EuroHub4Sino

European Hub
for Contemporary China

September 2025

The Logic of China's AI Regulation and Its Implications for the European Union

by Łukasz Gacek

Funded by
the European Union

https://doi.org/10.31175/eh4s.a6f4

KEY TAKEAWAYS

- Ensure effective implementation and enforcement of the AI Act: The EU should prioritize consistent application and monitoring of its regulatory framework, as only credible enforcement can strengthen its position as a global normative actor in AI governance.
- Build technological sovereignty: Long-term investment in strategic technologies – particularly semiconductors, computing infrastructure, and open AI models – is essential to reduce Europe's vulnerability to external pressures and to maintain the capacity to shape standards independently.
- Advance technology diplomacy: The EU should actively promote its rights-based regulatory model, deepen cooperation with democratic partners, and strengthen its negotiating capacity within multilateral forums.
- Offer credible alternatives for the Global South: Providing infrastructure and governance solutions grounded in transparency, accountability, and human rights can counter the diffusion of authoritarian digital models while enhancing Europe's normative appeal.
- Increase engagement in international standard-setting processes: Active participation in ISO, ITU, UNESCO and similar organizations is critical to defending European principles of interoperability, transparency, and accountability against competing frameworks promoted by China.
- Develop systematic monitoring of authoritarian digital models: The EU should establish analytical tools to identify and assess the spread of China's regulatory and infrastructural frameworks, enabling proactive protection of the democratic digital order and anticipation of geopolitical risks linked to global technological fragmentation.

Keywords

Artificial Intelligence Regulation

China AI

European Union

AI Governance

Human Rights

Introduction

China's model of artificial intelligence (AI) regulation constitutes a coherent, comprehensive, and highly centralized system in which technology is subordinated to the strategic interests of the state. Within this framework, AI is treated simultaneously as an economic resource, a tool of national security, and an instrument of social control. The system rests on the integration of legal, institutional, and technological components into a unified governance mechanism for this emerging technology. Its legal architecture encompasses both overarching provisions, establishing the foundations of digital security and detailed sectoral regulations targeting technologies with significant social impact. A common feature across these instruments is strict oversight of data, algorithms, and research processes. Chinese authorities embed this control in a narrative of "digital sovereignty" and the protection of the public interest, but in reality it legitimizes extensive state intervention in information flows. This model not only structures China's domestic innovation ecosystem but also serves as a vehicle for projecting influence internationally. For the European Union, the Chinese model illustrates a state-centric approach to technological governance that may challenge Europe's rights-based standards. Grasping these dynamics is crucial for reinforcing the EU's regulatory capacity and advancing transparent, democratic frameworks for AI.

Political and Strategic Drivers of AI Development in China

China's strategy for AI development has been permanently tied to the goals of state modernization and technological autonomy. The New Generation Artificial Intelligence Development Plan (2017) *[1]* identified AI as a key pillar of the economy, national security, and defense, as

well as a tool for gaining advantage in geopolitical competition. It set out a three-stage roadmap: catching up with global leaders by 2020, achieving major technological breakthroughs by 2025, and becoming the world's leading AI power by 2030.

Beijing has constructed a top-down governance model in which political priorities determine the direction of research and deployment, while central authorities integrate the public, private, and academic sectors into joint strategic projects. This approach was exemplified in Chinese leader Xi Jinping's speech of October 2018, in which he described AI as a key driving force behind a new round of scientific and technological revolution and industrial transformation. The political framing of AI as an "important strategic lever" (重要战略抓手) served as a signal for the intensification of both regulatory and investment efforts *[2]*. This message was reiterated and reinforced in Xi's June 2024 address, which elevated AI to the rank of a transformative factor capable of reshaping the global technological and civilizational order. Xi emphasized that its impact extends beyond the economy and society to include models of civilizational development *[3]*. The importance of AI was also underscored in the 14th Five-Year Plan (2021-2025) *[4]*, which listed AI as one of the pillars of the digital economy, alongside big data, blockchain, cloud computing, and cybersecurity. The complementary 14th Five-Year Plan for Digital Economy Development *[5]* called for the integration of AI into critical sectors such as smart cities, public administration, industry, and mobility.

