Crypto, TradFi & Digital

Spécial AI : fragmentation réglementaire mondiale

Décrypter la réglementation financière, IA et données pour anticiper, se conformer et décider

Cinq géographies, cinq réponses : l'IA et les données personnelles en tension mondiale

Les éditions précédentes du Regulatory Brief ont accompagné pas à pas la montée en application du cadre européen : l'AI Act et son Omnibus (Éditions #7, #18), son articulation avec le RGPD (Édition #8), la convergence IA × cybersécurité (Édition #11), l'accélération réglementaire mondiale de l'IA en juillet 2026 (Édition #15), le vote du Parlement européen sur les stablecoins (Édition #16), la recommandation CNIL sur les pixels de suivi (Édition #19) et la clarification ESMA-AMF du périmètre du conseil sur crypto-actifs sous MiCA (Édition #20). Cette vingt-et-unième édition prolonge la logique en portant sur un moment particulièrement dense : la seconde quinzaine d'août 2026, au cours de laquelle cinq géographies réglementaires majeures que sont l'Union européenne, les États-Unis, la Corée du Sud, la Chine et la France dans son articulation nationale, ont pris des positions coordonnées ou divergentes sur l'IA et la protection des données personnelles.

Cinq événements sont à mettre en perspective. Le 17 août 2026, la CNIL a publié la mise à jour de sa FAQ sur l'articulation entre l'AI Act et le RGPD, en intégrant les conséquences du règlement européen dit « Digital Omnibus on AI », texte adopté le 8 juillet 2026, publié le 24 juillet et entré en vigueur le 27 juillet. Le 18 août 2026, le règlement européen 2023/1543 relatif aux preuves électroniques (« e-Evidence ») est devenu directement applicable dans l'ensemble de l'Union. Le 19 août 2026, la Federal Trade Commission américaine a soumis à consultation publique un projet de doctrine sur la tarification personnalisée fondée sur les données personnelles ; la même journée, l'autorité chinoise du cyberespace (CAC) a publié un bilan intermédiaire de ses opérations de contrôle de la vie privée sur plus de 20 000 applications. Le 20 août 2026, l'Assemblée nationale de Corée du Sud a adopté un amendement à la loi coréenne sur la protection des informations personnelles (PIPA) créant une base légale spécifique et conditionnelle pour l'entraînement des

modèles d'IA ; le même jour, les mesures chinoises d'évaluation des risques de sécurité des données du réseau sont entrées en vigueur.

Lues ensemble, ces cinq publications documentent une réalité que le Regulatory Brief a régulièrement anticipée : la gouvernance mondiale de l'IA et des données personnelles se construit désormais dans une tension permanente entre convergence (mêmes préoccupations, mêmes principes) et fragmentation (approches, calendriers, degrés de contrainte très différents). Pour les acteurs financiers, les responsables de la conformité, les DPO, les directions juridiques, les DSI et les investisseurs institutionnels à empreinte internationale, cette fragmentation devient un paramètre stratégique, au même titre que le risque de marché ou le risque cyber.

Cette édition propose une lecture géographique de la séquence, avec un dernier focus sur ce qu'elle change concrètement pour les acteurs européens.

Le signal faible

La fragmentation réglementaire mondiale n'est plus un décalage temporel entre juridictions ; elle devient un choix de doctrine assumé : cinq géographies, cinq réponses différentes à des enjeux essentiellement identiques.

Ce qui frappe dans la séquence du 17 au 20 août 2026, c'est moins la coïncidence chronologique des publications que la structure de leurs approches. L'Union européenne consolide son cadre par la clarification opérationnelle (CNIL) et étend son bras armé transfrontalier par un texte devenu directement applicable (e-Evidence). Les États-Unis explorent, par la voie de la consultation publique, une régulation lente et négociée d'une pratique qu'ils ne prétendent pas interdire (la tarification personnalisée). La Corée du Sud construit un régime intermédiaire, ni interdiction ni autorisation générale, mais une autorisation conditionnelle et supervisée. La Chine articule contrôle centralisé (mesures d'évaluation des risques) et enforcement de masse (bilan CAC sur 20 000 applications).

Ces quatre modèles, à savoir la clarification européenne, la consultation américaine, l’autorisation supervisée coréenne et le contrôle massif chinois, ne convergent pas naturellement. Ils traduisent des philosophies différentes sur le rapport entre les pouvoirs publics, les entreprises et les citoyens. Pour les acteurs internationaux, cette diversité n'est pas transitoire : elle exige de bâtir des dispositifs de conformité capables d'opérer simultanément dans plusieurs régimes, sans les confondre. Elle demande aussi d'admettre que la conformité à un régime tel que l'AI Act européen, par exemple, ne garantit pas la conformité à d'autres.

