

CYBERSECURITY IN CHINA: LEGAL RESPONSES, FIRM COMPLIANCE AND FUTURE CHALLENGES

QIAN Jiwei

EAI Background Brief No. 1798

Cybersecurity has emerged as a critical and increasingly vital policy area given China's rapidly growing digital economy, presenting significant challenges for policymakers. The country has experienced a surge in cybersecurity incidents, with over 42 million malicious software samples detected in 2020 alone. In response, China has formulated a comprehensive legal framework, including the Cybersecurity Law, Data Security Law and Personal Information Protection Law. These regulations aim to strengthen national security, protect individual privacy and ensure the integrity of critical information infrastructure. The legal framework is based on concepts such as "data sovereignty" and uses a hierarchical data classification system for data security. Despite substantial compliance efforts by firms and enforcement efforts from government agencies, several challenges persist. These include high compliance costs, varying enforcement capacities across sectors, regulatory uncertainty due to overlapping jurisdictions among government agencies and regulatory fragmentation across countries. The rapid pace of technological advancement, particularly in Artificial Intelligence, continually introduces new risks and vulnerabilities. Cybersecurity remains a priority on China's policy agenda, as evidenced by recent calls to strengthen the national cybersecurity system.

(Click on the link to read the above in [Chinese](#), [French](#) and [Spanish](#))

Date of Publication: 28 November 2024

Chinese:

中国的网络安全：法律应对、企业合规与未来挑战

鉴于中国快速增长的数字经济，网络安全已成为一个关键且日益重要的政策领域，为政策制定者带来了重大挑战。该国经历了网络安全事件的激增，仅在 2020 年就检测到超过 4200 万个恶意软件样本。作为回应，中国制定了全面的法律框架，包括《网络安全法》、《数据安全法》和《个人信息保护法》。这些法规旨在加强国家安全、保护个人隐私以及确保关键信息基础设施的完整性。法律框架基于“数据主权”等概念，并采用分级的数据分类系统来保障数据安全。尽管企业在合规方面付出了巨大努力，政府机构也在努力执法，但仍存在若干挑战。这些挑战包括高昂的合规成本、不同部门的执法能力差异、因政府机构间管辖权重叠导致的监管不确定性以及跨国监管的碎片化。同时技术的快速发展，特别是在人工智能领域，不断引入新的风险和漏洞。近来加强国家网络安全体系的政策表明，网络安全仍是中国政策议程上的优先事项。

French:

CYBERSÉCURITÉ EN CHINE: RÉPONSES LÉGALES, CONFORMITÉ DES ENTREPRISES ET FUTURS DÉFIS

La cybersécurité est devenue un domaine politique crucial et de plus en plus vital compte tenu de l'expansion rapide de l'économie numérique en Chine, avec des défis significatifs pour les décideurs politiques. Le pays a connu une augmentation des incidents de cybersécurité, avec plus de 42 millions de cas de logiciels malveillants détectés rien qu'en 2020. En réponse, la Chine a élaboré un cadre juridique complet, comprenant notamment la Loi sur la cybersécurité, la Loi sur la sécurité des données et la Loi sur la protection des informations personnelles. Ces réglementations visent à renforcer la sécurité nationale, protéger la vie privée des individus et garantir l'intégrité des infrastructures critiques d'information. Le cadre juridique est fondé sur des concepts tels que la "souveraineté des données" et utilise un système de hiérarchisation des données pour assurer leur sécurité. Malgré des efforts de conformité significatifs de la part des entreprises et d'application de la part des agences gouvernementales, plusieurs défis persistent. Ceux-ci incluent des coûts de conformité élevés, des capacités de mise en œuvre variables selon les secteurs, une incertitude due à des compétences qui se chevauchent entre les agences gouvernementales et une fragmentation réglementaire à travers les pays. Le rythme rapide des avancées technologiques, en particulier en Intelligence Artificielle, introduit continuellement de nouveaux risques et vulnérabilités. Le sujet reste une priorité sur l'agenda politique de la Chine, comme en témoignent les récents appels à renforcer le système national de cybersécurité.

Spanish:

CIBERSEGURIDAD EN CHINA: RESPUESTAS LEGALES, CUMPLIMIENTO EMPRESARIAL Y DESAFÍOS FUTUROS

La ciberseguridad ha surgido como un área política crítica y cada vez más vital dada la economía digital de rápido crecimiento de China, presentando desafíos significativos para los responsables de políticas. El país ha experimentado un aumento en los incidentes de ciberseguridad, con más de 42 millones de muestras de software malicioso detectadas solo en 2020. En respuesta, China ha formulado un marco legal integral, que incluye la Ley de Ciberseguridad, la Ley de Seguridad de Datos y la Ley de Protección de Información Personal. Estas regulaciones tienen como objetivo fortalecer la seguridad nacional, proteger la privacidad individual y garantizar la integridad de la infraestructura crítica de información. El marco legal se basa en conceptos como la “soberanía de los datos” y utiliza un sistema de clasificación jerárquica de datos para la seguridad de los mismos. A pesar de los esfuerzos sustanciales de cumplimiento por parte de las empresas y los esfuerzos de aplicación por parte de las agencias gubernamentales, persisten varios desafíos. Estos incluyen altos costos de cumplimiento, capacidades de aplicación variables entre sectores, incertidumbre regulatoria debido a la superposición de jurisdicciones entre agencias gubernamentales y fragmentación regulatoria entre países. El rápido ritmo de avance tecnológico, particularmente en Inteligencia Artificial, introduce continuamente nuevos riesgos y vulnerabilidades. La ciberseguridad sigue siendo una prioridad en la agenda política de China, como lo demuestran los recientes llamados a fortalecer el sistema nacional de ciberseguridad.

Executive Summary

1. Cybersecurity, encompassing the prevention of cybercrime, data protection and privacy safeguards, has become a critical and increasingly vital policy area given the rapid growth of China's digital economy.
2. In recent years, China has experienced a surge in cybersecurity incidents, including data breaches, cybercrimes and legal cases related to privacy.
3. In response to these challenges, the Chinese state has formulated a comprehensive legal and regulatory framework with the enactment of the Cybersecurity Law, Data Security Law and Personal Information Protection Law.
4. Central to China's policy is the concept of "data sovereignty", which has become a cornerstone in formulating regulations for domestically generated data, encompassing its collection, use, storage and cross-border transfer.
5. The 2017 Cybersecurity Law plays a critical role in combating cybercrime by ensuring that sensitive data remains under Chinese jurisdiction, thereby allowing for more effective law enforcement and cybersecurity measures.
6. The Data Security Law, enacted in 2021, introduced a hierarchical data classification system, categorising data into "general", "key" and "core" levels based on their sensitivity, potential impact on national security and severity of consequences in the event of a data breach.
7. The Personal Information Protection Law, introduced in 2021, grants individuals rights similar to those under the EU's General Data Protection Regulation, such as access, correction and deletion of personal data.
8. In recent years, government agencies have taken efforts to enforce these laws and firms in China have made substantial efforts to comply with cybersecurity regulations.

9. Cybersecurity continues to be important in China's policy agenda, with the July 2024 "Decision of the Central Committee on Further Deepening Reform and Promoting Chinese-Style Modernisation" calling for the strengthening of the national cybersecurity system.
10. Several challenges remain, including the substantial compliance costs businesses face. Enforcement capacity also varies across sectors, largely depending on the capabilities of the responsible government agencies. Regulatory fragmentation across countries is another concern.
11. Additionally, the rapid pace of technological advancement, particularly in areas like Artificial Intelligence, continually introduces new risks and vulnerabilities.