Crypto, TradFi & Digital

AI special: global regulatory fragmentation

Decoding financial, AI and data regulation to anticipate, comply and decide

Five geographies, five answers: AI and personal data in global tension

Previous editions of the Regulatory Brief have tracked, step by step, the ramp-up of the European framework: the AI Act and its Omnibus (Editions #7 and #18), its interplay with the GDPR (Edition #8), the convergence of AI and cybersecurity (Edition #11), the global acceleration of AI regulation in July 2026 (Edition #15), the European Parliament's vote on stablecoins (Edition #16), the CNIL recommendation on tracking pixels (Edition #19) and the ESMA-AMF clarification of the perimeter of advice on crypto-assets under MiCA (Edition #20). This twenty-first edition continues that thread by focusing on a particularly dense moment: the second half of August 2026, during which five major regulatory geographies, namely the European Union, the United States, South Korea, China and France in its national articulation, took coordinated or divergent positions on AI and the protection of personal data.

Five events need to be read together. On 17 August 2026, the CNIL published the update of its FAQ on the interplay between the AI Act and the GDPR, incorporating the consequences of the European regulation known as the “Digital Omnibus on AI”, adopted on 8 July 2026, published on 24 July and in force since 27 July. On 18 August 2026, European Regulation 2023/1543 on electronic evidence (“e-Evidence”) became directly applicable throughout the Union. On 19 August 2026, the US Federal Trade Commission put out for public consultation a draft policy statement on personalised pricing based on personal data; on the same day, the Chinese cyberspace authority (CAC) published an interim report on its privacy inspection operations covering more than 20,000 applications. On 20 August 2026, South Korea's National Assembly adopted an amendment to the Korean Personal Information Protection Act (PIPA) creating a specific, conditional legal basis for the training of AI models; the same day, the Chinese measures on network data security risk assessment entered into force.

Read together, these five publications document a reality that the Regulatory Brief has regularly anticipated: the global governance of AI and personal data is now being built in a permanent tension between convergence (the same concerns, the same principles) and fragmentation (very different approaches, timetables and degrees of constraint). For financial institutions, compliance officers, DPOs, legal departments, CIOs and institutional investors with an international footprint, this fragmentation is becoming a strategic parameter in its own right, on a par with market risk or cyber risk.

This edition offers a geographical reading of the sequence, with a final focus on what it changes in concrete terms for European players.

The main signal

Global regulatory fragmentation is no longer a matter of timing differences between jurisdictions; it is becoming a deliberate doctrinal choice: five geographies, five different answers to essentially identical issues.

What is striking about the sequence of 17 to 20 August 2026 is less the chronological coincidence of the publications than the structure of their approaches. The European Union is consolidating its framework through operational clarification (CNIL) and extending its cross-border reach through a text that has become directly applicable (e-Evidence). The United States is exploring, through public consultation, a slow, negotiated regulation of a practice it does not claim to prohibit (personalised pricing). South Korea is building an intermediate regime, neither a prohibition nor a general authorisation, but a conditional, supervised authorisation. China is combining centralised control (risk-assessment measures) and mass enforcement (the CAC report on 20,000 applications).

These four models, namely European clarification, American consultation, Korean supervised authorisation and Chinese mass control, do not converge naturally. They reflect different philosophies of the relationship between public authorities, companies and citizens. For international players, this diversity is not transitory: it requires building compliance frameworks capable of operating simultaneously across several regimes without conflating them. It also requires accepting that compliance with one regime, such as the European AI Act, does not guarantee compliance with the others.

Focus 1 - Europe: the CNIL clarifies the AI Act and GDPR interplay, e-Evidence becomes applicable

Two European publications directly concern French and European players with immediate effect. On 17 August 2026, the CNIL updated its FAQ on the interplay between the AI Act and the GDPR, incorporating the consequences of the regulation known as the "Digital Omnibus on AI". The CNIL confirms the milestones already widely documented (see Edition #18): since 2 August 2026, certain transparency obligations under Article 50 apply, such as informing people when they interact with an AI, the ability to technically identify AI-generated content, and the visible flagging of deepfakes and artificially generated texts of public interest. For content-generating systems already on the market before 2 August 2026, the technical marking obligation is deferred to 2 December 2026. The obligations relating to high-risk systems under Annex III will apply from 2 December 2027, and those under Annex I from 2 August 2028. The CNIL's central message, however, is more structural: the AI Act does not replace the GDPR. Developing an AI from personal data remains processing subject to the GDPR; its operational use generally constitutes a separate processing operation, with its own purpose, its own legal basis and its own information obligations. Compliance with the AI Act is therefore not sufficient to establish compliance with the GDPR.

On 18 August 2026, Regulation (EU) 2023/1543 on electronic evidence ("e-Evidence") became directly applicable. It is not an AI-specific text, but it transforms cross-border access to personal data in criminal investigations. A judicial authority of one Member State may now address directly to a provider, or to its representative established in another Member State, a production order for data (ten days to produce; eight hours in an emergency) or a preservation order (sixty days, extendable by thirty days). The scope notably covers providers of electronic communications, messaging and email services, social networks, marketplaces, hosting or storage services, and certain domain-name and IP-address services. Financial services, like providers operating exclusively within a single Member State, are excluded. National penalties must be capable of reaching 2% of the provider's annual worldwide turnover. The complementary Directive 2023/1544 requires the providers concerned to designate an establishment or a legal representative in the Union; its transposition deadline was 18 February 2026.