Focus 1 – Europe : la CNIL précise l'AI Act × RGPD, l'e-Evidence entre en application

Deux publications européennes concernent directement les acteurs français et européens dans les plus brefs délais. Le 17 août 2026, la CNIL a mis à jour sa FAQ sur l'articulation entre l'AI Act et le RGPD, en intégrant les conséquences du règlement dit « Digital Omnibus on AI ». La CNIL confirme les jalons déjà largement documentés (cf. Édition #18) : depuis le 2 août 2026, certaines obligations de transparence de l'article 50 s'appliquent, telles que l'information lorsqu'une personne interagit avec une IA, la possibilité d'identifier techniquement les contenus générés par IA, et le signalement visible des hypertrucages ou des textes d'intérêt public générés artificiellement. Pour les systèmes générant du contenu déjà présents sur le marché avant le 2 août 2026, l'obligation technique de marquage est reportée au 2 décembre 2026. Les obligations concernant les systèmes à haut risque de l'annexe III s'appliqueront le 2 décembre 2027 ; celles de l'annexe I le 2 août 2028. Le message central de la CNIL est cependant plus structurel : l'AI Act ne remplace pas le RGPD. Le développement d'une IA à partir de données personnelles reste un traitement soumis au RGPD ; son utilisation opérationnelle constitue généralement un autre traitement, avec sa propre finalité, sa propre base légale et ses obligations d'information. Une conformité à l'AI Act ne suffit donc pas à établir la conformité au RGPD.

Le 18 août 2026, le règlement (UE) 2023/1543 relatif aux preuves électroniques (« e-Evidence ») est devenu directement applicable. Ce n'est pas un texte spécifique à l'IA, mais il transforme l'accès transfrontalier aux données personnelles dans le cadre des enquêtes pénales. Une autorité judiciaire d'un État membre peut désormais adresser directement à un fournisseur ou à son représentant établi dans un autre État membre une injonction de production de données (dix jours pour produire ; huit heures en urgence) ou une injonction de conservation (soixante jours, prolongeables de trente jours). Le périmètre couvre notamment les fournisseurs de communications électroniques, messageries et courriels, réseaux sociaux, places de marché, services d'hébergement ou de stockage, ainsi que certains services de noms de domaine et d'adresses IP. Les services financiers, comme les prestataires opérant exclusivement dans un seul État membre, sont exclus. Les sanctions nationales doivent pouvoir atteindre 2 % du chiffre d'affaires annuel mondial du fournisseur. La directive complémentaire 2023/1544 impose aux fournisseurs concernés de désigner un établissement ou un représentant légal dans l'Union ; sa date limite de transposition était le 18 février 2026.

Ce qu'il faut surveiller

- Les **premières positions supervisorielles françaises** (CNIL, autorités désignées par l'AI Act) sur la conformité des chatbots, générateurs de contenu, outils de détection d'émotions et systèmes produisant des hypertrucages, au 2 août 2026.

- La **mise en œuvre effective du circuit e-Evidence** : premiers volumes d'injonctions transfrontalières, adaptation des fournisseurs, articulation avec les régimes nationaux d'enquête préliminaire.
- L'**évolution du contentieux relatif à la transposition** de la directive 2023/1544, la France ayant été mise en demeure par la Commission européenne en mars 2026 pour absence de notification d'une transposition complète.

Focus 2 - États-Unis : le projet FTC sur la tarification personnalisée

Le 19 août 2026, la Federal Trade Commission américaine a soumis à consultation publique un projet de doctrine consacré à l'utilisation de données personnelles pour déterminer le prix maximal qu'un consommateur serait prêt à payer. Le texte est significatif dans sa formulation même : la FTC reconnaît explicitement qu'elle n'a pas le pouvoir d'interdire toute tarification personnalisée. Le projet n'est pas encore une doctrine définitive et, à supposer qu'il le devienne, il ne créerait pas de nouvelle infraction. Dans chaque procédure, la FTC devrait établir la violation d'une loi ou d'un règlement existant, principalement de la section 5 de l'Acte FTC relative aux pratiques commerciales déloyales ou trompeuses.

