



Nemko
Digital

Digital and AI Regulation in Asian Markets

Emerging Asian Frameworks
in a Global Context

Guide to AI Regulation in Asian Markets

Artificial intelligence (AI) regulation has become a defining feature of digital governance globally. The [EU AI Act](#) represents the world's most comprehensive, binding, and risk-based AI regulatory framework, setting a global benchmark for algorithmic accountability, transparency, and human-rights protection. However, regulatory innovation is not confined to Europe. Major markets in East Asia, including China, Taiwan, South Korea, and Japan, have developed distinct yet increasingly sophisticated approaches to AI and digital regulation tailored to their political systems, economic strategies, and societal values.

Rather than replicating the EU approach, Asian markets have opted for varied regulatory models that combine AI-specific legislation with strong data protection and cybersecurity regimes. This article looks at the key digital and AI regulations of four Asian markets: China, Taiwan, South Korea and Japan.

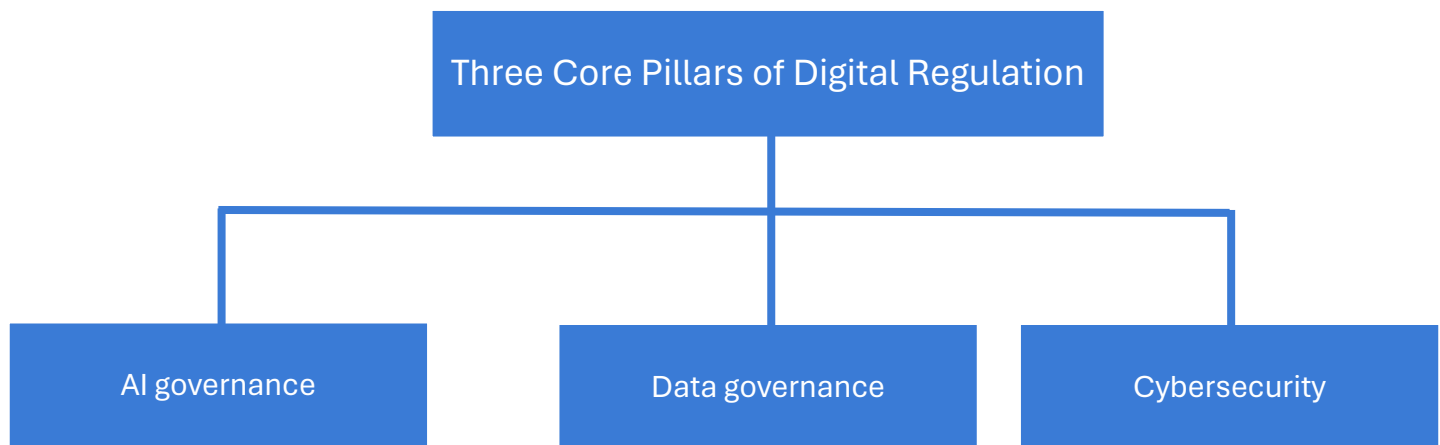


Figure 1: Three core pillars of modern digital regulation—AI governance, data governance, and cybersecurity—around which different jurisdictions, including those in Asia, structure their regulatory approaches

China

AI-specific regulations: Unlike the EU's comprehensive approach, China has adopted a sector-specific [AI regulatory framework](#). Key instruments include the Interim Measures for Generative AI Services, the Provisions on Algorithmic Recommendation, the Provisions on Deep Synthesis Technology, and the Measures on AI-Generated Synthetic Content Identification. Collectively, these instruments form a sector-specific governance regime emphasizing content control, transparency, and traceability across the lifecycle of public-facing AI services.

Personal Information Protection Law (PIPL) & Data Security Law (DSL): The PIPL establishes GDPR-like principles, including purpose limitation, consent, and individual rights, but imposes stricter cross-border data transfer controls. Certain processors, including critical information infrastructure operators and large-scale processors, must pass security assessments administered by the Cyberspace Administration of China (CAC). China's data governance framework is further complemented by the DSL, which applies broadly to all data and introduces a data classification system with heightened protection for important and core data.