What to watch

- The **first French supervisory positions** (CNIL, authorities designated under the AI Act) on the compliance of chatbots, content generators, emotion-detection tools and systems producing deepfakes, as at 2 August 2026.
- The **effective implementation of the e-Evidence circuit**: the first volumes of cross-border orders, providers' adaptation, and the interplay with national preliminary-investigation regimes.

- The **development of litigation over the transposition** of Directive 2023/1544, France having received a formal notice from the European Commission in March 2026 for failing to notify complete transposition.

Focus 2 - United States: the FTC draft on personalised pricing

On 19 August 2026, the US Federal Trade Commission put out for public consultation a draft policy statement on the use of personal data to determine the maximum price a consumer would be willing to pay. The text is significant in its very wording: the FTC explicitly acknowledges that it does not have the power to prohibit all personalised pricing. The draft is not yet final doctrine and, even if it becomes so, it would not create any new offence. In each proceeding, the FTC would have to establish a violation of an existing law or regulation, principally Section 5 of the FTC Act on unfair or deceptive commercial practices.

Despite these jurisdictional limits, the draft calls on companies to state clearly that the displayed price is personalised, to disclose the personalisation logic and to specify the categories of data used. Presenting a price as fixed when it varies according to browsing history, purchases, location or an estimate of the consumer's financial capacity could, according to the FTC, be regarded as deceptive. Collecting or using data without appropriate information or consent could also fall under Section 5. The FTC does not yet take a position on whether fully disclosed pricing could nevertheless be inherently unfair. The question remains open.

This approach reflects an American doctrine which, in the absence of federal legislation equivalent to the GDPR or the AI Act, advances through sectoral authorities and their enforcement powers under existing texts. For financial institutions using differentiated pricing arrangements (insurance, credit, investment services) or recommendation engines based on propensity-to-pay scores, the FTC draft is a useful signal, without creating any immediate obligation.

What to watch

- The **outcome of the FTC's public consultation** and, where applicable, the final version of the policy statement.
- The **first FTC enforcement actions** based on Section 5 of the FTC Act against personalised-pricing practices deemed deceptive.
- The **comparison with the European framework** (the GDPR on automated decisions, the AI Act on high-risk systems for creditworthiness assessment and life and health insurance pricing; Annex III applicable from 2 December 2027).

Focus 3 - Asia: Korea builds a conditional legal basis, China industrialises control

Two distinct Asian dynamics unfolded simultaneously on 20 August 2026. In South Korea, the National Assembly adopted an amendment to the Personal Information Protection Act (PIPA), which is not yet applicable. It must be submitted to the State Council, promulgated, and will then enter into force six months after promulgation. The proposed mechanism allows personal data initially collected lawfully to be used to develop AI technology, subject to four cumulative conditions: where anonymous or pseudonymised data is not sufficient; where a public or social interest need is recognised; subject to reinforced safeguards; and after review and approval by the PIPC (the Korean data protection authority). For the riskiest processing operations, in particular those involving sensitive data or unique identifiers, a prior risk assessment and corrective measures are mandatory. The company must also publish the main characteristics of the processing in its privacy policy, and the PIPC, for its part, publishes information on the use of the special regime. This is not a general authorisation to train models without consent, but a conditional, individual and supervised legal basis.

In China, two events form part of the same intensification dynamic. On the one hand, the network data security risk-assessment measures entered into force on 20 August 2026. They are not aimed exclusively at AI, but directly concern systems processing “important data”. Operators of important data must conduct an annual assessment, conduct a new assessment when a significant change may affect security, and submit their report to the competent authority within twenty working days of the assessment. Other operators are encouraged to conduct an assessment at least every three years. The assessment may be internal or entrusted to a third party. On the other hand, the Cyberspace Administration of China (CAC) published on 19 August 2026 the interim report on its privacy inspection operations: more than 20,000 applications and SDKs inspected, more than 4,000 brought into compliance, more than 1,100 publicly flagged for irregularities, more than 400 removed or sanctioned, more than 1,000 products inspected for failure to provide information on advertising or profiling, and more than 90,000 organisations examined in the education, transport, health and finance sectors, with more than 12,000 issues corrected.

What to watch

- The **promulgation process of the Korean PIPA amendment** and the practical guidance the PIPC will publish for reviewing applications.
- The **first Chinese annual assessments** under the new network data security risk-assessment measures.
- The **impact of the CAC report** on European players present in China, in particular in the education, transport, health and finance sectors directly mentioned.

Focus 4: What this fragmentation changes for European players

For European organisations such as banks, insurers, asset managers, fintechs, CASPs, software publishers and SaaS providers, the sequence of 17 to 20 August 2026 requires three distinct operational readings.

