Corporate Governance, Technology, and the Law -Perspectives from China and India

Law Working Paper N° 855/2025
July 2025

Akshaya Kamalnath
Australian National University

Lin Lin
National University of Singapore and ECGI

ECGI Working Paper Series in Law

Corporate Governance, Technology, and the Law -Perspectives from China and India

Working Paper N° 855/2025

July 2025

Akshaya Kamalnath
Lin Lin

We are grateful to participants of the Asian Corporate Law Forum for insightful discussion and comments on a previous draft of this paper. We are particularly thankful to Dan W. Puchniak for his feedback on a previous draft of this paper. Any errors are our own.

Abstract

As technology becomes integral to corporate functioning, governance must address two key dimensions: leveraging technology within governance structures and managing the risks it introduces. This paper examines how companies in China and India navigate these dimensions, with a focus on AI and data protection-two of the most pressing concerns today. Using empirical data, the study evaluates board-level disclosures of tech expertise and risk management practices, alongside an analysis of regulatory frameworks and high-profile techrelated incidents such as cybersecurity breaches. By bringing the corporate governance-tech interface from China and India to a broader audience, the paper highlights contrasting regulatory approaches. Unlike the EU's cautious stance, both countries adopt pro-innovation strategies that prioritize digital growth and competitiveness. Yet, key differences emerge: China leads in AI development with active regulatory guidance and policy incentives, while India maintains a more reserved, 'wait-andsee' approach. These variations reflect deeper institutional contexts and raise critical questions about balancing innovation with accountability in corporate governance.

Keywords: Corporate Governance, AI, Data Protection, China, India

Akshaya Kamalnath*
Associate Professor
Australian National University
5 Fellows Road
ACTON ACT 2600, Australia
e-mail: Akshaya.kamalnath@anu.edu.au

Lin Lin
Associate Professor
National University of Singapore, Faculty of Law
469G Bukit Timah Road
Singapore, 259776, Singapore
e-mail: lawll@nus.edu.sg

*Corresponding Author

Corporate Governance, Technology, And The Law - Perspectives from China and India

Akshaya Kamalnath* and Lin Lin†

Abstract

As technology becomes integral to corporate functioning, governance must address two key dimensions: leveraging technology within governance structures and managing the risks it introduces. This paper examines how companies in China and India navigate these dimensions, with a focus on AI and data protection—two of the most pressing concerns today. Using empirical data, the study evaluates board-level disclosures of tech expertise and risk management practices, alongside an analysis of regulatory frameworks and high-profile tech-related incidents such as cybersecurity breaches.

By bringing the corporate governance-tech interface from China and India to a broader audience, the paper highlights contrasting regulatory approaches. Unlike the EU's cautious stance, both countries adopt pro-innovation strategies that prioritize digital growth and competitiveness. Yet, key differences emerge: China leads in AI development with active regulatory guidance and policy incentives, while India maintains a more reserved, 'wait-and-see' approach. These variations reflect deeper institutional contexts and raise critical questions about balancing innovation with accountability in corporate governance.

Key words: **Corporate Governance, AI, Data Protection, China, India,**

* Associate Professor, Australian National University, Law School. I would like to thank Krishna Natesan for his research assistance. I am thankful to Centre for Asian Legal Studies at NUS for hosting me in 2024 which gave rise to this joint project. We are grateful to participants of the Asian Corporate Law Forum for insightful discussion and comments on a previous draft of this paper. We are particularly thankful to Dan W. Puchniak for his feedback on a previous draft of this paper. Any errors are our own.
† Associate Professor, National University of Singapore, Faculty of Law. I would like to thank Che Shirui and Wang Qingruo for their research assistance.

Contents

Introduction

The world is currently in an 'AI race' with the current geopolitical tensions only serving to heat up this race.[1] While the U.S. tech companies were seen to be at the forefront of this race and the EU is seen to be regulating heavily and perhaps even exporting its regulations (famously termed Brussels effect[2]), recent advances in China have woken up the world about China being a formidable competitor.[3] At the same time, other countries like India are looking to encourage AI development, and use; and American big tech and other investors are keen to increase investments into India's AI industry.[4] India playing the role of co-chair at the Paris summit of

[1] Mark Craddock, 'The AI Superpower Showdown - Inside the US-China Race for Technological Supremacy' (Medium, 29 January 2025) https://medium.com/@mcraddock/inside-the-us-china-race-for-technological-supremacy-52cb5c3df063.
[2] Anu Bradford, The Brussels Effect, 107 NW. U. L. REV. 1 (2012).
[3] John Thornhill, 'With DeepSeek, China innovates and the US imitates' (Financial Times, 30 January 2025) https://www.ft.com/content/d72e0750-6a8b-4ef4-b9e1-6d35fd2a69b8.
[4] Anisha Sircar, 'India's DeepSeek Moment: Where The Country Stands In The Global AI Race' (Forbes) https://www.forbes.com/sites/anishasircar/2025/02/20/indias-deepseek-moment-where-the-country-stands-in-the-global-ai-race/ [20 February 2025) "So far a more quiet contender in the broader AI conversation, India's tech ecosystem has seen an

the Global Partnership on AI and being positioned to host the 2026 AI summit also signals both India's ambitions and the world's acceptance of its importance in the development of AI.[5] As these countries – China and India - emerge as major players in AI development and use, it is important to understand, from a corporate governance perspective, what the legal environment in these two countries is, in terms of technology creation and deployment.[6] Our focus is on corporate governance issues vis-à-vis AI and data security because although companies are dealing with a host of tech related issues that are relevant for corporate governance, these are the two most significant areas. Corporate governance today must consider technology across two verticals – first, the use of technology within corporate governance, and second, factoring in the risks of using technology in corporate activity. This paper considers both these verticals in this paper. For short, we will refer to these governance challenges faced by companies and any measures taken to deal with them, as 'digital governance'.[7]

We seek to answer three key questions in this paper : 1. What regulatory approaches are China and India adopting to manage AI and data protection within the corporate governance framework? 2. How are companies in China and India incorporating technological expertise into their corporate governance structures, and to what extent is this information being disclosed publicly? 3**.** To what extent do institutional and developmental differences between China and India shape their respective responses to technology-related risks and innovation within corporate governance?

Methodologically, the paper will mostly aim to provides a descriptive account of digital governance (which considers hard law, soft law and corporate practice) across the two countries and then draw some comparative conclusions where possible. While this descriptive contribution is itself significant because it will bring the corporate governance and technology story from two Asian giants – China and India – to a wider audience, the paper also has a normative focus. Drawing on relevant corporate law scholarship, the paper's normative

ostensibly slower, more measured start in carving out a prominent niche — but its burgeoning startup scene is increasingly drawing global attention from venture capitalists and investors alike."]; 'India pulls in tech giants for its AI ambitions' (Financial Times, 17 June 2024) https://www.ft.com/content/414e912f-c50c-4bc8-b3a2-b9ac36c34ebb.

[5] Megha Shrivastava, 'Paris AI Action Summit – A Missed Opportunity' (ORF America, 2025) http://orfamerica.org/orf-america-comments/paris-ai-summit-missed-opportunity. ["India's co-chairing of the Paris Summit and announcement of its role as the host for 2026 signifies the involvement of global actors, preventing mainstream AI discussions from becoming a part and parcel of the U.S.-China tech fight."]

[6] Other countries like the UK, UAE, South Korea, Singapore, and Japan are also significant current and emerging players in the AI space and we hope that other scholars take up our call for similar research from these jurisdictions.

[7] One of us (Kamalnath) has used this label to refer to corporate governance vis-à-vis all technology related issues in other work. Akshaya Kamalnath, *Corporations, Technology, and the Law: Future of the Firm* (OUP, forthcoming 2025/26).

component will stress the need for strong 'digital governance' regimes although what this looks like will be context specific and take into consideration both law on the books and law in action.

We employ a range of methods within the descriptive section of the paper because to paint the full picture, we must not only look at the law and policy available, but also how digital governance is being done in the two countries. To set out the relevant laws and how they work, we use traditional doctrinal analysis. In order to understand the practice of digital governance we conduct some exploratory empirical studies. In the China section, we are able to search for corporate disclosures on tech related risks in a wide range of documents because of the availability of relevant databases. In the India section, data had to be hand-collected and we therefore use very small data sets. These studies are therefore exploratory (rather than empirical) in nature.

The remainder of this paper is organised as follows. Part 1 discusses the law, practice, and future challenges around digital governance in China and Part 2 similarly discusses the same for India. Part 3 concludes with some analytical discussion about what insights can be drawn from the digital governance journeys of China and India.

1. China

A growing number of Chinese enterprises, including both state-owned and private companies, are increasingly leveraging artificial intelligence ("***AI***") to restructure production processes and enhance operational efficiency. For example, PetroChina has applied AI to optimize drilling parameters, reducing the cost per well by 15%; China Grain Reserves Corporation (Sinograin) has utilised IoT + AI to lower grain loss rates to below 0.3%; and China State Construction Engineering Corporation has implemented computer vision to monitor construction site safety, reducing accident rates by 60%.[8] Similarly, CRRC's autonomous train operation system has increased metro transportation capacity by 30%.[9]

Central state-owned enterprises ("***SOEs***") are also using AI to advance ecological collaboration and integrate ESG practices into their operations. For instance, Sinopec has used AI algorithms to harness excess heat from refineries for heating, establishing a new paradigm for green and low-carbon development.[10] Moreover, industries such as manufacturing and finance are

[8] Zhu Jiujun, "The Combination Of Central Enterprises And Artificial Intelligence (AI): Catalyzing Profound Industrial Change" , 23 Feb 2025, https://mp.weixin.qq.com/s/bNeO0dnPNcI4U5NJz6JXIg
[9] Supra note **Error! Bookmark not defined.**.
[10] Supra note 8.

accelerating AI adoption. The penetration rate of AI in the Technology, Media, and Telecommunications sector has exceeded 30%, with companies listed on the (the Shanghai Stock Exchange Science and Technology Innovation Board (the STAR Market) particularly standing out. AI applications in quality inspection and intelligent customer service have significantly improved operational efficiency.[11]

Beyond process optimisation, AI is also demonstrating multi-dimensional advantages in corporate risk governance in China. It enhances review efficiency through automation tools (e.g., ESG investment analysis), enables real-time risk monitoring (e.g., contract management), updates risk control strategies based on real-time data (e.g., anti-money laundering in finance), and provides accurate early warnings for potential risks (e.g., financial audits).[12] AI has gradually made its way into corporate boardrooms in China. As early as 2014, the Hong Kong-based venture capital firm Deep Knowledge introduced a machine-learning algorithm called "VITAL" to assist in decision-making. However, while it could vote on investment matters, it did not hold the legal status of a board director.[13] Since then, more companies have integrated AI into board decision-making. For example, in 2022, NetDragon Websoft announced the appointment of a digital human as a rotating CEO, responsible for organisational management and strategic execution.[14]

1.1 Hard and soft law on digital governance

The relationship between AI and data protection is both intricate and deeply interdependent, primarily involving multiple aspects such as data collection, storage, processing, and usage. In China, the regulatory approach to both AI and data protection reflects a dual objective: promoting the application of artificial intelligence while strengthening data protection, thereby achieving the dual goals of technological innovation and risk prevention. The relevant legal framework includes both hard law (laws, administrative regulations, departmental rules) and soft law (policy guidance, industry standards, etc.).