Cybersecurity Law (CSL): China's CSL, amended in 2025, sets out general cybersecurity obligations for network operators in China. Key obligations include multi-level protection scheme, incident and vulnerability response and reporting, content management, and security maintenance for products and services. It also introduces enhanced obligations for critical information infrastructure.

Under China's three foundational data and cybersecurity laws, namely the DSL, PIPL and CSL, the State Council, the CAC and other designated and sector-specific authorities are responsible for issuing and enforcing detailed implementing regulations within their respective mandates. The four AI-specific regulations discussed above were promulgated by the CAC pursuant to this framework.

Taiwan

AI Basic Act: Rather than imposing immediate, horizontal, EU-style compliance obligations on private actors, Taiwan's AI Basic Act adopts a high-level and principles-based approach. Detailed operational requirements will be developed by sectoral regulators using a risk classification framework to be issued by the Ministry of Digital Affairs (MODA). For high-risk AI systems, the Act imposes labeling requirements; liability distribution and mechanisms for remedies, compensation, or insurance are to be clarified by the government.

Personal Data Protection Act (PDPA): The PDPA serves as the primary legal framework for personal data protection in Taiwan. Most recently amended in 2025, it comprehensively regulates the collection, processing, and use of personal data by both public and private entities. Enforcement follows a sector-based model, under which designated central authorities supervise compliance within their respective domains and issue sector-specific guidelines consistent with the PDPA's core principles.



Cybersecurity Management Act (CSMA): The CSMA governs information and communications security for government agencies and designated non-government entities. It requires regulated organizations to maintain prescribed cybersecurity levels, implement internal security plans, appoint dedicated cybersecurity personnel, and report incidents. MODA issues supplementary rules on matters such as security classification and product reviews, while sectoral authorities oversee compliance within their jurisdictions.

Personal Information Protection Act (PIPA): The PIPA is the overarching privacy legislation in Korea and one of the strongest data protection regimes in Asia. It has been recognized as providing an “adequate” level of protection under the EU GDPR. The most recent amendment in March 2026 has significantly strengthened enforcement by introducing measures including 10% aggravated surcharge, CEO accountability and mandatory ISMS-P certification for certain controllers, calling for organizations to strengthen their privacy governance.

South Korea

AI Framework Act: South Korea’s [AI Framework Act](#), effective from 22 January 2026, is the closest counterpart to the EU AI Act among the four Asian markets. It introduces transparency obligations for operators of generative AI and high-impact AI, defined as AI systems that may significantly affect human life, safety, or fundamental rights. Operators of high-impact AI are subject to additional requirements, including impact assessments, risk management planning, explainability, user protection measures, human oversight, and documentation. Additionally, enhanced safety obligations apply to operators of AI systems exceeding specified compute thresholds.

Sectoral cybersecurity regulations (Network Act, etc.):

South Korea’s cybersecurity obligations are set out across sector-specific laws. For example, the Network Act governs telecommunications operators and online service providers, the Electronic Financial Transactions Act applies to financial institutions, and critical infrastructure is regulated under the Act on the Protection of Information and Communications Infrastructure. Notably, beyond cybersecurity, the Network Act also emphasizes user protection, and its December 2025 amendment introduced new definitions of “disinformation” and “large-scale information and communications service provider,” reflecting influence from the EU Digital Services Act (DSA).

