Submitted: March 16th, 2026
Reviews completed: May 27th, 2026
Published: June 12th, 2026

Financial Law Review

No. 41 (1)/2026

UNIVERSITY OF GDAŃSK • MASARYK UNIVERSITY • PAVEL JOZEF ŠAFÁRIK UNIVERSITY
http://www.ejournals.eu/FLR

Klemens Katterbauer* Laurent Cleenewerck**

SOVEREIGN ALGORITHMS, BORDERLESS FINANCE: NAVIGATING LEGAL PATHWAYS FOR EU-CHINA FINTECH AI INTEGRATION AMIDST DATA LOCALIZATION REGIMES

Abstract

The convergence of financial technology (fintech) and artificial intelligence (AI) promises unprecedented efficiency in credit scoring, fraud detection, and algorithmic trading. However, the deployment of these technologies across the European Union (EU) and the People's Republic of China (PRC) is increasingly obstructed by divergent data sovereignty regimes. This article examines the legal pathways available for EU fintechs utilizing China-trained AI models, and vice versa, within the context of conflicting data localization rules. By analyzing the General Data Protection Regulation (GDPR), the EU AI Act, China's Personal Information Protection Law (PIPL), and the Data Security Law (DSL), this paper identifies the jurisdictional friction points regarding cross-border data transfers. It argues that while traditional transfer

* Klemens Katterbauer is professor for International Law and Global Management at EUCLID University and EULER, specializing in Artificial Intelligence and its application to legal, business and energy as well as environmental applications. Author of more than five books and more than 80 reviewed articles in prestigious journals.
Contact email: katterbauer@efmu.nl, ORCID: 0000-0001-5513-4418.

** Laurent Cleenewerck is a professor of International Administration and Theology for EUCLID / Euclid Consortium and an ordained presbyter of the Ecumenical Patriarchate of Constantinople (2004) current serving as acting-rector at St. Innocent's Orthodox parish in Eureka, California.
Contact email: cdk@euclid.int, ORCID: 0000-0002-9267-0428.

mechanisms (such as adequacy decisions) are politically unviable, technical-legal hybrids—specifically federated learning, model localization, and synthetic data generation—offer the only viable compliance architecture. The article concludes with recommendations for regulatory sandboxes and mutual recognition of technical standards to mitigate the risk of technological decoupling in the financial sector.

Key words: Artificial Intelligence Governance; Cross-Border Data Transfers; Data Localization; EU-China Fintech Integration; Privacy-Enhancing Technologies

JEL Classification: F55

1. Introduction

The contemporary financial ecosystem stands at a crossroads where technological innovation collides with geopolitical fragmentation. Financial technology—fintech—has emerged as a transformative force, reimagining how credit is assessed, how fraud is detected, and how capital markets operate across borders. At the heart of this transformation lies artificial intelligence, particularly machine learning models that derive predictive power from massive datasets. These technologies promised a future of frictionless global finance, where algorithms trained in one jurisdiction could seamlessly enhance financial services in another. Yet, as the 2020s unfold, this vision confronts an uncomfortable reality: the architecture of global data governance is fracturing along sovereign lines. Nowhere is this tension more pronounced than in the relationship between the European Union and the People's Republic of China—two of the world's most influential regulatory powers, each advancing comprehensive but fundamentally incompatible frameworks for data protection and AI governance.

The European Union has constructed its digital regulatory architecture upon the foundation of fundamental rights. The General Data Protection Regulation [GDPR], since its implementation in 2018, has established itself as the global benchmark for privacy protection, treating personal data as an extension of human dignity requiring robust safeguards against unauthorized processing and transfer. Building upon this foundation, the EU AI Act—finalized in 2024—introduces a risk-based taxonomy for artificial intelligence systems, classifying fintech applications such as credit scoring and identity verification as "high-risk" and subjecting them to stringent requirements regarding transparency, data governance, and human oversight [Mahmutovic 2025; Raddatz, Green 2025]. This regulatory philosophy

reflects a deeply embedded European commitment to individual autonomy and algorithmic accountability, but it simultaneously erects substantial barriers to data mobility. Chapter V of the GDPR restricts cross-border data transfers to jurisdictions lacking "adequate" protection, a designation China has not received and, given persistent concerns regarding state surveillance and intelligence access, is unlikely to obtain in the foreseeable future [Deshpande 2025].

China's regulatory trajectory proceeds from an entirely different set of priorities. The tripartite framework comprising the Cybersecurity Law [CSL], the Data Security Law [DSL], and the Personal Information Protection Law [PIPL] subordinates individual privacy interests to collective state security objectives. Under this paradigm, data constitutes not merely an economic asset but a strategic resource requiring rigorous oversight to prevent outflow that might compromise national interests. The DSL introduces a hierarchical classification system—distinguishing between general, important, and core data—with increasingly stringent localization requirements attached to higher categories. The Cyberspace Administration of China's Measures for the Security Assessment of Outbound Data Transfer [2022] mandate government approval before specified volumes of personal information or categories of "important data" can cross China's borders [Akhmatova 2025]. More recently, the Interim Measures for the Management of Generative Artificial Intelligence Services [2023] require that training data align with "socialist core values," creating content compliance barriers for models developed in liberal democratic contexts. China's approach, as Bassens, Fang, and Pascal [2025] observe, reflects a deliberate strategy of asserting "sovereignty across the cloud finance stack"—constructing a digital bulwark against perceived technological domination by Western platforms [Bassens et al. 2025]. Conversely, a Chinese fintech expanding into European markets confronts the dual burden of securing CAC approval for any outbound transfer of domestic data while simultaneously complying with the GDPR's stringent requirements for data processing within EU territory. As Dong and Zhang [2024] note in their analysis of cross-border payment systems, the compliance burden multiplies exponentially when firms must navigate overlapping but non-aligned regulatory expectations across multiple jurisdictions [Dong, Zhang 2024].

This article examines the legal pathways available for EU fintechs utilizing China-trained AI models, and conversely, for Chinese fintechs seeking to deploy European-developed AI capabilities. Throughout, the article attends to sector-specific variations within fintech, recognizing that credit scoring, anti-money laundering, and robo-advisory applications present distinct risk profiles and regulatory expectations [Horobets et al. 2025; Remolina 2025]. The argument unfolds in eight parts. Following this introduction, Section 2 reviews the existing literature on comparative data protection law and cross-border AI governance. Section 3 outlines the research methodology, combining doctrinal legal analysis with comparative regulatory assessment. Section 4 provides a detailed exposition of the EU and Chinese regulatory landscapes, emphasizing points of irreconcilable conflict. Section 5 addresses the threshold legal question of whether model weights and algorithmic parameters constitute "personal data" subject to transfer restrictions—a question upon which much of the proposed technical architecture depends. Section 6 evaluates specific compliance pathways, assessing their feasibility, limitations, and remaining legal risks. Section 7 stress-tests these pathways against three distinct fintech use cases: credit scoring, anti-money laundering, and robo-advisory services. Section 8 concludes with recommendations for policymakers and industry stakeholders, advocating for regulatory sandboxes, technical standard harmonization, and contractual innovations that might mitigate the risk of complete technological decoupling in the financial sector. The article ultimately contends that while frictionless cross-border AI deployment has indeed ended, an era of "sovereign computing"—wherein algorithms travel while data remains home—offers a viable, if technically demanding, path forward for fintech innovation in an age of regulatory fragmentation.

2. Literature Review

The comparative analysis of EU and Chinese regulatory frameworks constitutes the most developed strand of literature. Foundational industry analyses, such as Kaya et al. [2019], established the transformative potential of AI in banking, predicting the very regulatory tensions that have subsequently materialized in EU-China relations [Kaya et al. 2019]. Deshpande [2025] provides a comprehensive examination of AI regulation and policy pathways across China, the European Union, and the United States, identifying fundamental philosophical divergences that render harmonization politically

improbable [Deshpande, 2025]. The European approach, as Mahmutovic [2025] elaborates in analyzing the EU AI Act, proceeds from a fundamental rights perspective that treats algorithmic accountability and individual autonomy as non-negotiable prerequisites for technological deployment [Mahmutovic 2025]. This orientation manifests in the Act's risk-based taxonomy, which classifies fintech applications such as credit scoring and identity verification as "high-risk" systems subject to stringent transparency, data governance, and human oversight requirements. Raddatz and Green [2025] extend this analysis by examining how institutional structures shape trust in AI financial systems, arguing that the EU's regulatory architecture reflects deeper commitments to democratic accountability and individual redress that resist compromise with alternative governance models [Raddatz, Green 2025].