(a) AI Regulation

[11] Chen Jingshan, Normative Approaches to AI-Enabled Corporate Risk Governance, 12 October 2024, https://mp.weixin.qq.com/s/02DZC8RGtioRr_zzc8B5fg.
[12] Wu Jianzu, Corporate Risks and Board Governance in the AI Era, 30 July 2024, https://mp.weixin.qq.com/s/CeO7hCDdaTTAyZANJaoeLw.
[13] 'Hong Kong VC's Robotic Breakthrough: AI Program Joins Investment Committee, 8 August 2014, https://www.chuandong.com/news/news142834.html.
[14] Appointing a Digital Human as CEO? This Listed Gaming Company's Move Goes Viral, 5 September 2022, https://www.thepaper.cn/newsDetail_forward_19758651.

China's legal and policy framework governing AI primarily addresses three interrelated dimensions: (i) the promotion of AI application, (ii) the protection of personal information, and (iii) a multi-agency collaborative regulatory model.

(i) Promoting the Application of AI

Since the release of the *New Generation Artificial Intelligence Development Plan*[15] in 2017, China has introduced numerous policies to drive AI adoption in enterprises and refine AI governance frameworks. In February 2025, the State-owned Assets Supervision and Administration Commission launched the "AI+" initiative, requiring central SOEs to invest in computing infrastructure and open-source large models. Companies such as China Telecom and China Southern Power Grid have already released proprietary large models, integrating technologies from Huawei and Baidu.[16]

At the subnational level, several local governments have also introduced regulations to encourage AI adoption in enterprises, emphasizing its role in core business functions such as design, production, management, logistics, and marketing, thereby accelerating intelligent transformation. Notably, relevant laws and regulations promote the application of AI in corporate governance to enhance decision-making efficiency and risk management. For instance, the *Shanghai Regulations on Promoting the Development of the Artificial Intelligence Industry*[17] and the *Shenzhen Special Economic Zone Artificial Intelligence Industry Promotion Regulations*[18] encourage enterprises to integrate AI in commerce, manufacturing, finance, and other sectors to facilitate intelligent upgrades.[19]

The regulations also place strong emphasis on ethics and safety standards. For example, Article 69 of the *Shenzhen Special Economic Zone Artificial Intelligence Industry Promotion Regulations*[20] mandates AI enterprises to incorporate ethical safety standards into professional conduct requirements, strengthen employee training, and leverage technological innovation to

[15] Notice of the State Council on Issuing the New Generation Artificial Intelligence Development Plan (国务院关于印发新一代人工智能发展规划的通知) (State Council, 8 July 2017).
[16] Meng Yuan, 'How Should State-Owned Enterprises Embrace the New Era of AI?, *State Assets Report* 7 (27 September 2024), https://mp.weixin.qq.com/s/Rn9xbv-wIX94ROVwatYXrg.
[17] Shanghai Regulations on Promoting the Development of the Artificial Intelligence Industry (上海市促进人工智能产业发展条例) (Shanghai Municipal People's Congress, 22 September 2022; Effective 1 October 2022).
[18] Regulations of the Shenzhen Special Economic Zone on Promoting the Artificial Intelligence Industry (深圳经济特区人工智能产业促进条例) (Shenzhen Municipal People's Congress, 30 August 2022; Effective 1 November 2022).
[19] See Table 3: Selected Laws on AI Governance in China, including the *Shanghai Regulations on Promoting the Development of the Artificial Intelligence Industry* and the *Shenzhen Special Economic Zone Artificial Intelligence Industry Promotion Regulations*
[20] Supra note 18.

mitigate ethical and compliance risks. Article 72 requires enterprises to conduct ethical safety audits and risk assessments on potential adverse impacts of their AI products and services. Similarly, Article 66 of the *Shanghai Regulations on Promoting the Development of the Artificial Intelligence Industry*[21] establishes an AI Ethics Expert Committee responsible for formulating ethical guidelines, promoting corporate AI safety governance, and conducting risk assessments. Article 67 explicitly prohibits enterprises from engaging in activities that endanger national or public security, infringe on personal privacy, or use algorithms for discriminatory practices, including price discrimination. Article 69 outlines ethical standards for companies using AI in human resources management. Additionally, Article 16(2) encourages enterprises to submit evaluation reports on public-interest-related algorithms to relevant authorities and to explain algorithmic principles in a publicly understandable manner. Article 37 incentivizes enterprises to participate in setting technical standards for algorithm performance, data security, and privacy protection.

(ii) Personal Information Protection

To safeguard the use of AI in corporate governance, China's relevant laws and regulations establishes clear principles regarding personal information protection in AI applications. Key legislation includes the *Data Security Law*[22], *Personal Information Protection Law*[23], and *Interim Measures for the Administration of Generative AI Services*[24], which collectively provide a solid legal foundation for personal information protection. These laws specify that enterprises must ensure personal information security in the collection, use, and management of data, prevent data leaks, and adhere to principles of legality, legitimacy, necessity, and user consent.[25] The revised *Company Law of China* further strengthens board responsibilities, prompting many Chinese enterprises to establish dedicated committees overseeing AI compliance to ensure that technological applications remain ethically and legally sound.[26][27]

[21] Supra note 17.
[22] Data Security Law of the People's Republic of China (中华人民共和国数据安全法) (NPC Standing Committee, 10 June 2021; Effective 1 September 2021).
[23] 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) (NPC Standing Committee, 20 August 2021; Effective 1 November 2021).
[24] Interim Measures for the Management of Generative Artificial Intelligence Services (生成式人工智能服务管理暂行办法) (Cyberspace Administration of China et al., 10 July 2023; Effective 15 August 2023).
[25] See Table 3: Selected Laws on AI in China, including the *Personal Information Protection Law of the People's Republic of China* and the *Interim Measures for the Management of Generative Artificial Intelligence Services*
[26] Deloitte, Director Training: Progress and Trends in Corporate Governance, 19 December 2024, https://mp.weixin.qq.com/s/YJ12HxazR9SX8BnAcdTqMw.
[27] Leo E Strine Jr, Corporate Governance and Regulation of AI Applications, 21 July 2024, https://mp.weixin.qq.com/s/O7ooIsrT0jomD-XSHaCfUQ.

In addition to binding laws, soft law instruments such as the *New Generation Artificial Intelligence Ethics Code*[28] and the *Global AI Governance Initiative*[29] provide policy guidance to promote AI applications in core business areas while ensuring privacy protection and data security in AI research[30] and deployment.[31]

(iii) Multi-Agency Collaborative Regulation

China employs a multi-agency, cross-sectoral collaborative regulatory approach to oversee AI adoption in businesses. Oversight of the use of AI in corporate decision-making and governance is shared by multiple regulatory bodies, including the Cyberspace Administration of China, the National Development and Reform Commission, the Ministry of Industry and Information Technology, and the Ministry of Public Security. For instance, the Cyberspace Administration of China oversees AI data security, while the State Administration for Market Regulation ensures AI compliance in market competition[32].

(b) Data Protection Regulatory Framework

In China, AI applications in corporate governance and data protection regulations are characterized by a dual focus on development and security. On one hand, policies and technical standards incentivize AI adoption, while on the other, hard laws set clear boundaries for data security, emphasizing personal information protection, data classification and grading, and cross-border compliance. At the same time, sector-specific regulations tailor oversight requirements to industry characteristics. To achieve both innovation and regulatory compliance, enterprises must establish robust data management systems while addressing ethical risks and multi-agency regulatory requirements.

The core legislative pillars in this area include the *Data Security Law,*[33] *Cybersecurity Law,*[34] and *Personal Information Protection Law,*[35] complemented by industry-specific regulations

[28] Ethical Norms for the New Generation Artificial Intelligence (National Governance Committee for New Generation AI, 25 September 2021).
[29] Global Initiative for AI Governance (全球人工智能治理倡议) (Cyberspace Administration of China, 18 October 2023).
[30] See Table 3: Selected Laws on AI in China, including *The State Council's Notice on Issuing the New Generation Artificial Intelligence Development Plan*[30] and the *Global AI Governance Initiative*
[31] Supra note 29.
[32] See Table 3: Selected Laws on AI in China, including the *Interim Measures for the Management of Generative Artificial Intelligence Services*
[33] Supra note 22.
[34] Network Security Law of the People's Republic of China (中华人民共和国网络安全法) (NPC Standing Committee, 7 November 2016; Effective 1 June 2017).
[35] Supra note 23.

governing data flow security, personal information protection, and cross-border data transfers. Key regulatory priorities include:

(i) Data Flow Security and Governance

To address systemic risks associated with data circulation, relevant laws and regulations mandate that enterprises establish and improve data classification and protection mechanisms, ensure lawful data sourcing, implement privacy safeguards, and regulate data flow and transactions. For example, the *Implementation Plan for Improving Data Flow Security Governance to Enhance the Marketization and Value of Data Assets*[36] requires enterprises to identify and report important data and comply with regulatory supervision to ensure secure data flows.