Malgré ces limites juridictionnelles, le projet appelle les entreprises à indiquer clairement que le prix affiché est personnalisé, à divulguer la logique de personnalisation et à préciser les catégories de données utilisées. Présenter un prix comme fixe alors qu'il varie selon l'historique de navigation, les achats, la localisation ou une estimation de la capacité financière du consommateur pourrait, selon la FTC, être considéré comme trompeur. La collecte ou l'utilisation de données sans information ou consentement appropriés pourrait également relever de la section 5. La FTC ne prend pas encore position sur la question de savoir si une tarification entièrement divulguée pourrait néanmoins être intrinsèquement déloyale. La question reste ouverte.

Cette approche témoigne d'une doctrine américaine qui, faute de législation fédérale équivalente au RGPD ou à l'AI Act, avance par le biais des autorités sectorielles et de leur pouvoir d'enforcement sur des textes existants. Pour les acteurs financiers utilisant des dispositifs de tarification différenciée (assurance, crédit, services d'investissement) ou des moteurs de recommandation reposant sur des scores de propension à payer, le projet FTC constitue un signal utile, sans créer d'obligation immédiate.

Ce qu'il faut surveiller

- L'**issue de la consultation publique de la FTC** et, le cas échéant, la version définitive de la doctrine.

- Les **premières actions d'enforcement FTC** fondées sur la section 5 du FTC Act contre des pratiques de tarification personnalisée jugées trompeuses.
- La **comparaison avec le cadre européen** (RGPD sur les décisions automatisées, AI Act sur les systèmes à haut risque d'évaluation de solvabilité et de tarification d'assurance vie et santé ; annexe III applicable au 2 décembre 2027).

Focus 3 – Asie : la Corée bâtit une base légale conditionnelle, la Chine industrialise le contrôle

Deux dynamiques asiatiques distinctes se déploient simultanément le 20 août 2026. En Corée du Sud, l'Assemblée nationale a adopté un amendement à la loi sur la protection des informations personnelles (PIPA), qui n'est pas encore applicable. Il doit être soumis au Conseil d'État, promulgué, puis entrera en vigueur six mois après la promulgation. Le dispositif proposé permet d'utiliser, pour développer une technologie d'IA, des données personnelles initialement collectées de manière licite, sous quatre conditions cumulatives : lorsque des données anonymes ou pseudonymisées ne suffisent pas ; lorsqu'un besoin d'intérêt public ou social est reconnu ; sous garanties renforcées ; et après examen et approbation par la PIPC (autorité coréenne de protection des données). Pour les traitements les plus risqués, notamment ceux impliquant des données sensibles ou des identifiants uniques, une évaluation préalable des risques et des mesures correctrices sont obligatoires. L'entreprise doit également publier les principales caractéristiques du traitement dans sa politique de confidentialité, et la PIPC publie de son côté des informations sur l'utilisation du régime spécial. Ce n'est pas une autorisation générale d'entraîner des modèles sans consentement, mais une base légale conditionnelle, individuelle et supervisée.

En Chine, deux événements s'inscrivent dans la même dynamique d'intensification. D'une part, les mesures d'évaluation des risques de sécurité des données de réseau sont entrées en vigueur le 20 août 2026. Elles ne visent pas exclusivement l'IA, mais concernent directement les systèmes traitant des « données importantes ». Les opérateurs de données importantes doivent effectuer une évaluation annuelle, procéder à une nouvelle évaluation lorsqu'un changement significatif peut affecter la sécurité, et transmettre leur rapport dans les vingt jours ouvrables suivant l'évaluation à l'autorité compétente. Les autres opérateurs sont seulement encouragés à effectuer une évaluation au moins tous les trois ans. L'évaluation peut être interne ou confiée à un tiers. D'autre part, la Cyberspace Administration of China (CAC) a publié le 19 août 2026 le bilan intermédiaire de ses opérations de contrôle de la vie privée : plus de 20 000 applications et SDK contrôlés, plus de 4 000 mis en conformité, plus de 1 100 publiquement signalés pour irrégularités, plus de 400 retirés ou sanctionnés, plus de 1 000 produits contrôlés pour défaut d'information sur la publicité ou le profilage, et plus de 90 000 organismes examinés dans les secteurs éducation, transport, santé et finance, avec plus de 12 000 problèmes corrigés.