Japan

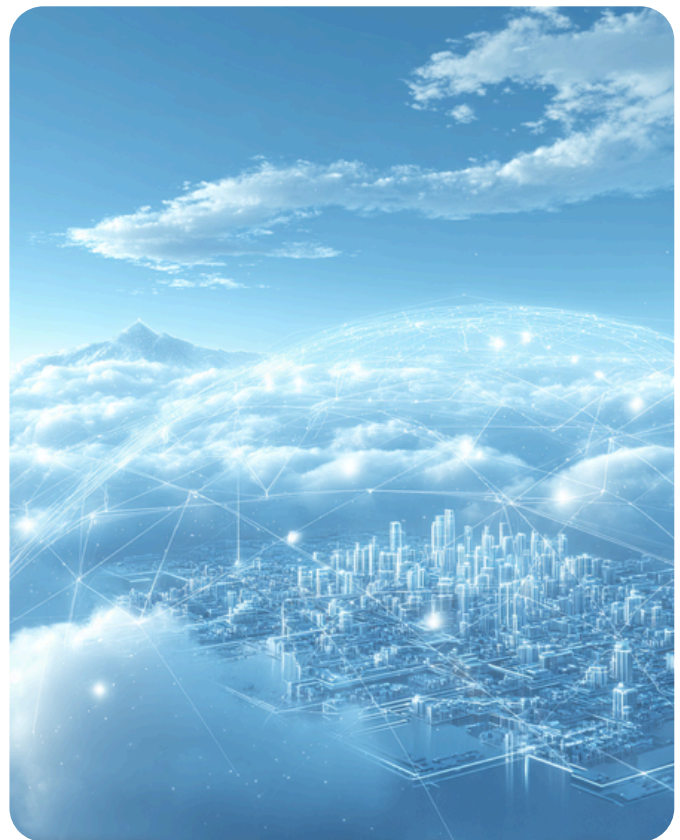
AI Promotion Act: Japan's [AI Promotion Act](#) takes an innovation-first, non-punitive approach that emphasizes voluntary cooperation and technological development rather than binding compliance obligations. Unlike the EU AI Act, it primarily sets out high-level principles and policy directions for AI research, development, and use, while clarifying the respective roles of government, businesses, research institutions, and citizens. The framework primarily relies on guidelines and national strategies instead of enforceable duties or penalties, with AI-related misconduct continuing to be addressed under existing laws.

Act on the Protection of Personal Information (APPI):

APPI is Japan's primary data protection law governing the collection, use, and sharing of personal information. Like South Korea, Japan has received an EU adequacy decision. Enacted in 2003 and amended multiple times, APPI has evolved alongside global privacy standards. A bill recently approved in April 2026 to amend the Act might further update the regime by introducing administrative fines, enhanced protection for children's and certain biometric data, and greater flexibility for personal data use in AI training, combining stricter enforcement with selective regulatory easing.

Basic Act on Cybersecurity & Active Cyber Defence

Act: The Basic Act on Cybersecurity establishes Japan's cybersecurity foundation, setting out the responsibilities of the government and encouraging critical infrastructure operators and businesses to strengthen security measures. The Active Cyber Defence Act, enacted in 2025, expands proactive government response capabilities and enhances information-sharing and incident-response coordination with key private-sector stakeholders. In addition, sector-specific cybersecurity obligations are imposed in areas such as finance and healthcare in sectoral legislation.



	China	Taiwan	South Korea	Japan
AI-specific framework	Multiple CAC regulations	AI Basic Act	AI Framework Act	AI Promotion Act
Data governance	PIPL + DSL	PDPA	PIPA	APPI
Cybersecurity	CSL	CSMA	Sector-based laws (e.g. Network Act)	Basic Act & Active Cyber Defence Act

Figure 2: Comparative overview of core digital regulatory frameworks in China, Taiwan, South Korea, and Japan

The EU's Influence on Digital Regulation in East Asia

Across East Asia, digital regulation exhibits a number of shared characteristics, many of which reflect the influence of the EU regulatory approach.

Privacy regimes across the region have been shaped, directly or indirectly, by the GDPR, whether through adequacy decisions, conceptual alignment, or the adoption of common principles such as transparency, data minimization, and individual rights.