Lu [2024] provides comprehensive treatment of global fintech regulation, situating EU-China dynamics within broader patterns of regulatory competition and convergence across major economies [Lu 2024]. China's regulatory trajectory, by contrast, subordinates individual privacy interests to collective state security objectives. Lia and Lic [2025] trace the diverging paths of EU and Chinese AI governance, demonstrating how China's tripartite framework comprising the Cybersecurity Law, Data Security Law, and Personal Information Protection Law constructs data as a strategic resource requiring rigorous oversight to protect national interests [Lia, Lic 2025]. Akhmatova [2025] examines China's approach to technology market regulation, revealing how anti-monopoly enforcement and data governance intersect to create a distinctive regulatory paradigm that prioritizes state control over market liberalization [Akhmatova 2025]. Bassens, Fang, and Pascal [2025] offer perhaps the most theoretically sophisticated treatment, conceptualizing China's strategy as an assertion of "sovereignty across the cloud finance stack"—a deliberate construction of digital bulwarks against perceived technological domination by Western platforms. Their relational comparison of the United States, European Union, and China illuminates how each jurisdiction's approach reflects distinct political economies and security anxieties [Bassens et al., 2025].

The geopolitical dimensions of technological competition feature prominently in recent scholarship. Gordon and Nouwens [2022] examine China's Digital Silk Road as a manifestation of broader ambitions to shape global

technological governance, while Hussain et al. [2024] analyze the economic implications of China's digital rise through the Belt and Road Initiative [Gordon, Nouwens 2022; Hussain et al. 2024]. García-Herrero et al. [2017] provide an earlier but still relevant assessment of EU-China economic relations, projecting trajectories that subsequent scholarship has largely confirmed [García-Herrero et al. 2017]. Demergis [2025] situates fintech AI integration within broader patterns of technological convergence and geopolitical fragmentation, arguing that data governance has become a central arena for great power competition. This geopolitical lens proves essential for understanding why traditional legal mechanisms for cross-border data transfers have proven inadequate [Demergis 2025].

A second strand of literature examines the threshold legal question of whether artificial intelligence models and their components constitute "personal data" subject to transfer restrictions. Katterbauer [2024] examines whether artificial intelligence can serve as a "gamechanger" for financial regulations in China, implicitly addressing how algorithmic systems might navigate between regimes. The risk of membership inference attacks—where adversaries query models to determine whether specific data points were part of training sets—complicates arguments that model weights are necessarily non-personal. If models memorize training data, the weights could indirectly reveal personal information, potentially triggering data protection law even when raw data never crosses borders [Katterbauer, 2024, p. 202]. The technology transfer dimensions of EU-China relations are explored in Tatlow et al. [2020], who examine Europe's role in China's quest for foreign technology, providing historical context for current AI governance tensions [Tatlow et al. 2020]. Dong and Zhang [2024] address these questions directly in their analysis of AI-driven compliance risk assessment in cross-border payments, identifying how different categories of data transfers attract different legal treatment under multiple jurisdictions [Dong, Zhang, 2024]. Gajula [2025] advances this analysis by proposing federated intelligence frameworks for privacy-preserving cross-border risk analysis, explicitly addressing how gradient transmission might be structured to minimize re-identification risks through differential privacy enhancements [Gajula 2025].

The third strand of literature evaluates specific technical-legal hybrids as potential compliance pathways. Horobets et al. [2025] examine artificial intelligence technologies in banking, focusing specifically on anti-money

laundering applications within the context of EU regulatory initiatives [Horobets et al. 2025]. Remolina [2025] extends this sectoral analysis to algorithmic auditing in financial institutions, drawing lessons from Singapore's approach to AI governance that might inform EU-China collaboration. The emphasis on auditability and transparency as non-negotiable requirements for financial AI suggests that technical solutions must address not only data localization but also explainability [Remolina 2025].

Perboli, Simionato, and Pratali [2025] provide a comprehensive overview of navigating AI regulatory landscapes, balancing innovation, ethics, and global governance considerations. Their analysis encompasses the full range of privacy-enhancing technologies, from federated learning and differential privacy to synthetic data generation and trusted execution environments [Perboli et al. 2025]. Importantly, they emphasize that technical solutions alone cannot resolve legal uncertainties; regulatory recognition of specific technical standards remains essential for creating predictable compliance pathways. This theme recurs in Badawy's [2025] examination of algorithmic sovereignty and democratic resilience, which argues that technical governance must be embedded within broader frameworks of democratic accountability [Badawy 2025].

Scholarship specifically addressing federated learning in cross-border contexts remains nascent but growing. Mirza et al. [2023] extend this technical analysis by comparatively assessing machine learning approaches for safeguarding fintech innovations, offering methodological insights relevant to cross-border deployment contexts [Mirza et al. 2023]. Gajula [2025] proposes federated intelligence frameworks for financial ecosystems, arguing that distributed learning architectures can preserve privacy while enabling cross-border model improvement [Gajula 2025].

The sector-specific challenges within fintech receive increasing scholarly attention. Iddrisu, Yakubu, and Asongu [2025] examine fintech innovations for sustainable banking, situating technical questions within broader development objectives [Iddrisu et al. 2025]. Truby, Brown, and Dahdal [2020] mandate proactive approaches to AI regulation in the financial sector, arguing that financial AI presents distinct risks requiring tailored governance responses [Truby et al. 2020]. Paleti [2025] provides comprehensive treatment of artificial intelligence, regulatory compliance, and data engineering in global banking transformation, offering practical frameworks for navigating

multi-jurisdictional requirements [Paleti 2025]. Ridzuan et al. [2024] examine the line between innovation, regulation, and ethical responsibility in financial AI, emphasizing that technical solutions cannot substitute for fundamental value choices about acceptable risks and trade-offs [Ridzuan et al. 2024]. The intersection of AI, finance, and sustainability receives systematic examination in Sadati et al. [2024], who provide an overview framework that accommodates cross-jurisdictional analysis [Sadati et al. 2024].

Katterbauer's [2022] earlier work on digital service taxation and sustainability frameworks, while not directly addressing fintech AI, establishes methodological approaches to analyzing cross-border data flows that inform subsequent scholarship [Katterbauer 2022]. The analysis of subsea cable data transmissions reveals how physical infrastructure shapes legal jurisdiction—a theme that resonates with contemporary debates about where data "is" for purposes of data protection law. Żmuda-Matan [2024] and Homa [2024] contribute analyses of related financial law questions, though their focus on local government finance and digital permanent establishments lies somewhat outside the core concerns of cross-border AI governance [Homa 2024; Żmuda-Matan 2024]. Sharma et al. [2021] anticipated many contemporary challenges in their analysis of governance, compliance, and cyber risk management in cross-border fintech operations, identifying friction points that have since intensified [Sharma et al. 2021]. Zhang [2025] examines the role of Chinese think tanks in AI governance, offering insights into how policy positions develop within China's institutional ecosystem, but bilateral mechanisms for technical standard harmonization receive limited attention [Q. Zhang 2025]. Da Fonseca Azevedo [2024] examines analogous questions in international trade law, considering how the WTO's Technical Barriers to Trade Agreement might accommodate mutual recognition of data protection regimes. Yet scholars acknowledge that such arrangements require levels of trust that currently appear unrealistic in EU-China relations [da Fonseca Azevedo 2024]. This recognition aligns with Katterbauer's [2024] concept of "algorithmic balkanization," where global financial infrastructure fragments into discrete technological spheres. The challenge for scholarship, and for practice, lies in identifying pathways that preserve sufficient cross-border collaboration to sustain innovation while respecting legitimate regulatory concerns about privacy, security, and sovereignty [Katterbauer 2024]. Zhang and Bilawal Khaskheli

[2025] offer a tripartite comparison of China, the EU, and the USA regarding digital technologies and sustainable development, reinforcing this article's comparative methodology [Y. Zhang. Bilawal Khaskheli 2025].