Further policy direction is provided by the *Opinions on Promoting Enterprise Data Resource Development and Utilization*[37], issued by the National Data Bureau, which encourages enterprises to lawfully utilize data resources, protect corporate data rights, and explore various data circulation models such as data sharing, exchange, and trade. In the industrial and IT sectors, the *Trial Measures for Data Security Management in the Industrial and Information Technology Sector*[38] require enterprises in these industries to refine their data governance structures and strictly manage data collection, storage, and sharing processes.[39]

In terms of emergency response and accountability, Article 42 of the *Cybersecurity Law*[40] and Article 29 of the *Data Security Law*[41] require enterprises to establish emergency response plans and promptly remedy and report data breaches. The Supreme People's Court's *Provisions on the Legal Issues of Using Facial Recognition Technology for Processing Personal Information*

[36] Implementation Plan On Improving The Security Governance Of Data Circulation And Better Promoting The Marketization And Valorization Of Data Elements (关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案) (NDRC et al., 15 December 2023).
[37] Opinions On Promoting The Development And Utilization Of Enterprise Data Resources (关于促进企业数据资源开发利用的意见)(National Data Administration, 21 January 2024).
[38] Measures for the Management of Data Security in the Field of Industry and Information Technology (for Trial Implementation) (工业和信息化领域数据安全管理办法（试行）) (Ministry of Industry and Information Technology, 13 December 2022).
[39] See Table 4: Selected Laws on Data Protection in China, including the *Notice on Improving Data Circulation Security Governance*, *Opinions on Promoting the Development and Utilization of Enterprise Data Resources*, and *Interim Measures for Data Security Management in the Industrial and Information Technology Sector*.
[40] Supra note 34.
[41] Supra note 22.

in Civil Cases[42] explicitly states that unauthorized use of facial recognition data constitutes an infringement of personal rights.[43]

(ii) Personal Information Protection

Enterprises are legally required to protect personal information across all stages of the data lifecycle–collecting, storing, processing, and sharing–by adhering to the principle of minimum necessity, enhancing data collection transparency, and strictly controlling the use of personal data. For example, regarding collection and usage restrictions, Article 6 of the *Personal Information Protection Law*[44] mandates minimizing the scope of data collection, while Article 14 emphasizes the principle of separate consent. Enterprises must have a clear purpose for collecting personal information and are prohibited from excessive data collection. Additionally, personal information processing should follow the principles of openness and transparency, requiring enterprises to disclose data processing rules. Article 22 of the *Regulations on Network Data Security Management*[45] prohibits the excessive processing of personal information, and sensitive data requires separate authorization.

Different industries are subject to differentiated regulatory requirements, particularly sectors that involve large-scale data processing, such as algorithmic recommendation systems, AI, healthcare, finance, and e-commerce. These industries are governed by additional compliance requirements related to user privacy protection, and algorithmic transparency. The *Regulations on the Administration of Algorithmic Recommendations for Internet Information Services*[46] require providers of algorithmic recommendation services to establish sound mechanisms for data security and personal information protection. Article 7 of the *Interim Measures for the Management of Generative Artificial Intelligence Services*[47] specifies that AI training data must come from lawful sources and must not infringe on intellectual property rights or user privacy. Additionally, Article 31 of the *Measures for the Administration of Information*

[42] Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law to the Trial of Civil Cases Relating to the Handling of Personal Information by Using Face Recognition Technology (最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定) (Supreme People's Court, 28 July 2021; Effective 1 August 2021).
[43] See Table 4: Selected Laws on Data Protection in China, including the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, and the *Supreme People's Court Provisions on the Application of Law in Civil Cases Involving the Use of Facial Recognition Technology*.
[44] Supra note 23.
[45] Supra note 34.
[46] Internet Information Service Algorithm Recommendation Management Regulations (互联网信息服务算法推荐管理规定)(Cyberspace Administration of China et al., 4 January 2022; Effective 1 March 2022).
[47] Supra note 24.

Technology by Securities and Fund Management Institutions[48] mandates that securities and fund management firms implement data encryption, access control, and backup measures to safeguard customer information and prevent data breaches and losses.[49]

(iii) Regulation of Cross-Border Data Flows

In response to increasing global demand for data circulation, China has imposed strict compliance requirements on enterprises for cross-border data transfers. The *Measures for Security Assessment of Outbound Data Transfers*[50] stipulate that enterprises must conduct security assessments and mitigate risks before providing data to overseas entities, ensuring the lawful and orderly flow of data. The *Measures for the Standard Contract for Cross-Border Transfer of Personal Information*[51] require enterprises to complete a personal information protection impact assessment before transmitting personal data abroad, ensuring the security and free flow of personal information.[52]

1.2 Corporate practice and challenges ahead

(a) Corporate Practice

The board of directors of a listed company may establish a risk committee to oversee risks and review the company's risk management framework at least once annually. Currently, many Chinese companies have set up risk management committees or combined audit and risk committees as effective mechanisms to ensure the company establishes proper risk oversight, management, and internal controls. These mechanisms provide the transparency, focus, and judgment necessary to oversee the company's risk management framework. For companies without a risk management committee, any issues typically addressed by such a committee should be raised through the board's procedures.

The risk management committee generally perform a broad range of functions, including:

---

[48] Measures for Information Technology Management of Securities Fund Operators (证券基金经营机构信息技术管理办法)(China Securities Regulatory Commission, 11 June 2021; Revised 1 January 2023).

[49] See Table 4: Selected Laws on Data Protection in China, including the *Personal Information Protection Law*, *Regulations on Network Data Security Management*, *Regulations on the Administration of Algorithmic Recommendations for Internet Information Services*, *Interim Measures for the Management of Generative Artificial Intelligence Services*, and *Measures for the Administration of Information Technology by Securities and Fund Management Institutions*.

[50] Data Exit Security Assessment Methodology (数据出境安全评估办法) (Cyberspace Administration of China, 7 July 2022; Effective 1 September 2022).

[51] Standard Contractual Approach to Personal Information Exit (个人信息出境标准合同办法) (Cyberspace Administration of China, 22 February 2023; Effective 1 June 2023).

[52] See Table 4: Selected Laws on and Data Protection in China, including the *Measures for Security Assessment of Outbound Data Transfers* and the *Measures for the Standard Contract for Cross-Border Transfer of Personal Information*

overseeing the risk management framework and its execution; reviewing risk reports and raising concerns; supervising the compliance framework; and evaluating the management's responses to critical risk issues while providing guidance. [53] Under this structure, the board plays a central role in the internal control and compliance, ensuring that risk is managed within a well-established system and orderly management. [54]

Risk considerations, including technological risks, are a clear responsibility of the board.[55] In response to the growing relevance of emerging technologies, several technology companies, particularly state-owned listed tech firms, have established specialized technology committees within their boards, such as Tian Era Electric, Guodian Nanrui, and Guotou Intelligent. Companies like Keshun Group [56]and Beixin Building Materials[57] have also set up technology committees to promote technological innovation and the transformation of new technology into value.[58] In other industries, such as those represented by Northeast Securities and Hongta Securities, companies have set up Information Technology departments to manage technological risks and integrate them into their overall risk control systems. [59]

In accordance with the PRC Code of Corporate Governance for Listed Companies, a listed company shall establish internal control and risk management systems, and set up a special department or designate an internal department to be responsible for the inspection and supervision of the company's important operations, control over subsidiary companies, disclosure of financial information and compliance with the laws and regulations." [60]

---

[53] KPMG (2 April 2024) , "Directors' Toolbox Series No. 10 Risk Management in Corporate Governance, https://mp.weixin.qq.com/s/pdRZ8I3Y5brFIRnoEF1_6w

[54] China Listed Companies Association (10 November 2023) , 2023 Corporate Governance Best Practice Case Sharing | SHUNFENG HOLDINGShttps://mp.weixin.qq.com/s/Crtw_CYGLyMpXTWaKkTV1g

[55] Finance & Economics, 20 November 2024, "To Enjoy the Technology Dividend, Boards Need Technology Committees" https://mp.weixin.qq.com/s/sXPVwg1tOAhUseypYs1Onw

[56] Keshun Group (20 Aug 2024), Keshun Group Technical Committee was formally establishedhttps://mp.weixin.qq.com/s/vqt8_SC9DYojyQznpHPbtA

[57] "Inaugural Meeting of Beixin Building Materials Science and Technology Committee Held" published by "Beixin Building Materials" on August 28, 2024, on the public number of "Beixin Building Materials", https://mp.weixin.qq.com/s/42fsNgm-KPIPe785235_6A

[58] "Creating an Intelligent Board of Directors: The Role and Value of the Science, Technology, and Innovation Committee," published on 14 May 2024 by Mixed Reform News.https://mp.weixin.qq.com/s/zJIITnCzrhnbc-HXzCzMaQ

[59] Source: "Credit Rating Report on Northeast Securities Co., Ltd. 2025 Public Offering of Short-term Corporate Bonds for Professional Investors (Second Issue)" "2024 Semi-Annual Report of Hongta Securities Co.

[60] Article 94, Announcement No. 29 [2018] of the China Securities Regulatory Commission—Code of Corporate Governance for Listed Companies (2018 Revision) states: " Listed companies shall establish an internal control and risk management system and set up a full-time department or designate an internal department responsible for inspecting and supervising the company's important operating behavior, control of subsidiaries, disclosure of financial information and compliance with laws and regulations."

As to disclosure of technology risk, China Securities Regulatory Commission,[61] states as follows:

> An issuer contemplating a listing on the STAR Market or ChiNext Market shall, in 'Business and Technology,' in light of the technological level of the industry and its contribution to the industry, disclose the technological sophistication of the issuer and specific indications; the application and contribution of the issuer's core technology in its main business and products or services; the proportions of core technical personnel and research and development personnel to the total number of employees, the academic background composition of core technical personnel, the professional qualifications and important scientific research achievements obtained, awards received, specific contributions to the research and development of the company, constraint and incentive measures implemented by the issuer for core technical personnel, major changes in core technical personnel during the reporting period, and the impact on the issuer.
>
> In the case of a contemplated listing on the STAR Market, the issuer shall disclose its research strength and achievements as to its core technology, including significant awards received, material research projects undertaken, and academic papers published in core academic journals; and the commercialization of new technology and products of the issuer.

To assess the extent to which Chinese listed companies disclose technology-related risks in practice, we conducted a search using the keyword "technological risks" as the main subject on the "Weiwei Data" website, limiting the search to announcements published by listed companies in China's three main stock markets (Shanghai, Shenzhen, and Beijing). The search covered "annual reports," "semi-annual reports," "quarterly reports," "initial public offerings and listings," "pre-disclosures," "secondary offerings," "convertible bonds," "supplements and corrections," "transactions," "shareholder meetings," "equity changes," "intermediary reports," "other significant matters," "bond announcements," "investor relations," "supervisory board announcements," "board announcements," "risk warnings," "corporate governance," "daily

[61]Article 97, Announcement No. 4 [2023] of the China Securities Regulatory Commission—Announcement on Issuing the Standards for the Contents and Formats of Information Disclosure by Companies Offering Securities to the Public No. 57—Prospectus）

operations," "other announcements," "equity refinancing," "issuance sponsorship letters," "prospectuses," "Mainboard - Inquiries and Responses," "Beijing Stock Exchange - Drafts," and other related announcements. The search, covering the period from January 1, 2024, to March 15, 2025, identified 1,695 companies from the three mainland stock markets that had disclosed or mentioned technological risks in their announcements. These companies represent a broad cross-section of industries, such as finance, wholesale and retail, manufacturing, information transmission, software, and information technology services. The market types include the Shenzhen Main Board, Shanghai Main Board, STAR Market (Sci-Tech Innovation Board), Beijing Stock Exchange, and Shenzhen ChiNext. In terms of announcement types, the most common are annual reports, semi-annual reports, quarterly reports, trading announcements, and corporate governance announcements.