Ce qu'il faut surveiller

- Le **processus de promulgation de l'amendement PIPA coréen** et les orientations pratiques que publiera la PIPC pour l'examen des demandes.
- Les **premières évaluations annuelles chinoises** au titre des nouvelles mesures d'évaluation des risques de sécurité des données de réseau.
- L'**impact du bilan CAC** sur les acteurs européens présents en Chine, notamment dans les secteurs de l'éducation, du transport, de la santé et de la finance directement mentionnés.

Focus 4 : Ce que cette fragmentation change pour les acteurs européens

Pour les organisations européennes telles que les banques, assureurs, sociétés de gestion, fintechs, CASPs, éditeurs de logiciels, prestataires SaaS, la séquence du 17 au 20 août 2026 impose trois lectures opérationnelles distinctes.

Première lecture, immédiate : les obligations européennes s'appliquent dès maintenant. Les organisations françaises devraient dès à présent vérifier leurs chatbots, générateurs d'images ou de textes, outils de détection d'émotions et systèmes produisant des hypertrucages au regard des obligations de transparence prévues par l'article 50 de l'AI Act. Pour les systèmes à haut risque (annexe III), les échéances ont reculé, mais la documentation RGPD, y compris les registres, la base légale, l'information, la minimisation et l'analyse d'impact, n'est pas reportée pour autant. En parallèle, tout fournisseur de services digitaux entrant dans le champ d'application d'e-Evidence doit vérifier qu'il dispose d'un représentant légal désigné dans l'Union et qu'il peut répondre aux injonctions dans des délais courts, avec une capacité de réponse en huit heures en cas d'urgence.

Deuxième lecture, prospective : les régimes coréen et américain doivent être suivis attentivement, sans être traités prématurément comme du droit applicable. L'amendement PIPA coréen n'est pas encore entré en vigueur ; le projet FTC n'est pas encore une doctrine définitive et, quand il le sera, ne créera pas de nouvelle infraction. Il ne serait donc pas juridiquement fondé de modifier immédiatement des pratiques en anticipation de textes non encore applicables. En revanche, ces deux évolutions indiquent des orientations que les acteurs internationaux gagneront à intégrer à leur veille et à leurs scénarios stratégiques à l'horizon 12-18 mois.

Troisième lecture, structurelle : pour les acteurs opérant en Chine, l'évaluation annuelle des risques pour les opérateurs de données importantes est désormais en vigueur. Ce sujet mérite un traitement de fond, incluant l'identification des jeux de données qualifiés d'« importants », la mise en place d'un dispositif d'évaluation reproductible et la préparation à des contrôles CAC de la même intensité que le bilan intermédiaire publié le 19 août. Cette dimension chinoise s'ajoute aux régimes européens, coréens et américains et confirme que la conformité mondiale des dispositifs d'IA et de

data n'est plus la juxtaposition de conformités nationales, mais une architecture multi-juridictionnelle à part entière.

Ce qu'il faut surveiller

- Les **premières publications sectorielles de l'ACPR et de l'AMF sur les usages de l'IA** par les acteurs financiers, attendues dans la continuité de la Cartographie AMF 2026 (cf. Édition #14) et des priorités de supervision 2026.
- La **cohérence globale des dispositifs de conformité** des acteurs financiers opérant sur plusieurs juridictions, sujet appelé à devenir un objet spécifique de contrôle interne et de reporting.
- L'évolution du **dialogue transatlantique et transpacifique** sur les données personnelles et l'IA, dans le prolongement du Global Dialogue on AI Governance de l'ONU (cf. Édition #15).

À retenir

Cinq points structurants à intégrer :

- La **CNIL a mis à jour le 17 août 2026 sa FAQ AI Act × RGPD** en confirmant que l'AI Act ne remplace pas le RGPD. La conformité à l'un ne vaut pas la conformité à l'autre.
- Le **règlement européen e-Evidence (2023/1543) est directement applicable depuis le 18 août 2026** : injonctions transfrontalières de production et de conservation avec des délais très courts (10 jours, 8 heures en urgence, 60 jours de conservation). Les services financiers sont exclus du champ.
- Le **projet FTC sur la tarification personnalisée du 19 août 2026** est en consultation publique, sans caractère contraignant à ce stade. Il pose néanmoins un cadre doctrinal relatif à l'information des consommateurs.
- L'**amendement PIPA coréen du 20 août 2026** crée une base légale conditionnelle pour l'entraînement d'IA sur des données personnelles licitement collectées, sous la supervision de la PIPC. Il n'est pas encore applicable.
- En Chine, les **mesures d'évaluation des risques de sécurité des données de réseau** sont effectives depuis le 20 août 2026 (évaluation annuelle pour les opérateurs de données importantes). Le bilan du CAC du 19 août fait état de plus de 20 000 applications contrôlées et de plus de 400 sanctions.