3. Research Methodology

This study employs a doctrinal legal methodology, supplemented by comparative regulatory analysis and a technology-centric case study approach, to examine the legal pathways for EU-China fintech AI integration. The doctrinal component systematically analyzes the relevant statutory frameworks, including the European Union's General Data Protection Regulation (GDPR) and the EU AI Act, alongside China's Personal Information Protection Law (PIPL), Data Security Law (DSL), and implementing regulations from the Cyberspace Administration of China. This analysis focuses on identifying jurisdictional friction points, particularly the specific conditions under which cross-border data transfers are either permitted or prohibited, and the legal qualifications of different data categories. The comparative dimension draws on existing scholarship to contextualize these frameworks within their respective philosophical underpinnings—contrasting the EU's fundamental rights-based approach with China's state security-oriented paradigm as elaborated in the literature [Bassens et al. 2025; Deshpande 2025; Lia, Lic 2025]. The comparative dimension draws on scholarship examining China's global integration strategies, including Araya and Peters' [2023] analysis of Chinese globalization through the Belt and Road Initiative, which contextualizes digital governance within broader geopolitical ambitions [Araya, Peters, 2023]. This comparison is essential for understanding why traditional transfer mechanisms like adequacy decisions remain politically unviable.

Furthermore, the research integrates a technology assessment methodology to evaluate the legal viability of proposed technical-legal hybrids. It examines specific architectural solutions—such as federated learning, model localization, and synthetic data generation—by applying the identified legal rules to the technical characteristics of each mechanism. This involves a granular analysis of how different components of AI systems (model weights, gradients, training data, inference inputs) are classified under data protection law, addressing the threshold question of whether algorithmic parameters constitute "personal data" subject to transfer restrictions.

The analysis is informed by emerging scholarship on privacy-enhancing technologies and their regulatory recognition [Gajula 2025; Perboli et al. 2025]. Finally, the methodology employs a sectoral stress-testing approach, applying the general legal-technical findings to three distinct fintech use cases—credit scoring, anti-money laundering, and robo-advisory—to account for variations in data sensitivity and regulatory expectations [Horobets et al. 2025; Remolina 2025]. This multi-layered approach ensures that the proposed compliance pathways are not only legally sound but also practically applicable across the diverse landscape of financial technology applications.

4. The Regulatory Landscape: A Clash of Sovereignties

The feasibility of cross-border fintech AI integration between the European Union and the People's Republic of China cannot be assessed without a deep understanding of the foundational legal philosophies that govern data and technology in each jurisdiction. These are not merely technical differences in statutory language; they represent a fundamental clash of sovereignties. The EU has constructed its digital regulatory architecture upon the inviolable foundation of fundamental human rights, viewing data protection as an extension of individual dignity. In stark contrast, China's framework proceeds from a collectivist paradigm where data is a strategic national asset, and its governance is inextricably linked to state security and social stability [Deshpande 2025; Lia, Lic 2025]. This philosophical chasm renders traditional harmonization efforts politically untenable and creates the compliance trap for fintech firms operating across both markets.

The European Union's approach is epitomized by the General Data Protection Regulation (GDPR), which has served as a global benchmark since its implementation. The GDPR's Chapter V establishes a territorial regime for personal data, strictly limiting transfers to "third countries" unless they ensure an "adequate level of protection." This adequacy designation is a political act, granted only to countries whose legal framework is deemed essentially equivalent to the EU's. As scholars have noted, China is unlikely to receive such a designation due to persistent and fundamental concerns regarding pervasive state surveillance and the obligations imposed by its National Intelligence Law, which compels organizations to cooperate with state intelligence activities [Deshpande 2025; Mahmutovic 2025]. In the absence of adequacy, firms must rely on "appropriate safeguards," such as Standard

Contractual Clauses [SCCs]. However, the Court of Justice of the European Union's landmark Schrems II ruling requires firms to conduct a Transfer Impact Assessment [TIA] to verify that the legal system of the recipient country does not undermine the protections of the SCCs. Given the broad powers of Chinese state authorities to access data, any TIA for a transfer to China would almost inevitably conclude that the safeguards are insufficient, effectively blocking the transfer of EU personal data to Chinese territory.

Adding another layer of complexity is the newly finalized EU AI Act, which introduces a risk-based taxonomy for artificial intelligence systems. Fintech applications central to modern banking—such as credit scoring, identity verification, and risk assessment—are classified as "high-risk" [Mahmutovic 2025; Raddatz, Green 2025]. This classification subjects them to a stringent set of requirements, including mandatory fundamental rights impact assessments, high-quality data governance to mitigate bias, and rigorous human oversight. For a European fintech seeking to deploy a model trained in China, the AI Act creates an immediate hurdle. It demands transparency into the model's training data and decision-making logic. If the model is a "black box" from a jurisdiction with different transparency norms, or if its training data provenance cannot be fully audited to ensure it is free from biases that could lead to discriminatory outcomes in the EU, it will fail to meet the AI Act's compliance bar. The EU's regulatory philosophy, therefore, effectively mandates that any AI system operating within its borders must be explainable and accountable according to European standards [Horobets et al. 2025].

China's regulatory trajectory, while resulting in equally powerful barriers to data flows, originates from a fundamentally different set of priorities centered on state security and control. The tripartite framework of the Cybersecurity Law (CSL), the Data Security Law (DSL), and the Personal Information Protection Law (PIPL) constructs data not merely as an economic asset but as a critical strategic resource. The DSL is particularly significant, as it introduces a hierarchical classification system—distinguishing between "general," "important," and "core" data—with increasingly stringent localization requirements attached to higher categories [Akhmatova 2025]. Buysse and Essers [2022] pose critical questions regarding China's digital trajectory, arguing that the combination of state surveillance infrastructure and data localization requirements creates fundamental incompatibilities with Western liberal democratic models—a diagnosis that aligns with the 'clash

of sovereignties' thesis advanced here [Buysse, Essers 2022]. "Important data," a broadly defined category that can encompass financial market analytics, transaction patterns, or aggregate consumer profiles, is subject to strict controls. Its transfer outside of China is not a matter of corporate policy but requires a mandatory security assessment by the Cyberspace Administration of China [CAC], a process characterized by its opacity, discretionary nature, and potential to deny outbound flows on national security grounds.

The operationalization of this regime is further detailed in the CAC's Measures for the Security Assessment of Outbound Data Transfer [2022]. These measures mandate government approval before any data processor meeting certain quantitative thresholds—such as processing the personal information of over one million individuals—can transfer data abroad. This effectively ensnares any major fintech firm with a substantial user base. Furthermore, the Interim Measures for the Management of Generative Artificial Intelligence Services [2023] introduce a content compliance barrier that is particularly relevant for AI models. They require that training data align with "socialist core values," creating a significant obstacle for models developed in liberal democratic contexts, which may be trained on datasets containing content deemed politically unacceptable in China [Lia, Lic 2025]. As Bassens, Fang, and Pascal [2025] argue, China's strategy is a deliberate assertion of "sovereignty across the cloud finance stack," constructing a digital bulwark to insulate its financial system from external influence and perceived technological domination [Bassens et al., 2025]. The spatial dimensions of China's digital expansion into Europe are mapped by Casagrande and Dallago [2025], whose analysis of BRI developments reveals the physical infrastructure underpinning digital sovereignty claims [Casagrande, Dallago 2025]. Huang et al. [2025] provide empirical comparative analysis of digital economy impacts on sustainable growth in China and the EU, quantifying the economic stakes underlying regulatory divergence [Huang et al. 2025].

The conflict point, therefore, is absolute and multi-layered. The EU's GDPR and AI Act create a regime of conditional openness, but one that conditions are impossible to meet for a jurisdiction like China due to its surveillance laws and lack of independent oversight. Simultaneously, China's DSL and PIPL create a regime of conditional exit, where the outflow of data is presumptively restricted and subject to unpredictable state approval. A model cannot travel from China to the EU for training without potentially violating

Chinese export controls. Data cannot travel from the EU to China for inference without violating the GDPR. This creates the logistical impasse described in the literature as "algorithmic balkanization", where the global financial infrastructure threatens to fragment into discrete, incompatible technological spheres [Katterbauer 2024]. Resolving this impasse requires moving beyond the traditional paradigm of data movement and towards architectures that respect both sovereignties by keeping data home while allowing algorithms to travel.