(b) Future directions and challenges

While AI applications bring numerous opportunities, they also present significant challenges.

(i) Corporate Governance and Development

The governance structures of enterprises have generally not kept pace with the rapid advancement of AI technologies. In the Asia-Pacific region, fewer than 10% of companies have mature AI governance frameworks, while 91% remain in the early stages. Security vulnerabilities and privacy concerns are major challenges.[62] Additionally, the AI-driven digital transformation of traditional industries comes at a high cost, with an average return-on-investment cycle of 5.2 years, limiting AI adoption among small and medium-sized enterprises.[63]

Boards of directors also face novel governance challenges, such as the lack of transparency in AI-assisted decision-making and unclear accountability. When AI systems make errors, it is difficult to determine whether the responsibility lies with the board or the technology providers.[64] Furthermore, independent directors, supervisory boards, and audit committees often lack the necessary technical expertise to effectively oversee AI applications.[65]

[62] Deloitte, Choices in the AI Era: Building Trust for Sustainable Intelligence, 16 January 2025, https://mp.weixin.qq.com/s/dWEqKbHoXkMsTS_n5ISlGA.
[63] Supra note 16.
[64] Supra note 11.
[65] Supra note 27.

Many real-world cases in China highlight these issues.[66] For instance, a leading automotive company implemented an AI-powered supply chain management system, which misjudged procurement decisions, leading to a billion-yuan loss.[67] The board members shifted blame, attributing the failure either to algorithmic flaws or to biased training data. Since no clear responsibility framework was established when AI was introduced, the lack of accountability hindered problem resolution and business improvement. Another example involves an advertising company that deployed an AI-based director to approve proposals. The AI system, prioritizing click-through rates, rejected creative but low-traffic proposals, resulting in the release of 2,000 uninspired advertisements in a year, ultimately damaging the brand's reputation.

(ii) Data Security and Privacy Protection

Despite the commercial potential of AI, data security, privacy protection, and weak oversight remain primary concerns for businesses. AI systems may exacerbate data misuse, such as excessive analysis of user data leading to privacy breaches.[68] The construction of large-scale datasets increases risks of data leaks or misuse. Additionally, AI applications can infringe on personal privacy and labour rights, particularly in employee management scenarios where the scope of data collection is expanded.[69]

Over the past year, 25% of enterprises have experienced AI-related incidents, such as data breaches, yet 40% of of these firms lack formal reporting mechanisms.[70] In response, some companies have attempted to address these risks by limiting excessive data collection through internal policies and establishing data ethics committees to oversee ethical data processing.[71]

Non-compliant or improperly regulated AI use can introduce risks in security, compliance, bias, and operations. For example, the emergence of "shadow AI" (where employees 'go rogue' so to speak and use AI even when company policy does not allow it) is becoming prevalent in China. Reports indicate cases such as an intern at a marketing firm using ChatGPT to draft content, inadvertently leaking confidential client information; a data scientist training AI

[66] AI Assistant, When Digital Human CEOs Take Over Boards: How AI Exposes Traditional Management, 25 February 2025, Wanwu Link, https://mp.weixin.qq.com/s/slMgh6HjKmjkxUmvGEIYRg.
[67] Supra note 11.
[68] Supra note 27.
[69] Supra notes 11 and 27.
[70] Supra note 62.
[71] Supra notes 11 and 27.

models with biased datasets, leading to unfair sales decisions; and a developer integrating vulnerable APIs, resulting in customer communication logs being stolen.[72] The accessibility of AI tools combined with a lack of technical oversight is a key factor behind these incidents.

(iii) Algorithmic Bias

The increasing use of "black-box" AI algorithms, whose internal decision-making processes are opaque even to developers, have become an increasing concern for Chinese enterprises. These mainstream AI models are highly complex and autonomous, but lack explainability and accountability. For example, in 2022, a Chinese matchmaking platform mistakenly flagged a regular user as a scammer due to an algorithmic misjudgement, highlighting the risk of "false positives" in AI systems.[73] The lack of transparency in AI decision-making makes it difficult to track and verify the legitimacy of such outcomes, reducing user trust and potentially hindering long-term business development.

In addition, SOEs face challenges in data governance, as issues with data quality and security can compromise the accuracy of AI-driven decision-making.[74] While some companies are exploring tiered data management and security frameworks, overall governance levels still need improvement.[75] Notably, China's "East Data, West Computing" project aims to integrate data and energy resources by systematically building key industry datasets.[76]

(iv) Data Quality and Decision-Making Risks

The emergence of AI-driven corporate governance, such as AI-powered board advisors, relies heavily on the quality, consistency and timeliness of underlying data. Inconsistent data definitions and siloed data systems can lead to inaccurate AI-driven analyses and flawed business decisions, placing firms at strategic risk.

---

[72] Cyberspace Pingliang, AI Abuse: Security Risks in Modern Enterprises, 5 March 2025, https://mp.weixin.qq.com/s/x1LQ8idGBJZqaFzk6Kd8qA.
[73] Guo Li, Algorithmic Ethics and Governance in the AI Era, 8 February 2025, MIIT Headlines, https://mp.weixin.qq.com/s/DNkKYdi3mjYu3a_XqGX8uw.
[74] Huang Jianbin et al., *AI-Driven Management Reform in State-Owned Enterprises*, 21 Jan 2025, https://mp.weixin.qq.com/s/JRSK-YYIo7KRTgO4Zqo9Pw.
[75] Supra note 16.
[76] Guozi Xiaoxin (SASAC News), SASAC Launches "AI+" Special Initiative for Central Enterprises, 21 December 2025, https://mp.weixin.qq.com/s/nPwucCmTjheH9Qe91UpHOw.

For AI-based decision-making systems to function effectively, AI board members require accurate, timely, and consistent data, which depends on a company's data management capabilities.[77] However, compliance requirements for data usage increase operational costs. Misjudging AI trends can also lead to resource misallocation or missed market opportunities. If boards over-rely on AI or misinterpret AI-driven insights, they risk short-term strategic pitfalls.[78]

(v) Organisational and Talent Challenges

China currently faces a severe shortage of AI talent. Reports indicate that the supply-demand ratio for AI engineers in China is 1:8, with an estimated shortage of over 1.5 million multidisciplinary professionals. Enterprises must also balance technological investment with practical business benefits.[79]

(vi) Legal Risks and Compliance Costs

Existing legal frameworks lag behind AI development and adoption, leading to regulatory gaps. For example, emerging AI-driven board proxies operate in an uncertain legal landscape, yet some companies have already begun experimenting with AI-based decision-making models. Additionally, companies face stringent cross-border data regulations, such as the EU's GDPR and the U.S. CLOUD Act, which increase compliance costs for multinational businesses.[80]

China's "*AI Security Governance Framework*" emphasises risk assessment and inclusive development.[81] However, on the international stage, AI governance remains unbalanced. The United Nations lacks a leading regulatory body, while global AI rules are increasingly competitive, which exemplified by U.S. and EU restrictions on AI technology exports. Furthermore, developing countries remain underrepresented in shaping AI governance frameworks.[82]

---

[77] Li, Zhaoyi, Artificial Fiduciaries (July 28, 2023). Washington and Lee Law Review, Vol. 81, No. 4, Forthcoming, U. of Pittsburgh Legal Studies Research Paper No. 2023-31, Available at SSRN: https://ssrn.com/abstract=4524129 or http://dx.doi.org/10.2139/ssrn.4524129.
[78] Supra notes 16 and 12.
[79] Loong, SASAC's AI+ Initiative for SOEs, 19 February 2025, https://mp.weixin.qq.com/s/t7sCnEdGzCvzLPzJ1eFHfQ.
[80] Supra note 11.
[81] Han Yonghui et al., Current Status, Challenges and China's Approach in Global AI Governance, 15 January 2025, https://mp.weixin.qq.com/s/WhQYONugMmTiXxa7i0E4ig.
[82] Supra note 81.

2. India

Although India's corporate law can broadly be said to be similar to its UK counterpart, the years since independence have resulted in some context-specific additions. Corporate governance however has sharply deviated from the initial voluntary approach inspired by the UK and has now taken on what has been called an 'ultra-mandatory approach'.[83] With technology related risks, there are a multitude of law and regulations regarding cyber security and data privacy issues, either in force or coming into force in the near future.

On the other hand, there is no legislation on AI as yet and so that is a space where corporations must attempt to practice good governance in anticipation of regulations. International AI laws will also be a factor considering that many Indian companies have cross-border operations or will look to market their products and services overseas. For example, companies in the West have a long history of outsourcing customer service operations to call centres in India and this is now taking the shape of chatbots (using GenAI) delivering customer service solutions to overseas companies.[84] Of course, AI development and deployment also data protection and cybersecurity issues, and so the entire gamut of digital governance will be very important.

Although India has not witnessed major developments like companies announcing the adoption of AI board members (as we saw with VITAL in Hoong Kong)[85] or even AI systems for making corporate decisions, companies are indeed deploying AI tools at various levels. In 2024, A BCG Report noted that 30% of Indian companies are using AI (as against the global average of 26%).[86]

2.1 Hard and soft law on digital governance

The main legal developments both in terms of hard and soft law that impact digital governance in India can be put into two broad categories – cybersecurity and data privacy, and AI governance.

---

[83] Umakanth Varottil, 'Corporate Governance in India: The Transition from Code to Statute' in Jean J. du Plessis and Chee Keong Low (eds) *Corporate Governance Codes for the 21st Century* (Springer International Publishing, 2017) 98.
[84] Jessica Sier, 'Indian outsourcers want Aussie companies to pay for bots not bodies' (Australian Financial Review 6 March 2023) https://www.afr.com/technology/indian-outsourcers-want-aussie-companies-to-pay-for-bots-not-bodies-20230226-p5cnpn. ["Indian services companies – which have provided offshore workers for some of Australia's biggest companies for decades – are retooling for the artificial intelligence era, where programs such as ChatGPT can automate their roles…"].
[85] Above n. 13.
[86] 'India is leading in AI adoption at 30%, surpassing global average of 26%: BCG Report' (Economic Times, Nov 12, 2024) https://cio.economictimes.indiatimes.com/news/artificial-intelligence/india-is-leading-in-ai-adoption-at-30-surpassing-global-average-of-26-bcg-report/115201819

For privacy and data security, the government introduced a cross-sectoral legislation – the Digital Personal Data Protection Act (DPDPA), 2023 which came into effect at the end of 2024. The legislation introduces a comprehensive privacy regime and mandates, amongst other requirements, the DPDPA requires companies to notify affected individuals of data breaches. While this is likely to impose a significant compliance burden on companies, it will also help address privacy and data security risks.