Similar influence can be seen in the emergence of risk-based approaches to AI regulation in jurisdictions such as South Korea and Taiwan, as well as in developments like South Korea's Network Act, which increasingly echoes elements of EU digital governance.

Together, these trends suggest that EU regulatory concepts have already left a significant imprint on digital regulation in Asia and may continue to inform future legislative developments in the region.

Divergent Policy Priorities in East Asia's Digital Governance

At the same time, digital regulation across Asia remains diverse, shaped by differing governance traditions, policy priorities, and economic objectives rather than a single common model. The digital and AI regulatory landscape in Asian markets demonstrates how they are balancing innovation with control.

China places particular emphasis on national security and social stability, reflected in measures such as stringent controls on cross-border data transfers and content-governance and filing obligations in algorithmic regulation. This approach illustrates a preference for early intervention and centralized oversight where technologies, especially those driven by algorithms or AI, are perceived to pose systemic societal or security risks.

Japan, by contrast, places greater emphasis on supporting AI development and limiting regulatory friction, consistent with its ambition to become "the most AI-friendly country in the world". This is especially reflected in the AI Promotion Act and the recent APPI amendment proposal that pair targeted safeguards with increased flexibility for AI-related data use.

South Korea and Taiwan fall between these approaches, drawing on EU-influenced concepts such as risk-based regulation and strong privacy baselines while diverging in emphasis—Korea favoring enforceable accountability and Taiwan adopting a more gradual, principle-driven policy approach.

AI Regulatory Approaches in East Asia

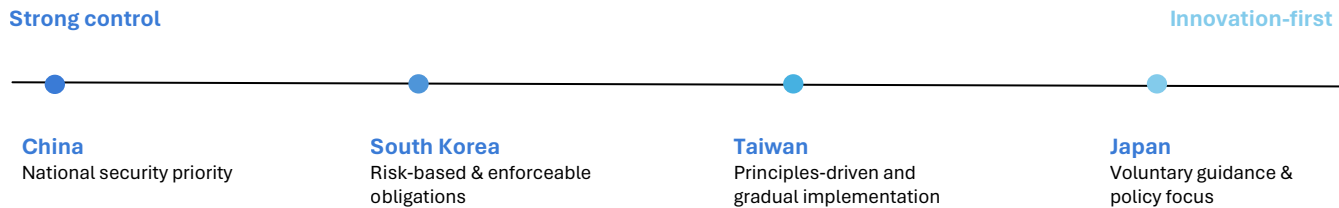


Figure 3: East Asian markets adopt differing AI regulatory philosophies, reflecting how each jurisdiction balances regulatory control and support for innovation based on its policy priorities.

Regional Trends and Takeaways for Businesses

Across East Asia, digital regulation is developing in a more diverse and context-specific way than in the EU.

While approaches differ, common themes include risk-based regulation, a focus on higher-impact uses of technology, and a preference for flexibility to keep pace with rapid innovation. Compared with the EU's prescriptive and horizontal model, East Asian markets tend to rely more on layered rules and sector-specific controls.

For businesses, this means compliance is less about ticking off uniform requirements and more about understanding regulatory intent and navigating jurisdiction- and sector-specific expectations. The regional divergence means that multinational companies must adapt to varying standards.

Companies should avoid isolated approaches to AI, data, and cybersecurity, and instead build coordinated [AI governance](#) structures that can adapt across jurisdictions. Maintaining flexible internal controls, closely tracking regulatory developments, and aligning practices with widely accepted international standards, while tailoring implementation to local requirements, can help manage diverging expectations while supporting sustainable growth in the region.

About the author



Hengying Zhang

Hengying Zhang is an experienced legal professional qualified in China and holds an LL.M. degree from the Netherlands. She studied law and digital technologies at Leiden University and brings a cross-jurisdictional perspective to digital compliance, with particular expertise in the regulatory frameworks of China and the EU.