Taken together, these elements reflect a consistently implemented vision of state dominance over AI, in which regulatory frameworks enable broad interpretations of concepts such as national security and the public interest. This flexibility allows central authorities to shape norms while simultaneously intervening in the circulation of information.

Pillars of China's AI Legal Order

At the core of China's domestic legal framework for artificial intelligence lies the conviction that AI constitutes strategic infrastructure, something that must be designed and governed in a manner that reinforces state sovereignty, social stability, and long-term technological autonomy. This principle finds institutional expression in an expansive set of horizontal frameworks that underpin regulatory oversight of data, algorithms, and digital processes.

According to official documents, the Cybersecurity Law (2016) *[6]*, which elevated cyberspace to the status of a component of national security, framing it as a domain of sovereignty. The law harmonized compliance requirements for digital products and services with national technical standards while institutionalizing the principle of data localization and the protection of critical information infrastructure. It also signaled the need for legality and proportionality in the processing of personal data. Complementing this institutional structure, the Data Security Law (2021) *[7]* introduced a comprehensive approach to data governance based on risk classification, mandatory incident reporting, risk assessments, and compliance with the principles of legality and public interest protection. The law restricts cross-border data transfers and underpins China's active participation in shaping international standards.

A further cornerstone is the Personal Information Protection Law (2021) [8], which strengthens state control over cross-border data flows by imposing requirements for local storage and government authorization for data sharing.

Operationalizing Control: Sector-Specific Technology Regulations

The operationalization of China's data governance principles is achieved through a range of implementing instruments. Beijing frames these measures as advancing ethics and transparency in data governance, emphasizing user protection, minimization of data use, and shared responsibility across government, enterprises, organizations, and citizens. For instance, The White Paper on the Protection of Personal Information in Mobile Internet Applications (Apps) (2021) [9] emphasizes transparency in data collection, minimization of data use, and technological oversight of apps, while assigning shared responsibilities to government, enterprises, organizations, and citizens. These principles are further developed in the Cybersecurity Standard Practice Guide – Guidelines for Self-Assessment of the Collection and Use of Personal Information by Mobile Internet Applications (Apps) (2020) [10], which require informed user consent, prohibit manipulative consent practices, and mandate that users be given the ability to delete or modify their data.

However, this rhetoric contrasts with the practical function of these instruments, which is to expand state capacity to monitor digital activity, enforce compliance obligations, and strengthen political oversight. By institutionalizing mechanisms of consent and transparency, the state positions itself as the ultimate guarantor of digital rights, while simultaneously consolidating control over the circulation of information. This logic is further entrenched in the Regulations on the Administration of Network Data Security (2024) [11], which introduce supervisory mechanisms applicable to both domestic and foreign entities. Officially, these measures are justified as strengthening data security and ensuring accountability of online platforms. In practice, however, they impose new obligations that bind private-sector actors more closely to the state's regulatory apparatus, requiring them to monitor user activity, remove non-compliant applications, and issue social responsibility reports.

Similarly, one of the most restrictive regulations in the biometric sphere – the Measures for the Security Administration of the Application of Facial Recognition Technology (2025) [12] – is framed as a privacy safeguard by mandating local processing of biometric data and explicit user consent. Yet, while presented as privacy protections, these measures ultimately operate as a powerful instrument of surveillance and centralized control over biometric information.

Together, these legislative measures form a coherent system that integrates sectoral and general regulations with enforcement mechanisms, thereby reinforcing China's institutional and technological architecture of oversight. The horizontal framework is further operationalized through vertical sectoral rules that translate general principles into specific applications. In the area of algorithmic recommendation systems, lawmakers not only prohibit the

manipulation of public opinion but also establish a registration infrastructure for systems with "significant social impact" and introduce multiple supervisory instruments. Due to the somewhat vague legal categories, however, these measures leave wide scope for discretionary interpretation by regulatory authorities.