5. Defining the Transfer: Model Weights vs. Personal Data

The viability of cross-border fintech AI integration between the European Union and China hinges on a threshold legal question that has yet to receive definitive adjudication from either jurisdiction's highest courts: does the transfer of an artificial intelligence model constitute a transfer of personal data? The answer to this question determines whether the formidable barriers erected by Chapter V of the GDPR and the Cyberspace Administration of China's outbound transfer regulations apply to the movement of algorithmic artifacts across borders. If model weights and parameters fall outside the scope of "personal data," then the entire architecture of data localization regimes becomes irrelevant to AI model transfers, opening pathways for cross-border deployment that would otherwise remain foreclosed. Yet if these mathematical representations retain sufficient linkage to the individuals whose data enabled their creation, then the same sovereignty conflicts that obstruct raw data flows will equally obstruct algorithmic collaboration. This section unpacks this complex question by examining the technical nature of trained models, the evolving guidance from European data protection authorities, and the distinct risks posed by membership inference and model inversion attacks that complicate any simple classification.

This conceptual distinction finds empirical support in the comparative compliance analysis presented in Figure 1, which quantifies the regulatory requirements triggered by different categories of cross-border data transfers. The figure illustrates a fundamental compliance hierarchy: raw personal data transfers face the most stringent requirements under both regimes, necessitating either adequacy decisions [EU] or CAC security assessments [China]—pathways that are politically and practically unavailable in the bilateral context. Model weights occupy an intermediate

position, where classification remains contested but where arguments for non-personal status offer potential compliance relief. Critically, the figure demonstrates that the legal treatment of gradients and aggregated analytics remains ambiguous under both GDPR and PIPL, creating the uncertainty that federated learning architectures must address through differential privacy enhancements.

The synthetic data pathway offers an alternative approach to this classification dilemma. Generative AI models trained on Chinese data can produce synthetic datasets that mimic the statistical properties of real financial information without containing actual personal identifiers. If an EU fintech can utilize such models to generate synthetic data within EU jurisdiction—or receive pre-generated synthetic datasets from China—the resulting artificial data may fall outside the scope of personal data protection regimes entirely. The European Data Protection Board's guidance on anonymization suggests that if re-identification risk is negligible, data ceases to be personal. Synthetic data, properly generated with rigorous privacy-utility trade-off testing, can achieve this standard. However, scholars caution that the "synthetic" label is not a legal safe harbor; if synthetic data can be reverse-engineered to reveal real identities through linkage attacks or if the generative model itself has memorized and reproduces actual training data points, data protection law applies. Perboli, Simionato, and Pratali emphasize that technical solutions alone cannot resolve legal uncertainties; regulatory recognition of specific technical standards for synthetic data generation remains essential for creating predictable compliance pathways [Perboli et al., 2025]. Okuno and Okuno [2025] provide a comparative analysis of liability protection for AI service participants across jurisdictions, offering frameworks relevant to allocating responsibility when China-trained models cause harm in EU markets [Okuno, Okuno, 2025]. Until such recognition emerges, fintechs utilizing synthetic data must conduct case-by-case assessments of re-identification risks and document their methodology to demonstrate compliance with both EU and Chinese requirements.

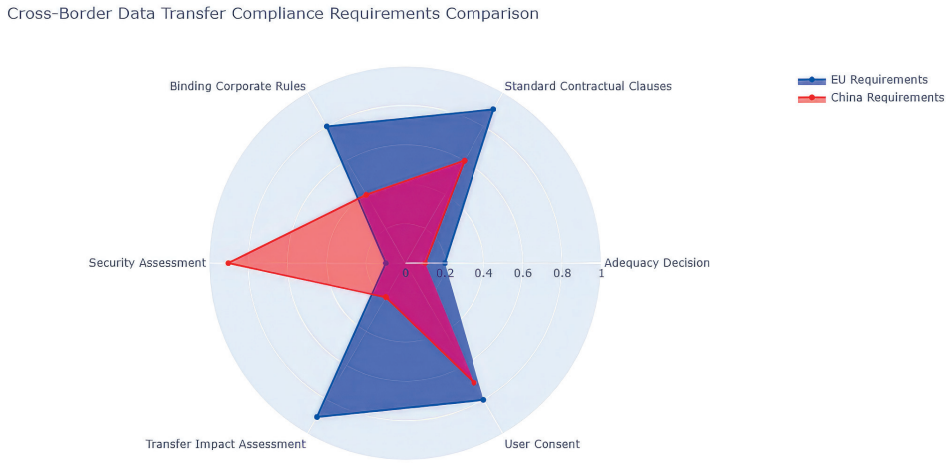

Figure 1: Cross-Border data transfer compliance requirements comparison.

The classification question ultimately resists simple resolution because it sits at the intersection of rapidly evolving technical capabilities and deliberately principle-based legal standards. The GDPR's definition of personal data—any information relating to an identified or identifiable natural person—was crafted to be technology-neutral and adaptable to unforeseen developments. Whether model weights and gradients fall within this definition depends not on their mathematical form but on whether they retain the capacity to identify individuals given the state of technology and the means reasonably likely to be used for identification. As model inversion and membership inference attacks become more sophisticated, the boundary between model and data blurs.

6. Pathways for EU Fintechs Using China-Trained AI and vice versa

The preceding analysis has established that conventional mechanisms for cross-border data transfers—adequacy decisions, standard contractual clauses, and binding corporate rules—face fundamental and likely insurmountable obstacles in the EU-China context. The philosophical chasm between the GDPR's fundamental rights orientation and China's state security paradigm, compounded by specific legal impediments such as China's National Intelligence Law and the EU's Schrems II jurisprudence, renders traditional data movement architectures legally untenable. For fintech firms seeking

to leverage artificial intelligence capabilities across both jurisdictions, this diagnosis demands innovative approaches that decouple algorithmic collaboration from raw data transfer. The viable pathways forward share a common architectural principle: data must remain within its home jurisdiction while algorithms—whether in the form of model weights, gradients, or synthetic representations—traverse borders under conditions that minimize re-identification risks and satisfy both regulatory regimes' core requirements. This section examines three principal pathways for EU fintechs seeking to utilize China-trained AI models, followed by complementary pathways for Chinese fintechs seeking access to European AI capabilities, assessing their legal viability, technical feasibility, and remaining compliance challenges.

This pathway, however, confronts significant challenges arising from the EU AI Act's transparency and data governance requirements. The AI Act classifies fintech applications such as credit scoring and identity verification as "high-risk" systems, subjecting them to stringent obligations regarding the quality and provenance of training data [Mahmutovic 2025]. Article 10 of the AI Act requires that high-risk AI systems be trained on datasets that are relevant, representative, and free from errors and biases. For an EU fintech deploying a China-trained model, satisfying this requirement necessitates understanding the composition and characteristics of the data upon which the model was originally trained. Chinese vendors may prove reluctant to disclose detailed information about training data provenance, citing both trade secret protection and, in some cases, state security concerns regarding the aggregation of financial data. The Interim Measures for the Management of Generative Artificial Intelligence Services further complicate matters by requiring that training data align with "socialist core values," a criterion that may be satisfied for Chinese domestic deployment but raises questions about suitability for European populations with different cultural and legal expectations [Lia, Lic 2025].

Mitigating these challenges requires contractual innovation and technical auditing mechanisms. EU fintechs should negotiate contractual warranties from Chinese vendors regarding the composition of training data, including representations that the data was lawfully obtained, that it does not contain unlawfully processed personal information, and that it meets basic standards of representativeness for the intended European use case. These contractual protections, while valuable for allocating risk, do not substitute

for independent verification. Third-party auditing of the model's bias characteristics and security properties should be conducted before deployment, potentially by EU-based certification bodies with expertise in both AI testing and regulatory requirements. The audit should assess whether the model exhibits discriminatory patterns when applied to European demographic groups, whether it is vulnerable to adversarial attacks, and whether its decision-making processes can be explained with sufficient clarity to satisfy regulatory expectations [Remolina 2025]. Where the model's complexity precludes full explainability—as with deep neural networks—firms must implement compensating governance measures, including human oversight mechanisms that satisfy Article 22 of the GDPR's prohibition on solely automated decision-making with legal effects.