One significant point to note under the DPDPA is that it follows a liberal approach regarding data localisation. Essentially, cross-border data transfers would be allowed to all countries except those that were restricted by the government. However, in January 2025, MeitY (India's Ministry of Electronics and Information Technology) notified draft rules under the DPDPA which allow for more ad hoc restrictions.[87] As these draft rules are yet to be finalised, the direction of future cross-border data governance remains uncertain.

Complementing the DPDPA are sector-specific cybersecurity regulations issued by the Securities Exchange Board of India ("***SEBI***"). In August 2024, SEBI issued a 'Cybersecurity and Cyber Resilience Framework' (CSCRF) (hereinafter called 'August 2024 Circular') complementing the DPDPA, followed by additional clarifications in December 2024 (hereinafter called 'December 2024 Circular').[88] The August 2024 Circular essentially mandates that all regulated entities must 'establish appropriate security monitoring mechanisms through Security Operation Centre (SOC)'.[89] For small companies, the two stock exchanges in the country are required to set up a Market SOC (M-SOC) with the objective of providing cybersecurity solutions.[90] Essentially, companies have to conduct regular cyber audits and report on this to SEBI. When there is a cybersecurity incident, actions taken to recover from the incident should be 'informed to all the relevant stakeholders as required'.[91] These requirements will be effective from early 2025 and, per the December 2024 circular, there will be lenient enforcement of these requirements up to March 2025. The two studies

[87] MeitY, Digital Personal Data Protection Rules, 2025.
[88] SEBI, 'Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)' (20 August 2024) SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113; SEBI, 'Clarifications to Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)' (31 December, 2024).
SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/184.
[89] Ibid (August 2024 Circular), 7.
[90] Ibid.
[91] Ibid, 16.

conducted in Section 2.2(b) of this paper will provide a snapshot of corporate practice in this regard in 2024, i.e., leading up to 2025 when the cybersecurity regulations come into force.

The CSCRF essentially came in on top of existing Information Technology Act under which the Computer Emergency Response Team – India (CERT-In) provides guidelines for monitoring, detecting, preventing, and managing cybersecurity incidents.[92] According to these guidelines, companies must take specific actions or provide information about cyber incidents and the responses to such incidents. The CERT-In operates under the aegis of MeitY.

While India has not introduced an AI legislation yet, there are broader policy indications around AI governance from reports issued by MeitY.[93] The last of these reports, Report of Committee – D on cyber security, safety, legal and ethical issues, provides some indication of the possible future directions of law on AI regulation. The committee has noted that a 'flexible framework for assessing the appropriate scope and technical feasibility of various accountability mechanisms will help, to maximise the benefits algorithms afford and mitigate potential drawbacks'.[94] It further notes that implementation of this ideal will require a multi-faceted approach consisting of flexible principles to allow self-regulation, consideration of algorithms 'in the context in which they are being applied and the potential social and economic impact of their application', establishment of 'best practices to scrutinise the data sets used to train the algorithms', testing and auditing algorithms internally, and engagement with civil society.[95] The report then goes on to note that sector specific regulations would be best suited to achieve these aims.[96]

The report also makes a point of noting the importance of engaging 'with governance bodies around the world to share and learn from experiences' and encouraging 'industry to share best

[92] CERT-In was introduced by the Information Technology (Amendment) Act 2008.
[93] There are four reports on AI issued by MeitY: Report of committee – A on platforms and data on Artificial Intelligence; Report of committee – B on leveraging Artificial Intelligence for identifying national missions in key sectors; Report of committee – C on mapping technological capabilities, key policy enablers required across sectors, skilling, reskill; and Report of committee – D on cyber security, safety, legal and ethical issues. See https://www.meity.gov.in/ministry/our-groups/details/ai-emerging-technologies-division.
[94] MaitY, 'Report of committee – D on cyber security, safety, legal and ethical issues' 31.
[95] Ibid, 31 – 32.
[96] Ibid, 36.

practices and promote codes of conduct'.[97] Thus there is an interest in collaborating internationally and also locally with members of the industry.

In the meantime, there are some judicial decisions regarding intellectual property issues, particularly allegations of copyright violations against OpenAI and other AI developers as we are seeing in the rest of the world.[98] In one case, the Delhi High Court in 2023 ruled against the use of deepfakes (fake images of a person) created by GenAI, to market products via false endorsements. Such conduct was held to be a case of personality theft.[99] Companies should factor in the evolving jurisprudence around AI, and even in the absence of available precedent be cautious about what use AI tools are being put to, because this is an evolving area of law and there are both reputational and liability issues that could arise as a publicity crisis unfolds, or the law evolves, respectively.

Thus, law and regulation around digital governance is still taking shape. However, there are many developments in terms of how attitudes, practice, and policy are playing out in the absence – even if regulation has been foreshadowed – of the law.

2.2. Attitudes, practice, and challenges ahead

(a) Attitudes

Corporate management in India is aware of the technology related risks. In a 2023 study conducted by Bloomberg interviewed 300 executives including CTOs (Chief Technology Officers) in India to understand the changing risk landscape for companies. The study found that data security risks, regulation risks, and reputational risks had increased significantly since a decade ago.[100] Not only this, data security and privacy risks were ranked as the highest in terms of frequency of happening.[101] It will be unsurprising if a similar study conducted today finds data security breaches as even more of a serious risk than before considering that the number of incidents involved data security breaches have only increased. One study found that

[97] Ibid, 38.
[98] Arpan Chaturvedi and Aditya Kalra 'OpenAI seeks to block Indian media groups from copyright lawsuit' (Reuters 28 January 2025) https://www.reuters.com/technology/openai-asks-indian-court-throw-out-book-publishers-challenge-copyright-battle-2025-01-28/.
[99] Anil Kapoor v Simply Life India & Ors CS(COMM) 652/2023.
[100] Bloomberg, 'In Flux: Navigating India's Changing Risk Landscape' (2023) 6 https://assets.bbhub.io/professional/sites/10/2521503_Bloomberg_Navigating_Indias_Changing_Risk_Landscape.pdf
[101] Ibid, 7.

there were '388 data breaches, 107 data leaks, 39 ransomware activities, and 59 cases of access sales or leaks in the first six months of 2024'.[102]

Beyond data security and privacy breaches there are other tech-related risks and strategic issues that are animating corporate governance discussions. In a 2025 study conducted by Russel Reynolds, it was noted that boards in India view AI as both something that 'continues to create new opportunities in business prospects and operational efficiency, as well as new risks regarding data integrity, IP infringement, and responsible usage'.[103] Interestingly, the report also notes that boards are and should adapt to new trends in consumer behaviour. It notes as follows[104]:

> Rising disposable incomes, telecom penetration, digital revolution, and disruptive business models have increased competition, leading consumers to purchase differently than they have in the past. Customer loyalty can no longer be taken for granted. With each passing generation, the Indian business landscape is witnessing a pace of change and appetite to experiment that is growing by leaps and bounds. Experts advise that companies and their boards reassess their strategic go-to-market blueprints and right-to-win amidst this dynamic demographic transformation.

These new consumer trends are prompted, amongst other things, by technology. Social media allows consumers to talk about companies with others and this has a reputational impact for companies.[105] This may explain why the 2023 Bloomberg study noted a rise in reputational risks, as perceived by corporate executives in India.[106] Supporting this, a 2024 survey by PWC found that 82% of Indian consumers surveyed 'stated that protection of their personal data is one of the most crucial factors to earn their trust'.[107] The survey also found that despite there being 'high interest in the use of chatbots, consumers demand direct connection with a sales representative'.[108] This underscores the importance of balancing AI adoption to enhance the customer experience, with human engagement in customer-facing. Based on its findings, PwC

[102] https://www.deccanherald.com/opinion/are-indias-companies-ready-to-tackle-data-breaches-3239613
[103] https://www.russellreynolds.com/en/insights/reports-surveys/global-corporate-governance-trends/2025/india.
[104] Ibid.
[105] In previous work, I have called this 'hashtag capitalism'. See Akshaya Kamalnath, 'Hashtag Capitalism – An Introduction' (2024) Alternative Law Journal
[106] Above n. 102.
[107] PwC, 'Voice of the Consumer Survey 2024 - India perspective' (2024) https://www.pwc.in/assets/pdfs/voice-of-the-consumer-survey-2024india-perspective.pdf.
[108] Ibid, 22.

proposed a 12-point action plan for companies in India, of which I extract three relevant points below:

- *Prioritise data protection*: Implement robust data security measures and clearly communicate these to consumers. Use data to enhance personalisation in a way that respects privacy and builds trust.
- *Integrate AI while ensuring human oversight*: While adopting AI for internal improvements and consumer-facing tasks, prioritise human oversight to address complex or unresolved issues.
- *Craft a regulatory-compliant AI strategy*: Given consumer concerns about GenAI, develop a responsible strategy aligned with emerging regulations to build trust and mitigate risks for the next few years.

PwC's pointers are meant as guidance for companies in India to adopt voluntarily, based on the findings of its survey, irrespective of whether regulations require any of this. While the DPDPA was set to take effect only at the end of 2024, corporate management was already on notice (based on stakeholder considerations which would have reputational impacts) to develop a policy and implement measures regarding data security and privacy. Likewise, despite the absence of a dedicated AI legal framework, the basic idea of human oversight has been around both in academic literature and from global regulations.[109] Crafting a company-specific AI strategy in anticipation of regulations that may be introduced in India (the MeitY report has clues that such regulation is coming) and in light of global regulations.[110]

The next section looks at corporate practice regarding technology related risks.

(b) Corporate practice

One obvious indication that companies in India are taking digital governance seriously is the fact that many companies have appointed Chief Technology Officers (CTOs) – thus,

[109] See eg. Jeremias Adams-Prassl, Halefom Abraha, and Sangh Rakshita 'Regulating algorithmic management: A blueprint' ELLJ 124.
[110] Above n. 94.

recognising the need for specialised expertise at the C-Suite level.[111] These CTOs are generally responsible for leading strategic tech transformation of companies and with tech risk management.

This section examines corporate responses to technology-related risks by, firstly, survey some incidents of data security and privacy breaches and how companies handled them. Next, this section will conduct an exploratory study of the top 14 (by market capitalisation) companies listed on India's National Stock Exchange (NSE), by looking at their disclosures regarding tech-related risks and digital governance practices in 2024. Together, the two studies offer insight into both the *ex ante* and *ex post* practices to digital risk, occurring against the backdrop of anticipated regulatory change with the forthcoming implementation of the DPDPA.