Algorithmic Regulation and Generative Systems

Within China's integrated framework for steering the digital future, sector-specific regulations operationalize the horizontal legal architecture in the context of concrete technological applications and risks. Their adoption represents a shift of regulatory emphasis to the application level, following a logic of prevention, accountability, and social mobilization. These instruments function as mechanisms of oversight for specific segments of the AI ecosystem.

A landmark development was the Interim Measures for the Administration of Generative Artificial Intelligence Services (2023) *[13]*. According to the Chinese government's official narrative, the measures are designed to balance the promotion of innovation with the safeguarding of security, ensuring transparency in content and data sources. In practice, however, they institutionalize a system of strict state supervision, granting authorities wide-ranging powers to inspect training data and audit algorithms. Crucially, the measures also apply extraterritorially to providers offering services within China, thereby extending Beijing's regulatory reach beyond its borders.

Their implementation was reinforced by the Basic Security Requirements for Generative Artificial Intelligence Services (2024) *[14]*, which mandate regular self-assessments, content labeling, and risk management from the design stage of AI models. Although formally a technical standard, in practice this document functions as a quasi-regulatory and enforcement tool, enabling monitoring and early-warning mechanisms against systemic risks. A similarly detailed regulatory architecture has emerged around deepfakes. The Provisions on the Administration of Deep Synthesis of Internet Information Services (2022) *[15]* impose supervisory duties on providers of synthetic content, requiring content identification, user verification, and active measures against disinformation. These provisions also integrate AI into China's state-led ideological infrastructure.

Further measures include the Provisions on the Administration of Algorithmic Recommendation for Internet Information Services (2021) *[16]* and the Guiding Opinions on Strengthening the Comprehensive Governance of Algorithms for Internet Information Services (2021) *[17]*. Together, they establish standards of supervision and accountability, coupled with requirements for algorithm registration and disclosure. These measures, and related supervisory practices, such as the obligation imposed on companies like Alibaba, Tencent, and ByteDance to disclose core algorithms—demonstrate the growing integration of private-sector actors into the state's regulatory apparatus. Despite occasional tensions, this cooperation has evolved into a mechanism of institutional learning that strengthens the state's regulatory capacity and adaptability.

Ethics and Trustworthiness as the Foundation of China's AI Model

Official Chinese documents characterize ethics and trustworthiness as the foundation of China's AI model. While Beijing presents these measures as advancing responsible and transparent governance, in practice they function as instruments of oversight and political control. Within China's integrated AI governance system, ethics, transparency, and trustworthiness permeate all levels of technology regulation. From data security and algorithmic architecture to sector-specific applications, ethical components are embedded in nearly every regulation and reinforced by dedicated normative instruments. Collectively, they underpin China's evolving concept of "trustworthy AI" (可信人工智能), a notion that legitimizes the extension of state authority rather than protecting individual rights.

The first systematic attempt to articulate this approach was the Cybersecurity Standard Practice Guide – Guidelines for Ethical Norms of Artificial Intelligence (2020) *[18]*, which identified five core categories of risk: loss of control, societal threats, violations of individual rights, discrimination, and lack of accountability. The document also called for the creation of an ethical ecosystem encompassing developers, operators, and users of AI systems. This was followed by the Ethical Norms for the New Generation of Artificial Intelligence (2021) *[19]*, which expanded on the idea of "human-centered AI" (以人为本). These norms emphasized the protection of individual rights, transparency of system operations, the prohibition of discrimination, and the obligation to inform users about the use of algorithms.

At the level of technical standardization, the White Paper on the Standardization of Artificial Intelligence Security (2018, updated in 2021 and 2023) *[20]* has remained a key reference, defining five essential qualities of AI: reliability (可靠性), transparency (透明性), explainability (可解释性), fairness (公平性), and privacy protection (隐私性). Complementing this, the Guidelines for Building a National New Generation Artificial Intelligence Standard System (2020) *[21]* present standardization as a coordination tool for the entire sector—from basic research to industrial deployment.