First reading, immediate: the European obligations apply now. French organisations should already be checking their chatbots, image or text generators, emotion-detection tools and systems producing deepfakes against the transparency obligations laid down by Article 50 of the AI Act. For high-risk systems (Annex III), the deadlines have moved back, but the GDPR documentation, including records, legal basis, information, minimisation and impact assessment, is not deferred as a result. In parallel, any digital service provider falling within the scope of e-Evidence must check that it has a designated legal representative in the Union and that it can respond to orders within short timeframes, with the capacity to respond within eight hours in an emergency.

Second reading, forward-looking: the Korean and American regimes must be monitored closely, without being treated prematurely as applicable law. The Korean PIPA amendment has not yet entered into force; the FTC draft is not yet final doctrine and, when it is, will not create any new offence. It would therefore not be legally sound to change practices immediately in anticipation of texts that are not yet applicable. On the other hand, these two developments indicate directions that international players would do well to build into their monitoring and their strategic scenarios over a 12 to 18 month horizon.

Third reading, structural: for players operating in China, the annual risk assessment for operators of important data is now in force. This subject deserves in-depth treatment, including identifying the datasets classified as “important”, putting in place a repeatable assessment process and preparing for CAC inspections of the same intensity as the interim report published on 19 August. This Chinese dimension adds to the European, Korean and American regimes and confirms that the global compliance of AI and data frameworks is no longer the juxtaposition of national compliances, but a fully fledged multi-jurisdictional architecture.

What to watch

- The **first sectoral publications by the ACPR and the AMF on the uses of AI** by financial institutions, expected in the continuation of the AMF 2026 Mapping (see Edition #14) and the 2026 supervisory priorities.
- The **overall consistency of the compliance frameworks** of financial institutions operating across several jurisdictions, a subject set to become a specific object of internal control and reporting.

- The development of the **transatlantic and transpacific dialogue** on personal data and AI, in the continuation of the UN Global Dialogue on AI Governance (see Edition #15).

Key takeaways

Five structural points to take on board:

- The **CNIL updated its AI Act and GDPR FAQ on 17 August 2026**, confirming that the AI Act does not replace the GDPR. Compliance with one does not amount to compliance with the other.
- The **European e-Evidence Regulation (2023/1543) has been directly applicable since 18 August 2026**: cross-border production and preservation orders with very short deadlines (10 days, 8 hours in an emergency, 60 days' preservation). Financial services are excluded from the scope.
- The **FTC draft on personalised pricing of 19 August 2026** is under public consultation and is not binding at this stage. It nevertheless sets out a doctrinal framework on consumer information.
- The **Korean PIPA amendment of 20 August 2026** creates a conditional legal basis for training AI on lawfully collected personal data, under the supervision of the PIPC. It is not yet applicable.
- In China, the **network data security risk-assessment measures** have been effective since 20 August 2026 (annual assessment for operators of important data). The CAC report of 19 August records more than 20,000 applications inspected and more than 400 sanctions.

Conclusion

The second half of August 2026 confirms that the global governance of AI and personal data is not entering a phase of convergence, but a phase of deliberate fragmentation. The five geographies covered, namely the European Union, the United States, South Korea, China and the French national articulation, respond to the same issues with different philosophies: operational clarification and direct applicability for the EU; slow, negotiated consultation in the United States; conditional supervised authorisation in Korea; massive centralised control in China. For French and European organisations, this fragmentation calls for a reading across three horizons: immediate compliance with the European obligations now applicable (AI Act, Article 50, e-Evidence, GDPR without relief), active monitoring of the Korean and American texts under construction, and structural treatment of the Chinese framework for players present in that market. The Regulatory Brief will continue to document this multi-jurisdictional architecture in future editions.

Main sources

- 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 », initially published 12 July 2024, updated 17 August 2026.
- Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending, in particular, Regulation (EU) 2024/1689 in order to simplify the implementation of the harmonised rules on artificial intelligence (the "Digital Omnibus on AI"), OJEU of 24 July 2026, in force since 27 July 2026; see also Edition #18.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (the "AI Act"), in particular Article 50 on transparency obligations and Annexes I and III on high-risk AI systems.
- Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European production orders and European preservation orders for electronic evidence ("e-Evidence"), applicable since 18 August 2026.
- Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of establishments and legal representatives for the purpose of gathering electronic evidence, whose transposition deadline was set at 18 February 2026.
- Federal Trade Commission (FTC), "FTC Seeks Comment on Enforcement Policy Statement Regarding Personalized Pricing", 19 August 2026; see also the draft policy statement put out for consultation.
- Personal Information Protection Commission (PIPC, South Korea), "Creation of a special regime for the use of personal data for the safe development of artificial intelligence", press release on the amendment to the Personal Information Protection Act adopted by the National Assembly on 20 August 2026.
- Cyberspace Administration of China (CAC), "Questions and answers on the implementation of the network data security risk-assessment measures", 20 August 2026.
- Cyberspace Administration of China (CAC), "Interim report on the special personal-information protection operations conducted in 2026", 19 August 2026.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "GDPR").

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