The legal viability of this approach turns on the classification of gradients under data protection law. The European Data Protection Board has not issued definitive guidance specifically addressing gradients, but its general approach to anonymization and pseudonymization suggests that gradients can constitute personal data if they permit re-identification of the individuals whose data generated them [Gajula 2025]. From the Chinese regulatory perspective, the inbound receipt of differentially private gradients presents distinct compliance questions. China's Data Security Law establishes a hierarchical classification system for data, with "important data"—a category that can encompass aggregated financial information revealing patterns about market infrastructure or systemic vulnerabilities—subject to stringent controls [Akhmatova 2025]. If the aggregated gradients from multiple EU fintechs, when combined, reveal patterns about European financial markets that Chinese regulators deem relevant to national security interests, the receipt of such gradients could trigger notification obligations or even require security assessments. The Cyberspace Administration of China's implementing regulations grant authorities broad discretion in determining what constitutes important data, creating uncertainty for firms attempting to structure compliant feedback loops. Chinese fintechs participating in federated learning arrangements should engage proactively with regulators, seeking guidance on whether specific gradient aggregation schemes trigger important data classifications and what compliance measures are required.

However, scholars caution that the "synthetic" label is not a legal safe harbor [Perboli et al. 2025]. If the generative model has memorized portions of its

training data—a known risk with complex neural networks, particularly when training data contains duplicates or unusual records—the synthetic outputs may inadvertently reproduce actual personal information. Moreover, even if individual synthetic records are not direct copies, linkage attacks might combine synthetic data with auxiliary information to re-identify individuals whose statistical patterns appear in the synthetic distribution. Fintechs pursuing this pathway must implement rigorous testing protocols to verify that synthetic data meets genuine anonymity standards. These protocols should include membership inference attack simulations to assess whether the generative model reveals information about its training set, distance to closest record metrics to detect memorization, and combinatorial analysis to evaluate re-identification risks when synthetic data is combined with publicly available information.

Recent regulatory developments offer partial relief. The CAC's Provisions on Promoting and Regulating Cross-Border Flow of Data [2024] establish exemptions from security assessment requirements for certain categories of transfers. If the data to be transferred is not classified as important data and falls below the quantitative thresholds—personal information of fewer than 100,000 individuals accumulated since January 1 of the current year—a security assessment is not required. This creates opportunities for Chinese fintechs to segment their data operations, distinguishing between sensitive financial data that must remain within China and non-sensitive operational data that can be processed internationally. For example, a Chinese fintech might maintain all customer transaction data on domestic servers while transferring aggregated, anonymized business intelligence to European partners for joint research or model development. The critical challenge lies in the breadth of the "important data" category, which the People's Bank of China may interpret expansively to encompass aggregate market analytics, systemic risk indicators, or cross-institutional transaction patterns [Dong, Zhang 2024].

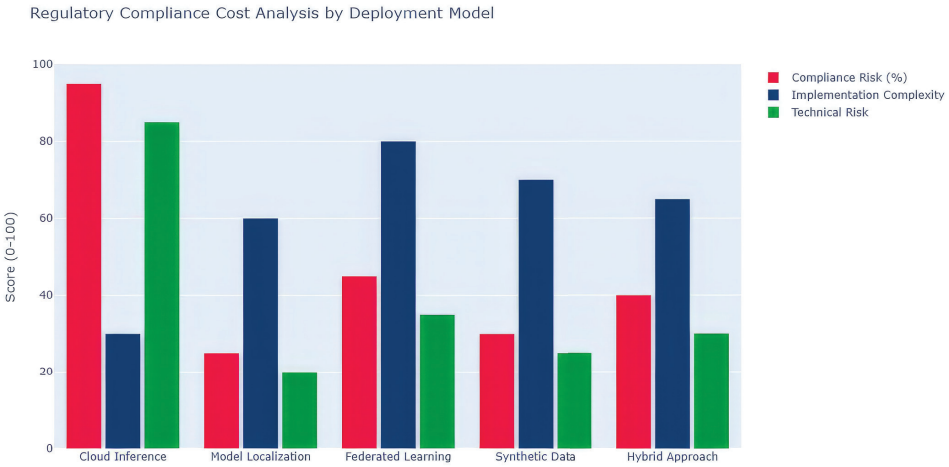

Figure 2: Regulatory compliance cost analysis by deployment model.

Data clean rooms represent an emerging technical-legal hybrid particularly suited to collaborative analytics between Chinese and EU fintechs. A data clean room is a trusted execution environment—typically operated by a neutral third party—into which both parties upload encrypted data. Computations occur within the clean room, and only the results—aggregated statistics, model outputs, "hit/no-hit" indicators—are revealed to participants. The underlying data remains encrypted and inaccessible to both the counterparty and the clean room operator. For EU-China collaboration, a clean room could enable joint anti-money laundering analytics without exposing transaction data across borders, or collaborative model training without revealing customer information. The legal viability depends on both jurisdictions recognizing the clean room's security protocols as providing adequate protection. Currently, no mutual recognition exists between EU and Chinese authorities regarding specific clean room technologies or operators, creating uncertainty that firms must address through case-by-case regulatory engagement [Perboli et al. 2025]. Pilot projects conducted within regulatory sandboxes could establish precedents and technical standards that, over time, evolve into recognized compliance pathways. Beyond compliance considerations, Jain [2024] situates fintech innovation within sustainable development objectives, suggesting that cross-border AI collaboration, properly structured, could advance broader policy goals beyond mere regulatory adherence [Jain,

2024]. The intersection of AI, blockchain, and sanctions compliance receives attention in Hung's [2024] analysis of how emerging technologies facilitate or complicate international sanctions regimes—directly relevant to the AML challenges examined in Section 7 [Hung 2024].

The comparative compliance cost analysis presented in Figure 2 quantifies the economic implications of the architectural choices examined throughout this section. The figure demonstrates that on-premise model localization—while requiring substantial upfront investment in auditing and governance infrastructure—achieves the lowest long-term compliance risk profile by avoiding cross-border data transfer triggers entirely. Federated learning architectures, though technically sophisticated, incur moderate compliance costs due to ongoing uncertainty regarding the classification of gradient transmissions and the necessity for differential privacy implementation. Cloud-based processing, conversely, emerges as the highest-risk and highest-cost option, as it triggers the full panoply of both EU and Chinese transfer restrictions without offering compensating compliance benefits. The visualization reinforces a central policy recommendation: fintech firms should prioritize architectural investments that eliminate cross-border data movement, even where such investments require higher initial capital expenditure, as the avoided compliance costs and litigation risks yield superior long-term outcomes. For Chinese fintechs specifically, the EU subsidiary model—while carrying the highest establishment costs—effectively eliminates recurring transfer compliance expenses by creating a permanent jurisdictional firewall between EU personal data and Chinese parent operations.

7. Sector-Specific Challenges in Fintech

Looking beyond current fintech applications, Aron [2025] examines the legal architecture of digital money, including cryptocurrencies and CBDCs, suggesting that the AI governance questions examined here will intersect with broader monetary sovereignty debates in the coming decade [Aron, 2025]. Stress-testing the proposed compliance architectures against these specific use cases reveals that while the principle of "data stay, model move" remains valid across all applications, its implementation must be calibrated to address sector-specific constraints arising from both financial regulation and data protection law.

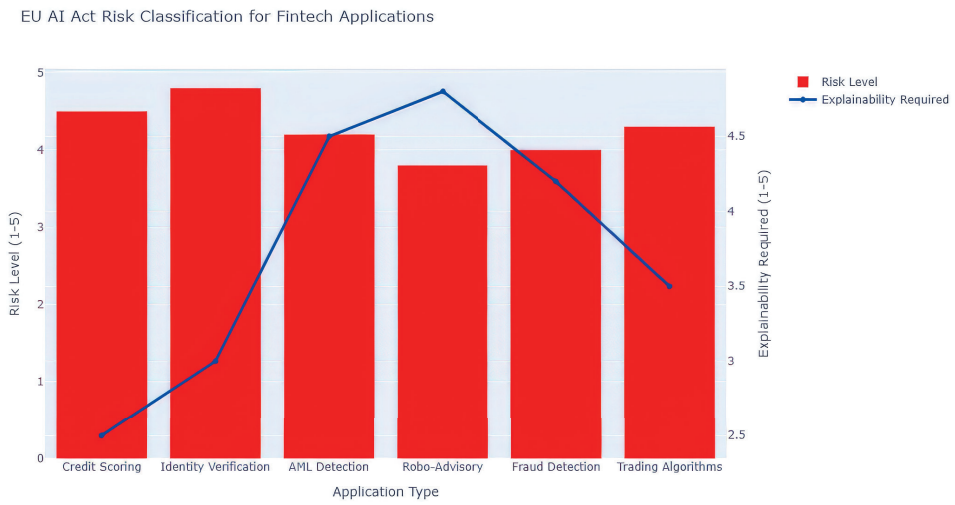

Figure 3: EU AI Act risk classification for fintech applications.