The first study focuses on corporate responses to cybersecurity and data privacy breaches reported in 2024. For this study, we looked at cybersecurity and data privacy breaches reported in 2024. Since we are relying on media reports, this list of incidents cannot be considered a full list. Despite this limitation, the study provides an interesting variety of responses from companies. The incidents occurred at a time when companies were already aware of their future compliance obligations under the DPDPA, providing insight into their state of preparedness. The study comes with the obvious limitation of only looking at the companies that have suffered data security breaches. This means that we cannot draw conclusions that can be generalised across the board, but it still gives us a flavour of corporate readiness or lack of it, to handle tech risks. However, when read in conjunction with the second study, focused on larger, presumably governance-leading companies, such as NSE Top 14 (by market capitalisation) companies which will ideally be the 'best in class' in terms of corporate governance practices, the overall analysis gains a degree of balance.

As Table 1 illustrates, corporate responses to data breaches varied considerably. Some companies denied[112] or did not acknowledge allegations of data breaches[113], while others

[111] Sreedha Basu 'CTOs in limelight as India Inc scrambles to navigate rapid digitalisation' (Economic Times, 8 February, 2024) https://economictimes.indiatimes.com/jobs/c-suite/ctos-in-limelight-as-india-inc-scrambles-to-navigate-rapid-digitalisation/articleshow/107501088.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[112] Bharti Airtel and Durex India.
[113] Motilal Oswal Financial Services.

barely acknowledged such allegations. A few firms demonstrated a more proactive approach by disclosing the breach and taking positive steps to address it[114]. One company even initiated legal action against the hacker and against Telegram (on which the bots that hacked the data were present).[115] It should also be noted that one of these companies, WazirX Crypto Exchange, became insolvent as a result of the cybersecurity incident, thus underscoring the importance of *ex ante* management of tech risks.[116]

Moving to the second study now, we see (from Table 2) that, as expected, many of the companies in the dataset (NSE top 13) are going above and beyond what was required per the law in India in 2024, which is the date of the annual reports in the data set. They mention being in compliance with the EU's GDPR and the DPDPA which is not yet in force in mid-2024 when most of these annual reports are published.

Only one company in our data set, RIL, does not report a cybersecurity/ data privacy policy, although it did classify data security as 'a key audit matter' and referred to data and cyber security measures in general terms in the annual report.[117]

Of the two PSUs in the data set, SBI mentions that its data protection measures align with both the EU's GDPR (noting SBI's 'SBI's international operational boundary' and the DPDPA)[118], while we do not have such language in the annual report of the Power Grid Corporation of India. However, the latter company is in the process of developing a cybersecurity readiness framework in association with the Indian Institute of Science.[119]

Several companies, such as ICICI Bank and ITC, have designated C-suite officers to oversee digital governance, consistent with emerging global best practices. Other companies, including TCS, noted innovative use of Generative AI or AI more broadly for 'protective threat

[114] WazirX Crypto Exchange.
[115] Star Health and Allied Insurance.
[116] Riya R. Alex, 'WazirX $230million hack: Creditors given two ways to recover stolen crypto -- 'extended delays till 2030 or...' (Mint, 5 February 2025) https://www.livemint.com/companies/wazirx-230million-hack-creditors-given-two-ways-to-recover-stolen-crypto-extended-delays-till-2030-or-11738758499959.html.
[117] RIL, Annual Report (2023-2024) https://rilstaticasset.akamaized.net/sites/default/files/2024-08/RIL-Integrated-Annual-Report-2023-24.pdf 33.
[118] 39, 40 https://bank.sbi/documents/17826/17948/270524-SBI+Sustainability+Report+2024.pdf.
[119] https://csp.iisc.ac.in/pgcil/

detection'. HDFC Bank disclosed having adopted a social media policy. Social media is also a key technology that has introduced both risks and opportunities and more companies should be putting together a policy on how it will leverage social media, and also address the risk associated with social media.[120] These examples indicate a willingness among leading firms to proactively invest in innovative digital governance measures voluntarily, often exceeding baseline legal requirements.

None of the companies in our data set have reported incidents of cyberattacks or data security breaches. This could mean that they did not have such incidents to report in 2024.

Finally, it should be noted that the 2024 annual reports made no mention of risks related to the deployment of AI tools. Further, many start-ups in India are developing AI tools and we cannot be sure about what guardrails these start-ups are voluntarily constraining themselves with, if any, while we await legislation on AI.

(c) Challenges ahead

All the challenges outlined in Part 1.2(b) of this paper, while discussing digital governance issues in China are challenges relevant to India as well:

(i) the need for relevant expertise on company boards and management to get digital governance right is relevant in India as well, as evidenced by the results of the two studies on corporate practices in India.

(ii) Data security and privacy protection is an ongoing challenge and in India, there will be a period of time during which the DPDPA is implemented by companies and its efficacy will be put to the test.

(iii) Algorithmic bias is a well-known problem with AI and MeitY's Report of Committee – D makes a note of this as well. It see's flexible principles around this that allows for self-regulation as a solution. The report notes as follows[121]:

> Best practices in identifying and eliminating potential bias within AI includes ensuring diversity in the sources of data, scrutinising initial datasets and inputs in order to eliminate

[120] As noted in the introduction, this paper restricts itself to two specific issues in technology – AI and data privacy.
[121] MeitY, Report of Committee D, n. 94, 29.

bias, continually testing and encouraging feedback, supporting research on practical techniques of promoting fairness and involving multistakeholder groups in these feedback processes.

(iv) Data quality and decision- making risks are an important consideration for corporate management because inappropriate decisions might have legal, reputational, and financial consequences. In line with international thinking on this, MeitY's Report of Committee – D, emphasises the need to involve humans in the decision-making loop.[122] The report also notes the issue of data quality and seems to support measures to improve access to data.[123]

(v) On organizational and talent challenges, Indian companies (and the country itself) will need to be able to retain top talent in the country and maybe even attract top AI talent from overseas.[124]

(vi) Legal risks and compliance costs are significant challenges for companies developing and deploying AI tools. Companies operating across jurisdiction will need to comply with a range of legislation and potential actions even on issues that presently unregulated. Although some level of global convergence would be desirable, the current 'de-globalising' phase of the world is unlikely to allow for this in the near future.

3. Conclusion

To date, legal scholarship on corporate law and legal developments of digital governance have largely concentrated on the extent to which emerging technologies may mitigate agency costs (which has been regarded as the core problem that corporate law seeks to address). Some optimistic scholars have even argued that we will have AI directors in future.[125] Enriques and Zetzsche have rightly cautioned us about the 'tech nirvana fallacy' noting that technology in corporate governance brings additional risks that need to be addressed.[126]

---

[122] Ibid, 29 – 30.
[123] Ibid, 31.
[124] Anirudh Suri, 'The Missing Pieces in India's AI Puzzle: Talent, Data, and R&D' (Carnegie India, 24 February 2025) https://carnegieendowment.org/research/2025/02/the-missing-pieces-in-indias-ai-puzzle-talent-data-and-randd?lang=en&center=india. ["While Indian information technology (IT) services firms and global AI majors will naturally do their bit to create an AI-enabled workforce by upskilling India's existing IT services talent, doing so will not be enough to meet the country's ambitions. India will need to attract, nurture, and retain cutting-edge, top-tier AI research talent to ensure that AI innovations for the world emerge from India."]
[125] John Armour & Horst Eidenmuller, 'Self-Driving Corporations?' (2020) 10 Harv Bus L Rev 87.
[126] Luca Enriques & Dirk A. Zetzsche, 'Corporate Technologies and the Tech Nirvana Fallacy' (2020) 72 Hastings LJ 55.

This paper has sought to shift the analytical lens from purely theoretical considerations to a grounded inquiry into how digital governance is being both regulated and practiced in China and India. B y examining both legal and policy developments alongside corporate practices, this study has aimed to identify the current challenges faced by companies in these two countries. Based on this comparative analysis, five key takeaways from the study of digital governance in China and India are laid out below. Some of these takeaways are also a call for further scholarship on digital governance in China and India.

Our first and main takeaway is that there is a convergence in corporate governance practices (if not laws and regulatory tools which remain a product of institutional factors) around AI risks.[127] We have seen higher AI adoption, more laws on AI use, and relevant issues that have come before the court in China; as compared to India. In practice, the sorts of solutions at the corporate level in both countries are not very different from what we see in the West – the use of Chief Technology Officers, a board committee to deal with tech risks, or integrating tech risks into the ambit of the risk management committee, and disclosures of tech use and risk-management of such use. However, while these come as top-down guidance from central and provincial authorities in China, they are simply responses to market demands in India. Both countries are also grappling with the political aspects of data protection, namely how cross-border data flow should be regulated. At present, India seems to have taken a more liberal approach but this is still evolving.

While corporate governance has legal and non-legal elements, it is ultimately aimed at governance of the company and this necessitates identifying and addressing risks. Our focus on digital governance as a subset of corporate governance has meant that we are looking at risk-management vis-à-vis development and deployment of technology. This risk management can be driven by law, or non-law considerations, or a combination of both. When we look at China and India, a point of similarity that stands out is that both countries have national policies to encourage development and adoption of AI by companies.

[127] For a discussion (with multiple views) of the persistence of the debate on convergence in corporate governance see Jeffrey N. Gordon and Mark J. Roe (eds.) CONVERGENCE AND PERSISTENCE IN CORPORATE GOVERNANCE (CUP, 2004).

China adopts a state-driven, pro-innovation regulatory model for AI governance that relies heavily on soft law tools such as guidelines, standards, and strategic plans. The government plays a central role in steering AI development through top-down coordination and policy incentives and guidance, rather than strict legal constraints. While China is beginning to introduce binding regulations in high-risk areas like generative AI, its overall approach remains flexible and adaptive, aiming to promote innovation while managing risks as they arise. This model contrasts with the EU's more precautionary and rights-based regulatory approach.

While China seems to have many specific regulations and soft law in terms of managing risks (as shown in Table 3 and Table 4), India has much fewer and the reason for this might be a combination of four things: First, India is a little behind in the AI adoption and consequently, law-making phase; second, India is attempting a more principles-based, flexible, and self-regulatory model of AI governance (although this is in contrast to the ultra-mandatory approach adopted in the broader corporate governance context [128]) as compared to China, which takes a rule-based regulatory model. Third, China, as a centralized state with strong state power, has a long-standing tradition of using the "invisible hand" of governance—through policy documents, administrative guidelines, and strategic plans—to steer market behaviour and shape industrial development without relying solely on formal legislation. Fourth, China, as a civil law country, relies heavily on written laws, administrative regulations, and formal guidelines to manage the risks associated with data protection and technology use. This legal tradition emphasizes codified rules and top-down regulation, resulting in a more structured and detailed regulatory framework. In contrast, India, as a common law country, tends to adopt a more principles-based and case-driven approach, with greater reliance on judicial interpretation and regulatory discretion. As a result, China has developed more comprehensive and prescriptive rules in areas like AI governance and data regulation compared to India's more flexible and evolving model.