The culmination of these efforts came with the White Paper on Trustworthy Artificial Intelligence (2021) *[22]*, which argued that AI systems must be transparent, predictable, resilient to errors, and understandable to both users and operators. Among its priority values were responsibility, fairness, data protection, and the prevention of discrimination. Although Chinese authorities emphasize ethics and trust in framing these measures, their practical effect is to reinforce regulatory control and consolidate political authority. Yet as China's online population surpassed one billion (close to 80% of the population) and generative AI tools spread rapidly, societal concerns have grown regarding the processing of personally identifiable data and information gathered from intelligent devices capable of analyzing user behavior and emotions. In this context, the regulator's process of institutional learning plays an increasingly important role. Obligations such as algorithm registration, regular consultations with major technology firms (e.g., Alibaba, Tencent, and ByteDance), and the development of supervisory tools have strengthened administrative capacities, clarified intervention

points, and standardized procedures such as algorithm security self-assessment reports. While officially presented as mechanisms that strengthen ethics and transparency, many of these regulations remain broad in scope and lack detailed implementation mechanisms. Their primary function is to reinforce state legitimacy in AI governance and to support a broader strategy of systemic oversight. Their domestic orientation and limited references to international standards (e.g., ISO, IEC), however, risk undermining interoperability and contributing to further fragmentation of the global regulatory ecosystem.

Ultimately, China's integrated system of AI regulation is built on the consistent subordination of technology to state objectives, combined with the development of detailed instruments of control and legitimization. This model not only organizes the domestic innovation ecosystem but also serves as a tool of international expansion through the export of norms, standards, and technological values to other countries. For the European Union, understanding this system is of critical importance, both in terms of the threats it poses to the democratic digital order and for its implications in shaping global regulatory frameworks.

Digital Authoritarianism and the Export of China's AI Model

While China's regulatory system is primarily designed to consolidate state control over the domestic AI ecosystem, its logic does not stop at the national level. The same principles of sovereignty, security, and state-led governance that structure internal regulation are increasingly projected outward. What emerges is a dual strategy. AI as a tool of modernization and legitimacy at home, and as an instrument of influence and norm diffusion abroad. This external dimension has been described as a form of "digital authoritarianism," through which China exports not only infrastructure and technology but also the regulatory logic and values that underpin its domestic system.

A key vehicle for this expansion is the Digital Silk Road (DSR), formally incorporated into the Belt and Road Initiative. It involves large-scale investments in cross-border fibre-optic cables, undersea networks, data centres, and satellite channels, designed to build an "Information Silk Road" with China at its centre. By offering low-cost access to infrastructure, Beijing positions itself as a primary partner for developing countries with limited alternatives *[23]*.

Artificial intelligence plays a pivotal role in this strategy. Chinese enterprises such as Huawei, ZTE, Hikvision, Dahua, CloudWalk, and Yitu export surveillance systems, biometric identification tools, and smart city platforms. These technologies are frequently installed under DSR projects and are often deployed in authoritarian regimes, where they can be used for political control and social monitoring. Open-source and inexpensive AI models, such as DeepSeek, further reinforce China's capacity to spread its standards, enabling adoption even in states with limited technological resources. This expansion is not only economic but also normative. By delivering integrated infrastructure and governance solutions, China promotes weaker standards of data protection and embeds its state-centric model of oversight abroad.

Confirmed incidents, such as the transfer of African Union data to Shanghai, illustrate the security and sovereignty risks that accompany such projects. The result is structural dependence on Chinese providers, erosion of transparency, and diminished regulatory autonomy in many Global South Countries [24] [25].

While China promotes the Digital Silk Road as a pathway to connectivity and shared prosperity, in practice it operates as both a technological and geopolitical instrument. It enables the export of AI-driven surveillance and projects China's state-centric governance model abroad. Through this dual track, Beijing strengthens its position as a leading technology partner for developing states while extending its normative influence well beyond its borders.