The EU AI Act's risk-based taxonomy, illustrated in Figure 3, provides the regulatory framework that mandates such sectoral calibration. The Act classifies credit scoring and underwriting systems as 'high-risk' under Annex III, subjecting them to mandatory fundamental rights impact assessments, stringent data governance requirements, and ongoing human oversight obligations. Anti-money laundering applications, while not explicitly listed, attract comparable scrutiny through the combination of financial regulatory requirements and the Act's general provisions for systems impacting individuals' access to financial services. Robo-advisory platforms, by contrast, may qualify for the Act's transparency obligations without the full panoply of high-risk requirements, provided they can demonstrate that investment recommendations are explainable and subject to appropriate human oversight. This classification hierarchy explains the differentiated compliance burdens illustrated in subsequent figures and grounds the sector-specific analysis that follows. Ghoshal [2025] addresses cross-border AI governance specifically in the legal technology context, offering parallel insights regarding standardization of ethical and legal norms that inform the financial sector analysis presented here [Ghoshal 2025]. For cross-border AI deployment, the AI Act's risk classification operates as a gateway: high-risk designation triggers obligations regarding training data provenance and algorithmic transparency that Chinese-developed models may struggle to satisfy without

substantial modification and auditing, whereas lower-risk applications may proceed with comparatively streamlined compliance verification.

Credit scoring and underwriting represent the most sensitive category of fintech applications, involving the processing of personal data that directly determines individuals' access to financial services and, by extension, their participation in economic life. The regulatory landscape for credit scoring is exceptionally stringent in both jurisdictions, though for different reasons. In the European Union, Article 22 of the GDPR establishes a qualified prohibition on solely automated decision-making that produces legal effects or similarly significantly affects data subjects. This provision, interpreted consistently by the European Data Protection Board and national supervisory authorities, requires that decisions with legal consequences—including credit denials—cannot rest entirely on algorithmic processing without meaningful human intervention. Data subjects must have the right to obtain human intervention, to express their point of view, and to contest the decision. The EU AI Act reinforces these requirements by classifying credit scoring systems as "high-risk" under Annex III, subjecting them to mandatory fundamental rights impact assessments, stringent data governance requirements, and ongoing human oversight obligations [Mahmutovic 2025; Raddatz, Green 2025]. The Act's transparency provisions further require that deployers of high-risk systems provide clear explanations of the logic involved, the significance of the processing, and the consequences of such processing.

The viable pathway for AML applications involves limiting cross-border data sharing to "hit/no-hit" indicators rather than full transaction profiles, and ensuring that screening algorithms are transparent and auditable. Rather than transmitting transaction data across borders for analysis, fintechs should deploy locally hosted models that generate alerts within the jurisdiction. When suspicious activity is detected, only the alert—stripped of underlying transaction data—should be shared with counterparties or regulators as required by law. This approach satisfies the GDPR's data minimization principle and avoids triggering cross-border transfer restrictions, while still enabling collaborative AML efforts. For sanctions screening specifically, fintechs must maintain jurisdiction-specific screening lists and ensure that models are trained to apply the correct legal standards. As Horobets et al. [2025] emphasize in their analysis of AI technologies in banking, explainability is particularly critical in AML contexts, as financial institutions must be able

to demonstrate to regulators why specific transactions were flagged and how screening decisions were reached [Horobets et al. 2025]. Complex deep learning models that cannot explain their decisions may satisfy data protection requirements but fail fundamental regulatory obligations in financial services. For cross-border AML collaboration involving government authorities, the preferred pathway is intergovernmental cooperation through established channels such as Interpol or bilateral treaties, rather than private fintech data transfers that would face insurmountable legal obstacles.

If a model cannot explain why it recommended a particular portfolio allocation—if its decision-making process is opaque even to its operators—then it cannot satisfy suitability requirements regardless of its predictive accuracy. This necessitates the use of "explainable AI" [XAI] architectures that trade some predictive power for interpretability. Simpler models such as decision trees, logistic regression, or rule-based systems may be preferable to deep neural networks for advisory applications, even if they achieve marginally lower accuracy, because their decision-making processes can be audited and explained.

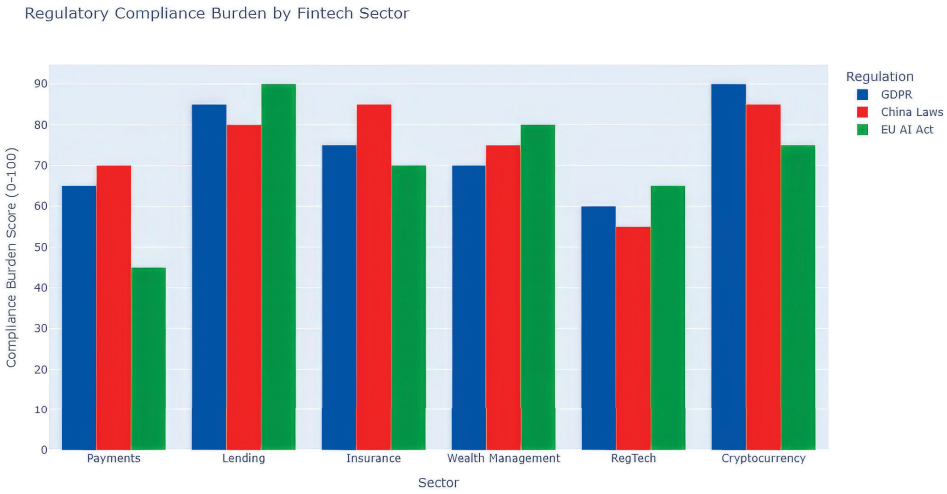

Figure 4: Regulatory compliance burden by Fintech sector.

Figure 4 illustrates the varying regulatory compliance burden across fintech sectors, confirming that credit scoring and AML applications face the highest compliance costs due to the combination of data protection requirements and sector-specific financial regulations. Robo-advisory services, while subject to substantial fiduciary obligations, benefit from the availability of explainable AI architectures that can satisfy both regulatory expectations and data protection requirements. Figure 5 presents a risk assessment matrix for cross-border AI deployment, demonstrating that credit scoring carries the highest combination of data sensitivity and regulatory scrutiny, while robo-advisory occupies a middle position, and certain payment processing applications may face lower barriers. These sectoral variations counsel against one-size-fits-all compliance strategies. Fintechs must calibrate their approach to AI deployment based on the specific applications they pursue, the jurisdictions in which they operate, and the regulatory expectations that attach to different financial activities. The technical-legal hybrids examined in Section 6 remain viable across all sectors, but their implementation must be tailored to address the distinct challenges posed by credit scoring, AML, and robo-advisory applications. Central bank digital currencies represent the next frontier of financial technology regulation, and as Bílek [2025] argues, their design will fundamentally implicate the same data sovereignty questions this article addresses regarding AI models [Bílek 2025].

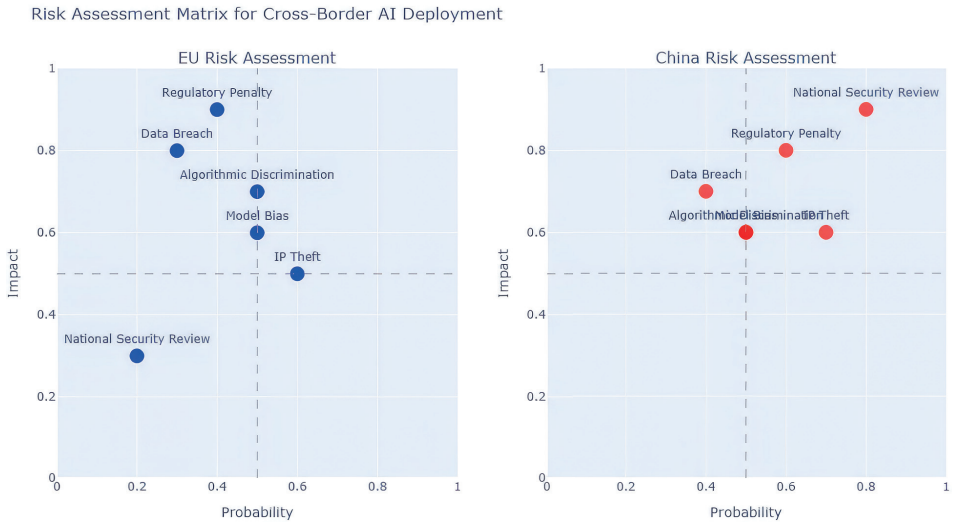

Figure 5: Risk assessment matrix for cross-border AI deployment.