Our second point is a reflection on what our study of both countries did not highlight. When one looks at corporate law scholarship focused on countries in Asian (and in Europe), on expects to see the issue of related party transactions (which arise as a result of the existence of

[128] Varottil, above n 83.

large controlling shareholders in these countries) become the focus. While our study has focused on company-level digital governance, we have not looked at how regulators and companies in the two countries might be using AI to monitor companies, i.e. SupTech and RegTech. Perhaps AI is a tool that they are already using to pick up patterns in corporate disclosures that indicate the possibility of related party transactions. If AI has not already been put to such use by regulators in these jurisdictions, the option should be explored because the AI applications ability to process large amounts of complex data would be well suited for the web of related parted transactions that exists in many companies in countries where firms are dominated by controlling shareholders.[129] However, it is again important to strike a cautionary note about AI not being a magic pill because even if problematic related party transactions can be identified by AI tools, as Kim warns us, regulators might be susceptible to political pressure or business lobbying depending on the context of the specific country.[130]

Third, environmental and societal concerns have become important in both AI discussion and corporate governance discussions. In China, as the discussion Part 2 of this paper shows, central SOEs are promoting ecological collaboration and ESG practices through AI. In India, these sorts of practices have not emerged in the public or private sectors. However, it is worth noting here that the policy paper on AI (titled 'National Strategy for Artificial Intelligence') by NITI Ayog (akin to a planning commission) has the subtitle '#AIForAll' and particularly notes that public sector undertakings India should be 'leaders in adoption of social AI tools'.[131] This focus from both China and India on SOEs and public sector companies respectively is not surprising considering both are emerging economies with development imperatives.

Fourth, companies everywhere are dealing with geopolitical concerns and the nature of today's AI race makes geopolitical concerns all the more relevant or companies developing or deploying AI. From the perspective of foreign companies, particularly American companies,

---

[129] For a discussion of related party transactions in East Asia including in China, see Kon Sik Kim, 'Related Party Transactions in East Asia' in Luca Enriques and Tobias H. Tröger (eds.) THE LAW AND FINANCE OF RELATED PARTY TRANSACTIONS (CUP, 2019) 285; and for a discussion of related party transactions in India (and other common law countries in Asia) see Dan W. Puchniak and Umakanth Varottil, 'Related Party Transactions in Commonwealth Asia Complexity Revealed' in Luca Enriques and Tobias H. Tröger (eds.) THE LAW AND FINANCE OF RELATED PARTY TRANSACTIONS (CUP, 2019) (noting the importance of enforcement by the regulator in the context of related party transactions) 327 – 341.

[130] Kim, ibid, 297.

[131] Niti Ayog, 'National Strategy for Artificial Intelligence #AIForAll' (2018) 93 https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

considerations of doing business in China and India is increasingly impacted by the vagaries of U.S. President, Trump's messaging.[132] A strand of corporate law scholarship talks about 'halo effect' where developing countries might adopt laws similar to western laws to attract foreign investments.[133] Likewise, in the context of the AI race, the type of laws a country adopts might not be the only thing that matters. For their part, companies will need to have geopolitics as a key risk consideration, and perhaps this will be more so for tech companies.

Fifth, leading scholars thinking about AI and corporate governance have explored the role of AI in enhancing the monitoring role of the board.[134] This emphasis is justified because monitoring of management is seen as the key function of the board in large public companies. The India and China stories suggest that, alongside monitoring (which is emphasised through the integration of AI risk-management in the risk management committee or tech committee of the board) the strategic and resource dependence roles of the board are also important. The strategic role is important because there is a push from the government in both China and India to encourage companies to adopt AI technologies which often involves large investments without the expectation of immediate returns. The resource dependence role of the board essentially identifies the ability of directors to bring their expertise and networks as valuable resources for the company. Drawing from the previously discussed issue of tech companies having to navigate geopolitical issues, and China and India being important markets and thus impacted by these issues, both the tech expertise of directors and the ability to navigate geopolitical considerations will be important for both international facing companies in these countries[135] and international companies seeking to enter China and India.

In conclusion, we should note that the pro-innovation approaches espoused by both China and India are not only in contrast with the EU's approach, but also offer alternative accounts of pro-innovation to that of the U.S. Although scholars have been preoccupied with the contrasting approaches of the U.S. and the EU, in regulating AI[136], our paper has added the accounts of China and India which are pro-innovation accounts despite having very different institutional contexts from that of the U.S. and from that of each other. We hope that political economy

[132] Liv McMahon and Zoe Klienman, 'Will iPhones cost more because of Trump's tariffs on China?' (BBC News, 11 April 2025) https://www.bbc.com/news/articles/cx28845z30go
[133] Dan W. Puchniak, 'The False Hope of Stewardship in the Context of Controlling Shareholders: Making Sense out of the Global Transplant of a Legal Misfit' (2024) 72 Am J Comp L 109 (on the stewardship code being a legal misfit in many countries.)
[134] See generally Enriques and Zetzsche, above n. 118.
[135] Curtis J. Milhaupt and Dan W. Puchniak, 'TikTok's Identity Crisis: Corporate Personality in a De-Globalizing World' (Harvard Law School Forum on Corporate Governance 3 January 2025) https://corpgov.law.harvard.edu/2025/01/03/tiktoks-identity-crisis-corporate-personality-in-a-de-globalizing-world/
[136] See eg. Anu Bradford, 'The False Choice between Digital Regulation and Innovation' (2024) 119 Nw U L Rev 377.

scholars will take up the call to provide more insights on the China and India stories regarding AI governance, using our paper (which was focused on corporate governance and technology) as a jumping off point.

Table 1: Cybersecurity/ Data Breach Incidents In 2024 In India and Company Responses

	Type of Breach	Company	Date of Breach	Steps taken to remedy (if any)
1.	The 'Kiberphantom' data breach compromised over 278 GB of data from BSNL's operations in telecom. Leaked SIM Card specifics, security keys, home location register data and intl. mobile subscriber register data numbers.	Bharat Sanchar Nigam Limited (BSNL). This is a Public Sector Undertaking. The government of India wholly owns this company.	June 26th 2024	Department of Telecommunications(DoT) informed this to the Lok Sabha (lower house of the Indian Parliament) following a CERT-In report. BSNL has changed access passwords for relevant servers and taken other technical actions to prevent a future breach.
2.	Allegations were that 375 million Airtel customers data (phone numbers, email ID, Aadhar numbers) were for sale on the dark web. This data has not been officially confirmed.	Bharati Airtel Ltd. This is an Indian multi-national company.	July 5th 2024	Allegations denied by Bharati Airtel Ltd.
3.	The cybersecurity attack targetted WazirX Crypto Exchange's multisig wallets resulting in theft of digital assets up to $230 million. The WazirX platform itself was not breached. Only the Etherium multisig wallet blockchain funds were affected.	WazirX Crypto Exchange	July 18th 2024	WazirX maintains daily reports on their website. On Daily Report dated July 18th 2024, Wazir X claims that it took the following steps after the cyberattack. Notified CERT-In Filed a complaint on the National Cyber Crime Reporting Portal Intimated all users about the cyber attack and its potential implications. However, these 'potential implications' are not disclosed on the website. Intimated Exchanges to block and

				recover stolen assets based on information that was available at that time. As WazirX admits: "*But we're not experts at forensics, so an external forensic team will be engaged to conduct a thorough audit.*"
4.	Ransomware Attack	Polycab India	March 17 2024	In a regulatory filing to the Stock Exchange, Polycab India said the Ramsomware attack has not affected its core services. Apart from saying external cybersecurity experts were working on it, no specific mention of steps taken has been disclosed.
5.	LockBit gang claimed responsibility for this Ransomware attack	Motilal Oswal Financial Services (MOFSL)	February 18, 2024	The company initially refused to acknowledge the attack to Media. Later, they accepted that there was 'malicious activity' but that business operations and IT was unaffected,
6.	Phone numbers, email IDs, shipping addresses, products ordered and amount paid - customer data was compromised. Durex India had *mistakenly exposed this data on their website themselves.*	Durex India	28th August 2024	Durex India has not acknowledged the same yet. A third party exposed this vulnerability to CERT-In. It is yet unknown what steps have been taken to remedy this issue.
7.	Medical data stolen through publicly accessible chatbots operating on Telegram. The samples could be viewed by asking the chatbots to divulge information.	Star Health and Allied Insurance	20th August 2024	Star Health acknowledged the breach happened but maintained there was no widespread compromise, and sensitive customer data remains secure. Legal action pursued against Telegram and hacker.

Table 2: Digital Governance Disclosures In 2024 Annual Reports of NSE Top 13 Companies

No.	*Company*	*Does it have a cybersecurity*	*Any other disclosures (in the 2024 annual report) of tech-risks and how they are being addressed?*

		policy and/ or a data privacy policy?	
1	Reliance Industries Limited (RIL)	No, although it has been designated as 'a key audit matter'.	RIL says its privacy and cyber security are in consonance with ISO certifications. RIL says it follows 'privacy by-design and privacy-by-default approaches' to ensure that personal data is processed ethically, securely, and legally. These phrases are not defined. RIL also claims to use a 'defense in depth' approach to tackle 'evolving threats' by use of multiple technology solutions. RIL does not elaborate on what these technologies are. The auditor has assessed and given it a clean chit regarding cybersecurity and 'IT controls' in the 2024 annual report.
2	Tata Consultancy Services (TCS)	Yes	Mentions that it has a Cyber Security business unit for risk mitigation. It also uses GenAI/AI for proactive threat detection.
3	HDFC Bank	Yes	Also mentions that it has a social media policy.
4	ICICI Bank	Yes.	Has a chief information security office (CSIO) who is tasked with implementing the cyber security and privacy policies. Has implemented a Data Leakage/Loss Prevention (DLP) system and operates a 24x7 Security Operation Centre (SoC) to monitor anonymous activities and cyberattacks, and ensure the highest level of cybersecurity standards. Conducts and participates in several cybersecurity attack simulation drills such as spear phishing drills on employees, Distributed Denial of Service (DDoS) attack drills for Internet Service Providers (ISPs), social engineering-based attacks on data center staff to gain physical access etc. Also has an Information Technology Strategy Committee to review IT Policy.
5	State Bank of India Ltd (SBI)	Yes.	Apart from regular training, drills, multi factor authentication, they use AMLOCK software that uses AI to detect money laundering.
6	Bajaj Finance Ltd.	Yes.	Bajaj Finance has implemented SOAR (Security Orchestration, Automation, and Response) technology to accelerate the maintenance of system security by automating the resolution of security alerts. This reduces response time to security alerts. Has adopted a continuous Vulnerability Assessment and Penetration Testing (VAPT) strategy for our digital assets, allowing for the swift detection and rapid remediation of exploitable vulnerabilities.