Externalising China's Regulatory Preferences

China seeks to build its own ethically and culturally embedded path of AI development, explicitly distancing itself from Western universalist frameworks. In Beijing's narrative, AI governance should not constrain innovation but instead guarantee technological progress pursued for the common good of humanity. Artificial intelligence is presented as a central arena of technological and ideological competition with the West, where normative claims play a decisive role. In Beijing's narrative, AI is portrayed as a tool for redistributing opportunities, reducing inequalities and building a more just international order. Yet this discourse ultimately serves to strengthen China's position as the advocate of the Global South and to promote its state-centric governance model internationally. It highlights values such as community, data sovereignty, and cultural as well as linguistic adaptation of AI models, contrasting these with the universal standards promoted by Western actors. This rhetoric centers on the notion of "true multilateralism" (真正多边主义) and the vision of "building a community with a shared future for mankind" (共同构建人类命运共同体), with the United Nations positioned as the primary coordinating platform.

A central expression of this ambition was showcased at the World Artificial Intelligence Conference (WAIC) in Shanghai in July 2024, during which participants adopted the Shanghai Declaration on Global AI Governance [26]. The declaration called for the "healthy development of AI, ensuring AI safety and building a common future for mankind," echoing China's preferred narrative of AI as a global public good. However, the declaration remained vague, lacking operational detail, and served mainly to legitimize China's leadership role in shaping global norms.

At the WAIC in July 2025, held alongside a high-level governance meeting, Premier Li Qiang presented AI as a new driver of economic growth and daily life. He framed China's agenda around three themes: inclusiveness, innovation, and global governance. The vision stressed open access and technology sharing with the Global South, joint research and talent exchange, and the creation of international regulatory frameworks. A key proposal was the establishment of a Global AI Cooperation Organization (世界人工智能合作组织) as a permanent platform to coordinate regulation and development at the international level [27]. Taken

together, these initiatives underscored Beijing's ambition to institutionalize its leadership and to position its model as an alternative to Western-led forums such as the G7 or OECD.

At the international level, China positions the UN as the cornerstone of its strategy for shaping global digital governance. China's multilateral strategy centers on the UN, which it portrays as the legitimate forum for inclusive digital governance. In July 2024, the UN General Assembly adopted a resolution on Enhancing International Cooperation on Capacity-Building of Artificial Intelligence [28], co-sponsored by China and backed by 143 states. It stressed the need to empower developing countries in global governance and to equip them with resources for effective participation. By working through the UN, Beijing seeks to reinforce its legitimacy and project itself as the advocate of the Global South. On the surface, this strategy highlights inclusivity, but in practice it embeds China's state-centric governance model into global debates.

Strategically, these initiatives demonstrate China's effort to externalize its state-centric governance model by embedding it within multilateral frameworks. While framed in terms of inclusivity, equality, and cooperation, they serve clear strategic objectives: counterbalancing Western influence in standard-setting, legitimizing digital sovereignty, and securing international recognition for China's approach. This trajectory poses a direct challenge for Europe and other democratic actors, who must respond by advancing credible alternatives that align rights-based values with effective governance structures.