8. Future Outlook and Conclusion

The trajectory of EU-China fintech AI integration confronts an unavoidable reality: the era of frictionless cross-border data flows has yielded to an age of sovereign computing, wherein regulatory fragmentation compels fundamental rethinking of technological architecture. The preceding analysis demonstrates that while traditional legal mechanisms—adequacy decisions, standard contractual clauses, and binding corporate rules—face insurmountable obstacles in the current geopolitical climate, technical-legal hybrids offer viable pathways for preserving cross-border algorithmic collaboration. The viability of these pathways, however, depends critically on sector-specific calibration. As Figures 4 and 5 illustrate, the regulatory compliance burden varies substantially across fintech applications, with credit scoring and anti-money laundering facing the highest combination of data sensitivity and regulatory scrutiny, while certain payment processing applications encounter comparatively lower barriers. This heterogeneity counsels against one-size-fits-all compliance strategies and demands tailored approaches that account for the distinct risk profiles and regulatory expectations attaching to different financial activities.

For EU fintechs seeking to leverage Chinese AI capabilities, the viable pathway lies in model localization—importing pre-trained weights while processing all inference data within EU jurisdiction—supplemented by rigorous auditing to satisfy the EU AI Act's transparency and data governance requirements [Mahmutovic 2025]. For Chinese fintechs seeking access to European AI capabilities, the pathway involves establishing EU-based subsidiaries that operate as independent data controllers, combined with strict data segmentation that distinguishes between sensitive financial data requiring domestic retention and anonymized business intelligence suitable for international collaboration [Dong, Zhang 2024]. In both directions, privacy-enhancing technologies—particularly federated learning enhanced with differential privacy and synthetic data generation verified through rigorous anonymity testing—serve as the critical bridge between conflicting legal regimes [Gajula 2025; Perboli et al. 2025]. Figure 6's effectiveness matrix confirms that combinations of multiple PETs achieve superior privacy protection compared to standalone implementations, though each introduces trade-offs between utility and compliance that require careful calibration.

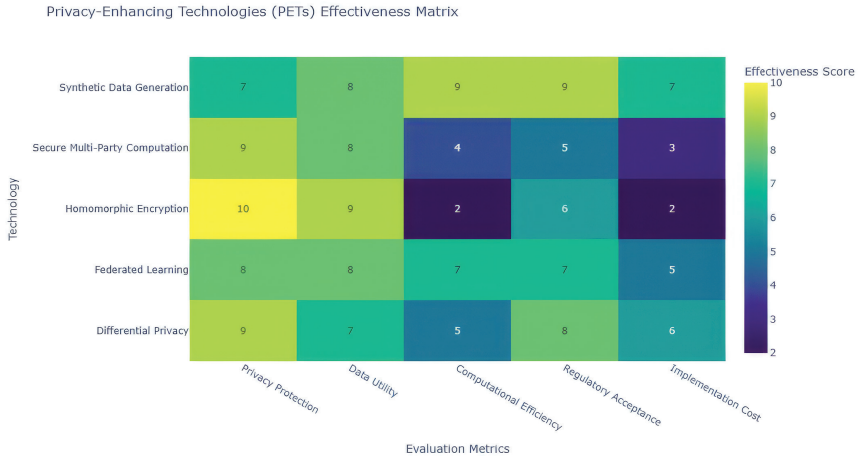

Figure 6: Privacy-enhancing technologies [PETs] effectiveness matrix.

Looking forward, regulatory sandboxes established jointly by the European Securities and Markets Authority and the People's Bank of China offer the most promising mechanism for generating empirical evidence on the risks and benefits of cross-border AI data flows. The trajectory projected in García-Herrero et al.'s [2017] comprehensive forecast of EU-China economic relations to 2025 has largely been validated by subsequent developments, though the intensity of regulatory fragmentation they anticipated has exceeded even their prescient analysis [García-Herrero et al. 2017]. Such sandboxes could enable limited pilot projects testing specific technical architectures under close supervisory oversight, potentially yielding tailored exemptions or sector-specific adequacy findings that create predictable compliance pathways. Simultaneously, industry bodies should pursue harmonization of technical standards for encryption, anonymization, and privacy-enhancing technologies through bilateral adoption of ISO/IEC frameworks. If both jurisdictions accept that specific differential privacy parameters render data effectively anonymous, legal friction decreases substantially even as substantive laws remain divergent. Contractual innovation must advance beyond standard clauses to develop AI-specific provisions addressing model inversion risks, gradient privacy, and liability for algorithmic bias, with regulatory pre-approval transforming such clauses into safe harbors.

Ultimately, fintech firms that treat data localization not as a barrier but as a design constraint will survive regulatory fragmentation. Those attempting to circumvent these rules through creative interpretations of ambiguous

provisions face existential legal risks. The future of cross-border fintech AI lies not in harmonizing substantive laws—a politically unrealistic objective—but in developing architectures that enable algorithms to travel while keeping data home. This is the defining challenge of sovereign computing, and its successful navigation will determine whether the financial sector fragments into incompatible technological spheres or preserves sufficient cross-border collaboration to sustain innovation in an age of regulatory divergence.

References

Akhmatova, D.-M.: Beyond the Western model? China's approach to anti-monopoly regulation of tech markets in the AI age and lessons for global peers. Peking University Law Journal, 13(2), 201–226, 2025.

Araya, D., Peters, M. A.: Chinese globalization: BRI and the future of higher education. Beijing International Review of Education, 4(4), 654–672, 2023.

Aron, O.: The Legal Architecture of Digital Money: Cryptocurrencies, CBDCs, Tokenisation and the Reconfiguration of Global Financial Regulation. CBDCs, Tokenisation and the Reconfiguration of Global Financial Regulation, 2025. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5914142, accessed: December 12th, 2025.

Badawy, W.: Algorithmic sovereignty and democratic resilience: Rethinking AI governance in the age of generative AI. AI and Ethics, 5(5), 4855–4862, 2025.

Bassens, D., Fang, C.,, Pascal, U.: Striving for sovereignty across the cloud finance stack: A relational comparison of the United States, the European Union, and China. Finance and Society, 1–21, 2025.

Bílek, L.: The Role of Central Bank Digital Currencies in Strengthening Financial Resilience. Financial Law Review, (39(3)), 1–25, 2025.

Buysse, K., Essers, D.: Should we fear China's brave new digital world? NBB Economic Review, 1–31, 2022.

Casagrande, S., Dallago, B.: Mapping China's Belt and Road Initiative in Europe: Developments and Challenges. Economies, 13(10), 301, 2025.

da Fonseca Azevedo, M.: Navigating the AI Frontier in International Trade Law: The Role of the WTO's TBT Agreement. World Trade Institute, Universität Bern, 2024. Available at: https://www.wti.org/media/filer_public/e6/c9/e6c95836-db63-4320-80b3-dc424521ef07/navigating_the_ai_frontier_in_int_trade_law.pdf, accessed: December 12th, 2025.

Dacev, N., Ibish, M.: Legal Arrangements of Artificial Intelligence in the European Union and the Republic of North Macedonia. Eur. J. Privacy L., Tech., 79, 2024.

Demergis, J.: Technology and Geopolitics: Convergence and Impact on International Relations and Geostrategy, (in:) F. Lemieux, M. P. Efthymiopolous, J. Demergis, Geopolitical Challenges to the Global Influence of Western Society, Emearld Publishing: 2025.

Deshpande, A.: AI regulation and policy pathways in China, European Union, and the USA, 2025.
Available at: https://www.econstor.eu/handle/10419/331266, accessed: December 12th, 2025.

Dong, B.,, Zhang, Z.: AI-driven framework for compliance risk assessment in cross-border payments: Multi-jurisdictional challenges and response strategies. Spectrum of Research, 4(2), 2024.
Available at: http://spectrumofresearch.com/index.php/sr/article/view/20, accessed: December 12th, 2025.

Gajula, S.: Federated intelligence in financial ecosystems: A privacy-preserving AI framework for cross-border risk analysis. Journal of Information Systems Engineering and Management, 10, 1040–1048, 2025.