Conclusion

La seconde quinzaine d'août 2026 confirme que la gouvernance mondiale de l'IA et des données personnelles n'entre pas dans une phase de convergence, mais dans une phase de fragmentation assumée. Les cinq géographies traitées que sont l'Union européenne, les États-Unis, la Corée du Sud, la Chine et l'articulation nationale française répondent aux mêmes enjeux par des philosophies différentes : clarification opérationnelle et applicabilité directe pour l'UE ; consultation lente et négociée aux États-Unis ; autorisation conditionnelle supervisée en Corée ; contrôle centralisé massif en Chine. Pour les organisations françaises et européennes, cette fragmentation appelle une lecture à trois horizons : conformité immédiate aux obligations européennes désormais applicables (AI Act, article 50, e-Evidence, RGPD sans allègement), veille active sur les textes coréens et américains en cours de construction, et traitement structurel du dispositif chinois pour les acteurs présents sur ce marché. Le Regulatory Brief continuera de documenter cette architecture multi-juridictionnelle dans les éditions à venir.

Sources principales

- Commission nationale de l'informatique et des libertés (CNIL), « Entrée en vigueur du règlement européen sur l'IA : les premières questions-réponses de la CNIL », publication initiale du 12 juillet 2024, mise à jour le 17 août 2026.
- Règlement (UE) 2026/1744 du Parlement européen et du Conseil du 8 juillet 2026 modifiant notamment le règlement (UE) 2024/1689 afin de simplifier la mise en œuvre des règles harmonisées relatives à l'intelligence artificielle (« Digital Omnibus on AI »), JOUE du 24 juillet 2026, entré en vigueur le 27 juillet 2026 — voir également l'Édition nº 18.
- Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (« AI Act »), notamment l'article 50 relatif aux obligations de transparence et les annexes I et III relatives aux systèmes d'IA à haut risque.
- Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et de conservation de preuves électroniques (« e-Evidence »), applicable depuis le 18 août 2026.
- Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements et de représentants légaux aux fins de l'obtention de preuves électroniques, dont la date limite de transposition était fixée au 18 février 2026.
- Federal Trade Commission (FTC), « FTC Seeks Comment on Enforcement Policy Statement Regarding Personalized Pricing », 19 août 2026 ; voir également le projet de doctrine soumis à consultation.
- Personal Information Protection Commission (PIPC, Corée du Sud), « Création d'un régime spécial d'utilisation des données personnelles pour le développement sécurisé de l'intelligence artificielle », communiqué relatif à l'amendement de la Personal Information Protection Act adopté par l'Assemblée nationale le 20 août 2026.
- Cyberspace Administration of China (CAC), « Questions-réponses sur la mise en œuvre des mesures d'évaluation des risques de sécurité des données de réseau », 20 août 2026.
- Cyberspace Administration of China (CAC), « Bilan intermédiaire des opérations spéciales de protection des informations personnelles menées en 2026 », 19 août 2026.

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« RGPD »).

The Seqlense Regulatory Brief - Crypto, TradFi & Digital - Édition #21

Cette publication est fournie à titre strictement informatif et ne constitue ni un conseil juridique, ni un conseil en investissement, ni une recommandation personnalisée. Elle ne saurait remplacer une analyse juridique ou opérationnelle propre à chaque organisation, susceptible de tenir compte de sa taille, de son secteur, de ses pratiques et de son écosystème contractuel.

Les informations présentées reflètent une analyse générale des dynamiques réglementaires à la date de publication. Les positions des autorités européennes, américaines, asiatiques et nationales peuvent évoluer rapidement ; les textes en construction (projet FTC, amendement PIPA coréen) ne créent pas d'obligation immédiate et ne doivent pas être traités comme du droit applicable.

Malgré les soins apportés à la sélection et à la vérification des sources, aucune garantie n'est donnée quant à l'exactitude, l'exhaustivité ou l'actualité des informations. Les pratiques opérationnelles doivent être ajustées à la lumière des positions supervisorielles à venir, des décisions de sanction et de l'évolution des cadres juridiques.

Toute décision de mise en conformité relève de la seule responsabilité de l'organisation concernée et doit, le cas échéant, être prise avec l'appui de conseils juridiques et techniques qualifiés dans chaque juridiction concernée.