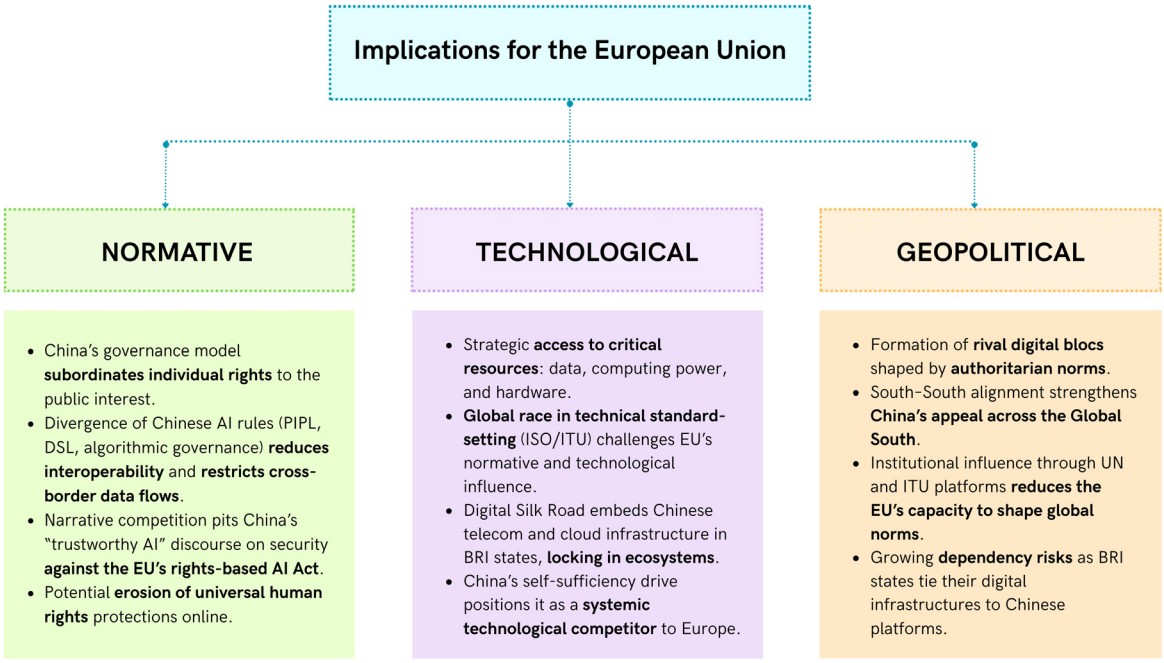
Implications for the European Union

The diffusion of China's AI regulatory model carries significant normative, technological, and geopolitical consequences for the European Union. On the normative level, China's approach challenges the universality of principles such as privacy protection, freedom of expression, and transparency of digital systems. Beijing promotes an alternative paradigm in which individual rights are subordinated to the public interest. This risks eroding the fragile international consensus on the protection of fundamental human rights in the digital domain. In practice, the export of this model in the form of regulations or technical standards may lead other states to adopt frameworks that curb civil liberties in the name of efficiency and security.

In the technological sphere, the contest extends beyond leadership in language models or generative systems to include access to critical resources such as data, computing power, and hardware components. Particularly important is China's drive for self-sufficiency in key inputs (notably semiconductors) and the development of its own infrastructural standards (e.g., 5G networks, smart city systems), which increasingly compete with European solutions on the global stage. On the geopolitical front, the expansion of Chinese regulatory and infrastructural models across the Global South risks creating rival digital blocs dominated by authoritarian norms and values. China's ability to combine technological offerings with political and financial incentives enhances its appeal to authoritarian governments and states

with weaker democratic institutions. This strategy undermines the EU's capacity to forge broad international coalitions around an open internet, interoperable standards, and transparent AI governance.

China's activism in international organizations (e.g., ITU, ISO, UNESCO) further enables it to shape global technical and ethical frameworks, often in ways that conflict with Europe's principles of transparency and accountability. The European Union must respond to these challenges through layered political, legal, and technological action. First, it is essential to consolidate its own regulatory framework by swiftly and effectively implementing the AI Act, coupled with robust enforcement mechanisms. At the same time, the EU must invest heavily in strategic technologies, including semiconductors, computing infrastructure, open AI models, and high-reliability systems, in order to reduce external dependencies and enhance technological sovereignty. Equally important is technology diplomacy: deepening cooperation with democratic partners, promoting the European regulatory approach, and offering developing countries credible alternatives in both infrastructure and governance. These alternatives should be grounded in transparency, accountability, and the protection of human rights.