García-Herrero, A., Kwok, K. C., Xiangdong, L., Summers, T.,, Yansheng, Z.: EU–China Economic Relations to 2025. Building a Common Future, Report by Chatham House, Bruegel, the China Center for International Economic Exchanges (CCIEE) and the Chinese University of Hong Kong, The Royal Institute of International Affairs, 2017.
Available at: https://www.bruegel.org/sites/default/files/wp-content/uploads/2017/09/CHHJ5627_China_EU_Report_170908_EMBARGOED.pdf, accessed: December 12th, 2025.

Ghoshal, R. Cross-border AI governance for legal tech: Standardizing ethical and legal norms in access to justice. International Journal of Law Justice and Jurisprudence, 5(1), 186–194, 2025.

Gordon, D.,, Nouwens, M.: The digital Silk Road: China's technological rise and the geopolitics of cyberspace. Taylor, Francis, 2022.
Available at: https://books.google.com/books?hl=en&lr=&id=gXqfEAAAQBAJ&oi=fnd&pg=PA1989&dq=SOVEREIGN+ALGORITHMS,+BORDERLESS+FINANCE:+NAVIGATING+LEGAL+PATHWAYS+FOR+EU-CHINA+FINTECH+AI+INTEGRATION+&ots=bMuSMtdiH8&sig=owhxcp1EnotPF2x_L58uOZo6LkY, accessed: December 12th, 2025.

Homa, T.: The Future of the Digital Permanent Establishment Concept: Challenges and Obstacles. Financial Law Review, (34(2)), 23–38, 2024.

Horobets, N., Reznik, O., Maliyk, V., Vyhivskyi, I.,, Bobrishova, L.: Artificial intelligence technologies in banking: Challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives. Journal of Money Laundering Control, 28(4–5), 593–608, 2025.

Huang, W., Jin, J.,, Guo, X.: The Impact of Digital Economy on Sustainable Economic Growth: A Comparative Study be-tween China and the European Union. Economics, Management, 6(4), 2025.
Available at: https://masonpublish.wordpress.com/wp-content/uploads/2025/12/14-43-the-impact-of-digital-economy-on-sustainable-economic-growth-a-comparative-study-between-china-and-the-european-union.pdf, accessed: December 12th, 2025.

Hung, A. H.-C.: How AI-enabled blockchain technology facilitates US sanctions on foreign businesses: An analysis based on international regulatory harmonization. Int'l JL Ethics Tech., 151, 2024.

Hussain, F., Hussain, Z., Khan, M. I.,, Imran, A.: The digital rise and its economic implications for China through the Digital Silk Road under the Belt and Road Initiative. Asian Journal of Comparative Politics, 9(2), 238–253, 2024.

Iddrisu, K., Yakubu, I. N.,, Asongu, S. A.: FinTech Innovations for Sustainable Banking. In I. N. Yakubu (Ed.), Strategic Approaches to Banking Business and Sustainable Development Goals (pp. 63–86). Springer Nature Switzerland, 2024.
Jain, S.: Fintech revolution: Role in achieving the sustainable development goals. In Advanced Technologies for Realizing Sustainable Development Goals: 5G, AI, Big Data, Blockchain, and Industry 4.0 Application (pp. 296–312). Bentham Science Publishers, 2024. Available at: https://www.benthamdirect.com/content/books/9789815256680.chapter-21, accessed: December 12th, 2025.

Katterbauer, K.: A Novel Digital Service Taxation, Sustainability Legal Framework Utilizing Artificial Intelligence Analysis of Subsea Cable Data Transmissions. Financial Law Review, 25(1), 146–157, 2022.

Katterbauer, K.: Financial regulation reforms in China – can artificial intelligence be a gamechanger to more sustainable financial regulations. Financial Law Review, 36(4), 1–33, 2024.

Kaya, O., Schildbach, J., AG, D. B.,, Schneider, S.: Artificial intelligence in banking. Artificial Intelligence, 1–9, 2019.

Lia, X.,, Lic, X.: Regulating AI in a Fragmented World: The Diverging Paths of the EU and China and Their Impact on Global Governance. Innovation and Development Policy, 7, 27–47, 2025.

Lu, L. Global fintech revolution: Practice, policy, and regulation. Oxford University Press, 2024.
Available at: https://books.google.com/books?hl=en&lr=&id=KzAFEQAAQBAJ&oi=fnd&pg=PP1&dq=+EU-CHINA+FINTECH+AI+INTEGRATION+&ots=nbjXz5isNB&sig=Q1L3V21t3VjU1LTHLasT3tk4v0Q, accessed: December 12th, 2025.

Mahmutovic, A.: The EU AI Act: A proactive framework for comprehensive AI regulation. International Journal of Law and Information Technology, 33, 2025.

Mirza, N., Elhoseny, M., Umar, M.,, Metawa, N.: Safeguarding FinTech innovations with machine learning: Comparative assessment of various approaches. Research in International Business and Finance, 66, 2023.

Okuno, M. J.,, Okuno, H. G.: Legal frameworks for AI service business participants: A comparative analysis of liability protection across jurisdictions. AI, SOCIETY, 40(7), 2025.

Paleti, S.: Smart finance: Artificial intelligence, regulatory compliance, and data engineering in the transformation of global banking. Deep Science Publishing, 2025.
Available at: https://books.google.com/books?hl=en&lr=&id=-JBeEQAAQBAJ&oi=fnd&pg=PA1&dq=Regulating+artificial+intelligence+in+the+financial+sector++banka&ots=2U5DEpCRHN&sig=1fMitaT0zPwsJs5ykm8pmeyIBBc, accessed: December 12th, 2025.

Perboli, G., Simionato, N.,, Pratali, S.: Navigating the AI regulatory landscape: Balancing innovation, ethics, and global governance. Economic and Political Studies, 13(4), 367–397, 2025.

Raddatz, N. I.,, Green, R.: Navigating Risk and Trust in AI Financial Systems: The Role of Institutional Structures and the EU AI Act. Journal of Information Systems, 1–18, 2025.

Remolina, N.: AI governance and algorithmic auditing in financial institutions: Lessons from Singapore. Journal of Risk Management in Financial Institutions, 18(3), 261–275, 2025.

Ridzuan, N. N., Masri, M., Anshari, M., Fitriyani, N. L.,, Syafrudin, M.: AI in the financial sector: The line between innovation, regulation and ethical responsibility. Information, 15(8), 432, 2024.

Sadati, A., Gramlich, D.,, Walker, T. Artificial Intelligence, Finance, and Sustainability: An Overview. In T. Walker, D. Gramlich,, A. Sadati (Eds.), Artificial Intelligence, Finance, and Sustainability (pp. 3–16). Springer Nature Switzerland, 2024.

Sharma, A., Adekunle, B. I., Ogeawuchi, J. C., Abayomi, A. A.,, Onifade, O.: Governance challenges in cross-border fintech operations: Policy, compliance, and cyber risk management in the digital age. IRE Journals, 4(9), 1–8, 2021.

Tatlow, D. K., Feldwisch-Drentrup, H.,, Fedasiuk, R.: Europe: A technology transfer mosaic. In China's Quest for Foreign Technology (pp. 113–129). Routledge, 2020. Available at: https://www.taylorfrancis.com/chapters/edit/10.4324/9781003035084-10/europe-didi-kirsten-tatlow-hinnerk-feldwisch-drentrup-ryan-fedasiuk, accessed: December 12th, 2025.

Truby, J., Brown, R.,, Dahdal, A.: Banking on AI: Mandating a proactive approach to AI regulation in the financial sector. Law and Financial Markets Review, 14(2), 110–120, 2020.

Zhang, Q.: Navigating the In-Between Space: The Roles of Chinese Think Tanks in Artificial Intelligence Governance. Global Policy, 16(3), 494–500, 2025.

Zhang, Y.,, Bilawal Khaskheli, M.:The role of digital technologies in advancing sustainable economic development into intersections of policy, law, environmental economics, and a comparative study of China, the EU, and the USA. Sustainability, 17(19), 8666, 2025.

Żmuda-Matan, K.: Impact of the So-Called the Budget-Related Act on the Pay Policy of Local Government Entities in Relation to Persons Managing Municipal Companies – Selected Issue. Financial Law Review, (34(2)), 91–108, 2024.