, plusieurs chantiers s'imposent dans les douze prochains mois. Le déploiement effectif d'un programme de littératie en IA pour l'ensemble du personnel de la fonction, en application directe de l'article 4 du règlement et conformément aux orientations qui se dégageront du Comité européen de l'IA. L'établissement d'une cartographie complète des systèmes d'intelligence artificielle déployés ou en projet de déploiement en LCB-FT, avec qualification fonctionnelle au regard de l'AI Act. La révision des procédures internes de gestion des alertes pour intégrer la dimension IA, et notamment les exigences de traçabilité, de contrôle humain et d'explicabilité.

La direction conformité doit également engager un dialogue structuré avec la direction des systèmes d'information et avec les éditeurs des outils déployés. Ce dialogue doit porter sur la documentation technique des systèmes, sur leur qualification au regard de l'AI Act, sur les engagements contractuels en matière de mise à jour réglementaire et sur les modalités de coopération en cas de contrôle par le superviseur. Les contrats existants avec les éditeurs de regtech doivent faire l'objet d'une revue systématique au regard des exigences du règlement.

6.2 Pour les directions juridiques

Pour les directions juridiques, le chantier principal consiste à structurer la gouvernance contractuelle de l'intelligence artificielle. Cela suppose la rédaction ou la révision des clauses contractuelles types applicables aux fournisseurs de systèmes d'IA, intégrant les engagements de conformité à l'AI Act, les garanties documentaires, les droits d'audit, les obligations d'information en cas d'évolution réglementaire, et les modalités de coopération en cas de contrôle.

La direction juridique est également en première ligne sur l'articulation entre l'AI Act et le RGPD, en particulier sur la portée de l'article 22 du RGPD à la lumière de l'arrêt SCHUFA Holding. Elle doit rédiger les mentions d'information à destination des personnes concernées, en veillant à concilier la transparence due au titre du RGPD avec la confidentialité de

la déclaration de soupçon protégée par l'article L. 561-19 du code monétaire et financier. Cette rédaction est délicate et appelle souvent l'intervention d'un conseil externe spécialisé.

6.3 Pour les directions générales

Pour les directions générales, l'enjeu principal est celui de la prise en compte stratégique de la conformité IA dans les décisions d'investissement et de transformation. La conformité IA ne doit pas être perçue comme une charge à minimiser, mais comme un avantage concurrentiel à construire. Les établissements qui auront, à horizon 2027-2028, internalisé la conformité IA dans la conception même de leurs systèmes (compliance by design) disposeront d'un atout significatif face aux régulateurs et face aux clients institutionnels qui exigent désormais des garanties documentées sur ces sujets.

La direction générale doit veiller à inscrire la conformité IA dans le pilotage stratégique de l'établissement, à doter les directions concernées des moyens nécessaires (budgétaires, humains, technologiques), et à arbitrer les conflits d'allocation entre la conformité IA, la conformité LCB-FT, la résilience opérationnelle et la transformation digitale. Ces arbitrages, lorsqu'ils ne sont pas explicites, se traduisent fréquemment par des dysfonctionnements opérationnels et par des risques de sanction qui auraient pu être évités.

CONCLUSION

Le rendez-vous *du 2 août 2026*

Le règlement (UE) 2024/1689 ne se contente pas d'ajouter une nouvelle couche normative au dispositif déjà dense de la conformité financière. Il transforme le rapport entre l'établissement et les outils technologiques qu'il déploie, en faisant de leur conception même un objet de droit. Cette mutation est d'autant plus structurante qu'elle s'inscrit dans le prolongement d'autres mouvements convergents : le paquet AML/CFT du 31 mai 2024, le règlement DORA, la révision en cours du règlement général sur la protection des données à l'aune des nouvelles technologies, et les standards internationaux émergents.

Pour autant, cette mutation n'est pas une fatalité contraignante. Elle est une opportunité de structurer rigoureusement une conformité IA qui, à terme, constituera un facteur différenciant entre les établissements. Ceux qui auront, à horizon 2027, achevé leur cartographie, formalisé leur gouvernance, structuré leur documentation et formé leurs équipes, disposeront d'un avantage stratégique sur ceux qui auront différé l'effort.

Le rendez-vous du 2 août 2026, date d'application générale des systèmes haut risque visés à l'annexe III, ne doit donc pas être appréhendé comme un cap réglementaire à franchir, mais comme un jalon dans une démarche continue d'intégration de l'intelligence artificielle dans la conformité financière. Notre cabinet accompagne les établissements dans cette démarche, depuis la qualification initiale des systèmes jusqu'à la défense des positions retenues devant le superviseur, en passant par la structuration contractuelle, la formation des équipes et l'articulation rigoureuse avec les autres pans de la réglementation applicable.

La recommandation stratégique est sans ambiguïté : agir tôt, structurer méthodiquement, documenter rigoureusement, anticiper les évolutions plutôt que les subir.

HASHTAG AVOCATS

Présentation du cabinet et contacts

Hashtag Avocats est un cabinet d'avocats parisien et luxembourgeois (Toque D1675) intervenant aux barreaux de Paris et de Luxembourg. Le cabinet se distingue par une expertise reconnue dans les matières de droit du numérique, intelligence artificielle, blockchain et crypto-actifs, régulation financière (MiCA, DORA, AIFM, supervision AMF et ACPR), corporate, propriété intellectuelle et IT, protection des données et droit social.

Il intervient en synergie avec Hashtag Finance, structure dédiée à la direction administrative et financière externalisée, au pilotage financier et aux services de transaction, ce qui permet d'offrir aux fonds d'investissement, à leurs participations et aux entreprises de l'écosystème un accompagnement intégré, depuis la structuration jusqu'à l'exécution des opérations.

L'équipe Hashtag Avocats accompagne les établissements financiers, les fintechs et les prestataires de services sur crypto-actifs dans l'ensemble du cycle de leur conformité, depuis la qualification initiale au regard de l'AI Act, MiCA et DORA, jusqu'à la mise en conformité aux régimes prudentiel et anti-blanchiment, en passant par la formation des équipes, la défense devant les autorités de régulation et la rédaction de la documentation contractuelle pertinente.

CONTACT DIRECT

Arnaud Touati

Avocat Associé Fondateur

Barreaux de Paris et de Luxembourg

a.touati@hashtagavocats.com

CABINET

SELARL Hashtag Avocats

51, avenue Franklin Delano Roosevelt, 75008 Paris

Toque D1675

Téléphone : +33 1 85 73 56 66

Courriel : contact@hashtagavocats.com

Site internet : www.hashtagavocats.com