[1] New Generation Artificial Intelligence Development Plan (新一代人工智能发展规划), State Council PRC (国务院), July 8, 2017, https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm

[2] Xi Jinping (习近平), Promoting the Healthy Development of China's New Generation of Artificial Intelligence (推动我国新一代人工智能健康发展), Xinhua (新华), October 31, 2018, http://www.xinhuanet.com/politics/2018-10/31/c_1123643321.htm

[3] Xi Jinping Sends Congratulatory Letter to the 2024 World Intelligence Expo (习近平向2024世界智能产业博览会致贺信), Xinhua (新华), State Council PRC (国务院), June 20, 2024, https://www.gov.cn/yaowen/liebiao/202406/content_6958352.htm

[4] Outline of the 14th Five-Year Plan for National Economic and Social Development and the Long-Range Objectives Through the Year 2035 of the People's Republic of China (中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要), Ministry of Commerce PRC (商务部), March 2021, https://zhs.mofcom.gov.cn/cms_files/oldfile//zhs/202107/20210715110152880.pdf

[5] The 14th Five-Year Plan for Digital Economy Development ("十四五"数字经济发展规划), State Council PRC (国务院), December 12, 2021, https://www.gov.cn/zhengce/zhengceku/2022-01/12/content_5667817.htm?ivk_sa=1023197a

[6] Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法), State Council PRC (国务院), November 7, 2016, https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

[7] Data Security Law of the People's Republic of China (中华人民共和国数据安全法), Xinhua (新华), State Council PRC (国务院), June 11, 2021, https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm

[8] Personal Information Protection Law of the People's Republic of China (中华人民共和国个人信息保护法), Xinhua (新华), State Council PRC (国务院), August 20, 2021, https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm

[9] White Paper on the Protection of Personal Information in Mobile Internet Applications (Apps) (移动互联网应用程序（APP）个人信息保护治理白皮书), China Academy of Information and Communications Technology (中国信息通信研究院), November 2021, http://www.caict.ac.cn/kxyj/qwfb/bps/202111/P020211119513519660276.pdf

[10] Cybersecurity Standard Practice Guide – Guidelines for Self-Assessment of the Collection and Use of Personal Information by Mobile Internet Applications (Apps) (网络安全标准实践指南 — 移动互联网应用程序（App）收集使用个人信息自评估指南), Secretariat of the National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会秘书处), July 2020, https://www.cebnet.com.cn/upload/resources/file/2020/07/27/119628.pdf

[11] Regulations on the Administration of Network Data Security (网络数据安全管理条例), State Council PRC (国务院), September 24, 2024, https://www.gov.cn/zhengce/content/202409/content_6977766.htm

[12] Measures for the Security Administration of the Application of Facial Recognition Technology (人脸识别技术应用安全管理办法), Cyberspace Administration of China (国家互联网信息办公室), Ministry of Public Security PRC (中华人民共和国公安部), March 13, 2025, https://www.cac.gov.cn/2025-03/21/c_1744174262156096.htm

[13] Interim Measures for the Administration of Generative Artificial Intelligence Services (生成式人工智能服务管理暂行办法), State Council PRC (国务院), July 10, 2023, https://www.gov.cn/zhengce/zhengceku/202307/content_6891752.htm

[14] Basic Security Requirements for Generative Artificial Intelligence Services (生成式人工智能服务安全基本要求), National Cybersecurity Standardization Technical Committee (全国网络安全标准化技术委员会), February 29, 2024, https://www.tc260.org.cn/upload/2024-03-01/1709282398070082466.pdf

[15] Provisions on the Administration of Deep Synthesis of Internet Information Services (互联网信息服务深度合成管理规定), State Council PRC (国务院), November 25, 2022, https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm

[16] Provisions on the Administration of Algorithmic Recommendation for Internet Information Services (互联网信息服务算法推荐管理规定), State Council PRC (国务院), December 31, 2021, https://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666429.htm

[17] Guiding Opinions on Strengthening the Comprehensive Governance of Algorithms for Internet Information Service (关于加强互联网信息服务算法综合治理的指导意见), Cyberspace Administration of China (国家互联网信息办公室), September 29, 2021, https://www.cac.gov.cn/2021-09/29/c_1634507915623047.htm