7	Hindustan Unilever Limited (HUL)	Yes.	Commitments towards data privacy and cyber security are worded vaguely, such as commitment to monitor and assess risks. HUL has not precisely specified what these measures are. The mention that their privacy policy is compliant with the DPDPA.
8	Indian Tobacco Company (ITC)	Yes.	A Cyber Security Committee, led by the Chief Information Officer (CIO), is established to focus specifically on cyber security risks. Its primary responsibility is to monitor emerging practices and technologies and provide recommendations to enhance the security of the organisation's IT systems and infrastructure. The Chief Information Security Officer (CISO), a recently added role within the organisation, ensures that the cyber security systems remain effective and up-to-date. The CIO actively participates in meetings of the Risk Management Committee whenever matters related to cyber security are discussed.
9	Adani Ports	Yes.	Provides details of cybersecurity and operational improvement, such as firewalls, multi factor authentication.
. 10	Tata Steel	Yes.	Discloses the existence of a Business Continuity plan to cope with cyberattacks, among other things like fire, natural disasters, etc. Explicitly tells shareholders why data security risks are important: *The Company's operations significantly rely on IT and digital infrastructure, which makes it vulnerable to cyber-attacks, data risks and technology obsolescence. Non-compliance to stringent IT legislations and regulations may lead to the imposition of penalties and an adverse impact on the Company's reputation.*
. 11	Adani Enterprises Limited.	Yes.	Lists steps taken by Adani Enterprises on cybersecurity.
. 12	Power Grid Corporation of India.	Yes.	Cybersecurity is listed as a material concern: *Lack of cybersecurity safeguards can lead to cyber-attacks which in turn lead to data breaches, disrupt operations and sometimes lead to legal liability. Cybersecurity breaches can also lead to loss of productivity and can damage the Company's reputation.* Says it has taken steps to mitigate risks: says it has taken steps to mitigate them: *Company has formulated Information Security policy and ensured processes in place for Cybersecurity & data privacy. Company complies with ISO27001:2013 and meets all the applicable legal, statutory, regulatory, and contractual requirements pertaining to cybersecurity.*
. 13	Mahendra and Mahendra Limited	Yes.	Measures to protect cybersecurity include the implementation of cloud security solutions, such as policy remediation and monitoring, with adherence to industry standards such as ISO27001: 2022, and DPDPA.

Table 3: Selected Laws on AI in China

No.	Name of the Law and Relevant Provisions	Issuing Authority and Date	Types of Law
Hard Law			
1	Personal Information Protection Law of the People's Republic of China Article 51 and Article 54	Standing Committee of the National People's Congress 2021.8.20	Laws
2	Interim Measures for the Administration of Generative Artificial Intelligence Services Article 4	Cyberspace Administration of China; National Development & Reform Commission (incl. former State Development Planning Commission); Ministry of Education; Ministry of Science & Technology; Ministry of Industry & Information Technology; Ministry of Public Security; National Radio and Television Administration 2023.7.10	Departmental Rules
3	Regulation of the Shanghai Municipality on Promoting the Development of the Artificial Intelligence Industry Article 53	Shanghai Municipality People's Congress (incl. Standing Committee) 2022.09.22	Provincial Local Regulations
4	Regulation of the Shenzhen Special Economic Zone on the Promotion of Artificial Intelligence Industries Article 41	Shenzhen City People's Congress (incl. Standing Committee) 2022.09.05	Regulations of Special Economic Zones
Soft Law			
1	Notice of the State Council on Issuing the Development Plan on the New Generation of Artificial Intelligence Article 2(3)	State Council 2017.07.08	Regulatory Documents of the State Council
2	Notice by Six Departments Including the Ministry of Science and Technology of Issuing the Guiding Opinions on Accelerating Scenario Innovation and Promoting High-quality Economic Development with High-level Application of Artificial Intelligence Article 2(4)	Ministry of Science & Technology; Ministry of Education; Ministry of Industry & Information Technology; Ministry of Transport; Ministry of Agriculture and Rural Affairs; National Health Commission 2022.07.29	Departmental Regulatory Documents
3	Ethical Norms for the New Generation Artificial Intelligence Article 3	National Governance Committee for the New Generation Artificial Intelligence 2021.09.25	Regulatory Documents of the Department

4	AI Safety Governance Framework Article 3.2	National Technical Committee on Cybersecurity of Administration of China 2024.09	Departmental Rules
5	Global AI Governance Initiative	Cyberspace Administration of China 2023.10	Departmental Working Documents

Table 4. Selected Laws on Data Protection in China

No.	Name of the Law and Relevant Provisions	Issuing Authority and Date Issued	Types of Law
Hard Law			
1	Civil Code of the People's Republic of China Articles 111 and 127	National People's Congress 2020.05.28	Law
2	Personal Information Protection Law of the People's Republic of China Articles 2, 6, 7, 13, 14 and 17	Standing Committee of the National People's Congress 2021.08.20	Law
3	Cybersecurity Law of the People's Republic of China Articles 40-42	Standing Committee of the National People's Congress 2016.11.07	Law
4	Data Security Law of the People's Republic of China Articles 27, 29 and 32	Standing Committee of the National People's Congress 2021.06.10	Law
5	E-Commerce Law of the People's Republic of China Article 23	Standing Committee of the National People's Congress 2018.8.31	Law
6	Anti-Money Laundering Law of the People's Republic of China (2024 Revision) Articles 6 and 7	Standing Committee of the National People's Congress 2024.11.08	Law
7	Regulation on Network Data Security Management Articles 9, 19, 21 and 22	State Council 2024.09.24	Administrative Regulation
8	Regulation on Protecting the Security of Critical Information Infrastructure Articles 14 and 15	Administrative Regulations 2021.07.30	Administrative Regulation
9	Measures for the Security Assessment of Outbound Data Transfer Article 3	Cyberspace Administration of China 2022.07.07	Departmental Rule
10	Measures for the Standard Contract for the Outbound Transfer of Personal Information Articles 3 and 5	Cyberspace Administration of China 2023.2.22	Departmental Rule

11	Provisions on Promoting and Regulating Cross-border Data Flow Articles 2 and 5	Cyberspace Administration of China 2024.3.22	Departmental Rule
12	Interim Measures for the Administration of Generative Artificial Intelligence Services Articles 7,9 and 11	Cyberspace Administration of China; National Development & Reform Commission (incl. former State Development Planning Commission); Ministry of Education; Ministry of Science & Technology; Ministry of Industry & Information Technology; Ministry of Public Security; National Radio and Television Administration 2023.07.10	Departmental Rule
13	Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services Article 7	Cyberspace Administration of China; Ministry of Industry & Information Technology; Ministry of Public Security; State Administration for Market Regulation 2021.12.31	Departmental Rule
14	Notice by the Ministry of Industry and Information Technology of Issuing the Administrative Measures for Data Security in the Field of Industry and Information Technology (for Trial Implementation) Articles 13, 14 and 18	Ministry of Industry & Information Technology 2022.12.8	Departmental Regulatory Document
15	Measures for the Administration of Information Technology Management of Securities Fund Trading Institutions (Amended 2021) Articles 29, 31 and 34	China Securities Regulatory Commission 2025.01.15	Departmental Rule
16	Several Provisions on the Management of Automobile Data Security (for Trial Implementation) Article 5	Cyberspace Administration of China; National Development & Reform Commission (incl. former State Development Planning Commission); Ministry of Industry & Information Technology; Ministry of Public Security; Ministry of Transport 2021.08.16	Departmental Rule
17	Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks Parts II-IV	Standing Committee of the National People’s Congress 2012.12.28	Decisions on Legal Issues and Significant Issues

18	Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to Processing of Personal Information by Using the Facial Recognition Technology Article 2	National Technical Committee on Cybersecurity of Administration of China 2024.09	Judicial Interpretation (quasi-hard law)
19	Notice by the National Health Commission, the National Administration of Traditional Chinese Medicine and the National Administration of Disease Control and Prevention of Issuing the Measures for Administration of Cybersecurity of Medical and Health Institutions Articles 18, 19 and 22	National Health Commission; National Administration of Traditional Chinese Medicine; National Administration of Disease Control and Prevention 2022.08.08	Departmental Regulatory Document
20	Notice by the National Financial Regulatory Administration of Issuing the Measures for the Data Security Management of Banking and Insurance Institutions Articles 9, 20, 22	National Financial Regulatory Administration 2024.12.27	Departmental Regulatory Document
21	Shanghai Data Regulations Article 6, paragraph 2	Shanghai Municipal People's Congress (including Standing Committee) 2021.11.25	Provincial Local Regulation
22	Regulations of Shenzhen Special Economic Zone On Data Article 72, 73, 75, 77 and 78	Shenzhen City People's Congress (incl. Standing Committee)2021.07.06	Regulations of Special Economic Zones
Soft Law			
1	Opinions of the CPC Central Committee and the State Council on Establishing a Data Base System to Maximize a Better Role of Data Elements Article 1	Central Committee of the Communist Party of China; State Council 2022.12.02	System of Party Regulations; Regulatory Documents of the State Council
2	Opinions of the National Data Administration and Other Departments on Promoting the Development and Utilization of Enterprise Data Resources Article 2	National Data Administration; Office of the Central Cyberspace Affairs Commission; Ministry of Industry & Information Technology; Ministry of Public Security; State-owned Asset Supervision & Administration Commission of the State Council 2024.12.20	Departmental Regulatory Document

3	Notice by the National Development and Reform Commission and Other Departments of Issuing the Implementation Plan for Improving Data Circulation Security Governance to Enhance the Marketization and Value Realization of Data Elements Article 1	National Development & Reform Commission (incl. former State Development Planning Commission); National Data Administration; Office of the Central Cyberspace Affairs Commission; Ministry of Industry & Information Technology; Ministry of Public Security; State Administration for Market Regulation 2025.01.06	Departmental Working Document
4	Cybersecurity technology- Basic security requirements for generative artificial intelligence service Article 5.1	National Technical Committee on Cybersecurity of Administration of China 2024.05.23	Departmental Rule

about ECGI

The European Corporate Governance Institute has been established to improve *corporate governance through fostering independent scientific research and related activities.*

The ECGI will produce and disseminate high quality research while remaining close to the concerns and interests of corporate, financial and public policy makers. It will draw on the expertise of scholars from numerous countries and bring together a critical mass of expertise and interest to bear on this important subject.

The views expressed in this working paper are those of the authors, not those of the ECGI or its members.

ECGI Working Paper Series in Law

https://ecgi.global/content/working-papers

Electronic Access to the Working Paper Series

The full set of ECGI working papers can be accessed through the Institute's Web-site (https://ecgi.global/content/working-papers) or SSRN:

Finance Paper Series	http://www.ssrn.com/link/ECGI-Fin.html
Law Paper Series	http://www.ssrn.com/link/ECGI-Law.html