[18] Cybersecurity Standard Practice Guide – Guidelines for Ethical Norms of Artificial Intelligence (网络安全标准实践指南—人工智能伦理道德规范指引), National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会), November 2020, https://www.tc260.org.cn/upload/2020-11-09/1604910605970089327.pdf

[19] thical Norms for the New Generation of Artificial Intelligence (新一代人工智能伦理规范), Ministry of Science and Technology PRC (科技部), September 26, 2021, https://www.most.gov.cn/kjbgz/202109/t20210926_177063.html

[20] White Paper on the Standardization of Artificial Intelligence Security (人工智能安全标准化白皮书), National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会), Special Working Group on Big Data Security Standards (大数据安全标准特别工作组), May 2023, https://www.tc260.org.cn/upload/2023-05-31/1685501487351066337.pdf

[21] Guidelines for Building a National New Generation Artificial Intelligence Standard System (国家新一代人工智能标准体系建设指南), State Council PRC (国务院), July 27, 2020, https://www.gov.cn/zhengce/zhengceku/2020-08/09/5533454/files/bf4f158874434ad096636ba297e3fab3.pdf

[22] White Paper on Trustworthy Artificial Intelligence (可信人工智能白皮书), China Academy of Information and Communications Technology (中国信息通信研究院), JD Explore Academy (京东探索研究院), July 2021, http://www.caict.ac.cn/kxyj/qwfb/bps/202107/P020210709319866413974.pdf

[23] Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road, National Development and Reform Commission, Ministry of Foreign Affairs, Ministry of Commerce PRC, March 2015, https://policy.asiapacificenergy.org/sites/default/files/Vision%20and%20Actions%20on%20Jointly%20Building%20Silk%20Road%20Economic%20Belt%20and%2021st-Century%20Maritime%20Silk%20Road%20%28EN%29.pdf

[24] Sameer Patil, Prithvi Gupta, The Digital Silk Road in the Indo-Pacific: Mapping China's Vision for Global Tech Expansion, „Issue Brief" 683, Observer Research Foundation, January 2024, https://www.orfonline.org/public/uploads/posts/pdf/20240103105252.pdf

[25] China's Digital Silk Road: Outlines and Implications for Europe, RKK/ ICDS, February 2024, https://icds.ee/wp-content/uploads/dlm_uploads/2024/02/ICDS_Brief_China%C2%B4s_Digital_Silk_Road_Maria_February_2024.pdf

[26] Shanghai Declaration on Global AI Governance (人工智能全球治理上海宣言), State Council PRC (国务院), July 4, 2024, https://www.gov.cn/yaowen/liebiao/202407/content_6961358.htm

[27] Li Qiang Attends the Opening Ceremony of the 2025 World Artificial Intelligence Conference and High-Level Meeting on Global AI Governance and Delivers a Speech (李强出席2025世界人工智能大会暨人工智能全球治理高级别会议开幕式并致辞), Xinhua (新华), State Council PRC (国务院), July 26, 2025, https://www.gov.cn/yaowen/liebiao/202507/content_7033942.htm

[28] Enhancing International Cooperation on Capacity-Building of Artificial Intelligence, Resolution adopted by the General Assembly on 1 July 2024, United Nations, https://documents.un.org/doc/undoc/gen/n24/197/26/pdf/n2419726.pdf

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which these article have been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent. Deed - Attribution 4.0 International - Creative Commons

This EuroHub4Sino Policy Paper contains links to external third-party websites. These links to third-party sites do not imply approval of their contents. EuroHub4Sino has no influence on the current or future contents of these sites. We therefore accept no liability for the accessibility or contents of such websites and no liability for damages that may arise as a result of the use of such content.

Funded by
the European Union

The project "European Hub for Contemporary China (EuroHub4Sino)" has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement number 101131737.

Funded by the European Union. Views and opinions expressed are however those of the authors) only and do not necessarily reflect those of the European Union or European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.